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

LODGED
CLERK, U.S. DISTRICT COURT
2/5/2024
CENTRAL DISTRICT OF CALIFORNIA
BY: CDO DEPUTY

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
February 5, 2024
CENTRAL DISTRICT OF CALIFORNIA
BY: ch DEPUTY

United States of America

v.

CHENGUANG GONG,

Defendant

Case No. 2:24-mj-00663-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 dates of March 31, 2023, to April 25, 2023, in the county of Ventura, in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1832(a)(1)	Theft of Trade Secrets

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Igor Neyman
Complainant's signature

Igor Neyman, 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: February 5, 2024

Judge's signature

City and state: Los Angeles, California

Hon. Brianna F. Mircheff, U.S. Magistrate Judge
Printed name and title

AUSAs: David C. Lachman (x5564) and Nisha Chandran (x2429)

AFFIDAVIT

I, Igor Neyman, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2022. I am currently assigned to the Los Angeles Field Office. As an FBI Special Agent, I have investigated various criminal violations, including the theft of trade secrets, the illegal export of dual-use items (meaning items having both military and commercial applications) and strategic technologies from the United States, and the illegal export of defense articles and other technologies. I attended 18 weeks of New Agent Training at the FBI Academy in Quantico, Virginia, and have since received both formal and informal training from the FBI, including training in identifying the techniques, methods, and procedures employed by groups, organizations, companies, and individuals to commit trade secret theft, economic espionage, and export goods and commodities in violation of United States export laws. Based on my experience and training, I am familiar with efforts and techniques used to unlawfully obtain trade secret information.

2. I make this affidavit in support of a criminal complaint and arrest warrant against Chenguang Gong ("**GONG**") for a violation of Title 18, United States Code, Section 1832(a)(1) (Theft of Trade Secrets).

3. 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 complaint and arrest 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, all amounts or sums are approximate, and all dates and times are on or about those indicated.

II. SUMMARY OF PROBABLE CAUSE

4. A research and development center based in Malibu, California (the "Victim Company"), develops sophisticated infrared sensor technology intended for use in various space-based and military missions, including in systems designed to detect nuclear missile launches and track ballistic and hypersonic missiles. Much of this work is funded through contracts with the U.S. Department of Defense and other U.S. government contractors.

5. Beginning in late January 2023, **GONG** worked as an application-specific integrated circuit ("ASIC") manager at the Victim Company. In that role, **GONG** was responsible for managing the design, development, and performance of readout integrated circuits used in the Victim Company's infrared sensors. Readout integrated circuits collect electrical signals from infrared photo detector arrays and output the data in a standard format. Sophisticated integrated circuit technology is required to achieve the low noise, high dynamic range, high resolution, and

fast readout rate performance required to detect and track missiles and identify other threats.

6. Between approximately March 30, 2023, and April 25, 2023, on 16 different days, **GONG** transferred more than 3,600 files from his work laptop to three personal storage devices, including a Verbatim flash drive and two Western Digital external hard drives. **GONG** transferred more than 1,800 files to the Verbatim flash drive after he had accepted a new job on or about April 5, 2023, at a technology company that directly competes with the Victim Company in the infrared sensor field ("Company 1"). **GONG** then transferred some of these files from the three personal storage devices to his personal computer and to other personal storage devices.

7. Many of the files **GONG** transferred from his work laptop to his personal storage devices contain proprietary and trade secret information, including files marked "[VICTIM COMPANY] PROPRIETARY," "FOR OFFICIAL USE ONLY," "PROPRIETARY INFORMATION," and "EXPORT CONTROLLED." Based on the Victim Company's analysis, the files **GONG** transferred to his personal storage devices include trade secret information, including archive files containing computer-assisted design ("CAD") libraries, relating to the development and design of: (1) the Serrano Readout Integrated Circuit, which combines high dynamic range and time-of-flight capabilities, enabling the tracking of incoming threats in low visibility environments; (2) the Anaheim Readout Integrated Circuit, which combines high sensitivity, a wide field of view, and robust command and control functions,

enabling the detection of missile launches and the tracking of ballistic and hypersonic missiles while providing resilience to radiation in space environments; (3) the Shasta technology development program, which concerns the development of next generation sensors to detect low observable targets while demonstrating improved survivability in strategic space applications; and (4) the mechanical assemblies used to house and cryogenically cool the Victim Company's sophisticated infrared sensors. These files describe the methods, designs, techniques, processes, specifications, testing, and manufacture of these technologies and would be extremely damaging economically if obtained by the Victim Company's competitors, and would be dangerous to U.S. national security if obtained by international actors.

8. On April 26, 2023, in response to **GONG**'s network activity, the Victim Company personnel searched **GONG**'s office and recovered the Verbatim flash drive, which was one of the three personal storage devices that **GONG** used to transfer files. The Victim Company then interviewed **GONG**, who provided evasive and contradictory answers but eventually admitted to having transferred files from his work laptop onto his personal drives and to having viewed those files on his personal computer. The Victim Company then terminated **GONG**'s employment. **GONG** began working for Company 1 on May 1, 2023.[1]

[1] According to records provided by Company 1, Company 1 terminated **GONG**'s employment on May 10, 2023, after receiving information about **GONG**'s file transfers from the Victim Company
(footnote cont'd on next page)

9. On May 8, 2023, the FBI executed a search warrant at **GONG**'s residence in Thousand Oaks, California, and also searched his vehicle and his person. The FBI recovered multiple digital devices belonging to **GONG**, some of which contained proprietary files belonging to the Victim Company. The FBI, however, did not locate the two Western Digital hard drives **GONG** used to exfiltrate the Victim Company's trade secret and proprietary information, and the whereabouts of those drives to date remains unknown. In FBI interviews on May 8, 2023 and May 10, 2023, **GONG** admitted to having transferred some files from his work laptop to his Verbatim flash drive and to having viewed those files on his personal computer, but he continued to deny possessing the Western Digital hard drives or knowing where they are located.

10. Based on my review of **GONG**'s communications and his digital devices, between approximately 2014 and 2022, **GONG** submitted numerous applications to "Talent Programs" administered by the People's Republic of China ("PRC") government. During that period, **GONG** was employed by several major U.S. technology companies and one of the world's largest defense contractors. From my training and experience, I understand that the PRC has established talent programs through which it identifies individuals located outside the PRC who have expert skills, abilities, and knowledge that would aid in

---

and concluding that as "a cleared government facility . . . the risk to the company [was] too great to continue [**GONG**'s] employment."

transforming the PRC's economy, including its military capabilities.

11. Based on my review of **GONG**'s communications and his digital devices, **GONG** took and retained documents, including CAD files, belonging to U.S. technology companies and the U.S. subsidiary of an international defense contractor. Many of these documents bear confidentiality markings, including "Confidential," "Confidential – Maximum Restrictions," "Strictly private and confidential," "Export Controlled," and "ITAR Restricted." In his submissions to the Talent Programs, **GONG** proposed projects that mirrored his work for several of these companies, and repeatedly touted that his proposals would be useful to China's military and that China did not yet have the technologies he was proposing to develop himself or share with Chinese companies.

III. LEGAL BACKGROUND ON TRADE SECRET OFFENSES

12. 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; [or]
>
> (4) attempts to commit any offense described in paragraphs (1) through (3) . . . .
>
> Shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

13. Title 18, United States Code, Section 1839(3) and (4) define 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, another person who can obtain economic value from the disclosure or use of the information[.]
>
> (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.

IV. STATEMENT OF PROBABLE CAUSE

A. The Victim Company Developed and Owns Various Trade Secrets

14. The Victim Company is a physical science and engineering research and development laboratory headquartered in Malibu, California. According to the Victim Company, it conducts research, development, and manufacturing in ultra-high-performance circuitry, robust computing and communications,

automated data extraction, and innovative architected materials for use in the space, aircraft, automobile, and consumer products industries. The Victim Company maintains several laboratories, including a laboratory that researches and develops infrared sensors with high sensitivity, low noise, and high dynamic range at a reduced cost (the "Victim Laboratory").

15. According to R.R., Vice President of the Victim Laboratory and **GONG**'s direct supervisor, the Victim Laboratory's sensors are being developed for use in space-based missile warning and tracking, space-based surveillance, and airborne infrared countermeasures systems, including by the U.S. Department of Defense.[2] The Victim Company is under contract to develop new products with enhanced performance for use in these space and military missions. The Victim Company won these contracts in competitive bids and, together with the U.S. government and others, has invested tens of millions each year for more than seven years to develop the technology, which distinguishes the Victim Company's products from its peer competitors.

16. According to R.R., the Victim Laboratory has developed multiple trade secrets, which are owned by the Victim Company and are associated with proprietary military technologies owned by the Victim Company. These trade secrets are associated with the following technologies:

---

[2] Airborne infrared countermeasures are capabilities that protect aircrafts from heat-seeking missiles by jamming the missile's infrared tracking ability.

a. The Serrano Readout Integrated Circuit is an integrated circuit that combines the functionality of infrared search-and-track with infrared countermeasures into a single chip. The Serrano Readout Integrated Circuit is able to offer both high dynamic range (to track threats in low visibility settings) and time-of-flight capabilities (to analyze how quickly the threat is approaching). The Victim Laboratory's technical team has spent years and millions of dollars to develop the Serrano Readout Integrated Circuit. The Victim Company considers the methods, techniques, processes, testing, and specifications -- both successful and unsuccessful -- regarding the design, manufacture, and operation of the Serrano Readout Integrated Circuit to each be trade secrets (collectively referred to as "Serrano Trade Secrets").

b. The Anaheim Readout Integrated Circuit is an integrated circuit that combines the features of high sensitivity, a wide field of view, small pixel pitch, and command and control and data handling that enable it to reliably detect missile launches and track ballistic and hypersonic missiles. The Anaheim Readout Integrated Circuit also is radiation hardened, making it suitable for high reliability space missions. The Victim Laboratory's technical team has spent years and millions of dollars in developing the Anaheim Readout Integrated Circuit. The Victim Company considers the methods, techniques, processes, testing, and specifications -- both successful and unsuccessful -- regarding the design, manufacture, and operation of the Anaheim Readout Integrated

Circuit to each be trade secrets (collectively referred to as "Anaheim Trade Secrets").

c. The Victim Company's Shasta program involves the development of next generation sensors that can detect low observable targets while demonstrating improved survivability in strategic space applications. Although the Shasta program is currently on hold, the Victim Company considers the methods, techniques, processes, testing, and specifications -- both successful and unsuccessful -- regarding the development of the Shasta program to each be trade secrets (collectively referred to as "Shasta Trade Secrets").

d. High-performance sensors like the Serrano and Anaheim Readout Integrated Circuits must be mechanically enclosed and cryogenically cooled from heat emitted by the circuit. To keep the circuits cool, the Victim Company has designed proprietary compact Integrated Dewar Cooler Assemblies. The Victim Company considers the methods, techniques, processes, testing, and specifications -- both successful and unsuccessful -- regarding the development of the mechanical assembly and cooling of its sensors to each be trade secrets (collectively referred to as "Mechanical Trade Secrets"). Collectively, the Serrano Trade Secrets, Anaheim Trade Secrets, Shasta Trade Secrets, and Mechanical Trade Secrets constitute the "Trade Secret Information."

17. According to L.M., the Victim Company's Executive Vice President, these trade secrets are foundational technologies that support the Victim Company's business. If the Victim

Company's competitors were to obtain the designs or development roadmaps for the Serrano, Anaheim, Shasta, or Mechanical Trade Secrets, they would be able to replicate and improve on the Victim Company's products, as well as the technology that goes into the Victim Company's products, resulting in those competitors being able to beat out the Victim Company for competitive bids and potentially rendering the Victim Company's business obsolete. The Victim Company estimates that the value of the Trade Secret Information is in the hundreds of millions of dollars. Additionally, if the Victim Company's Trade Secret Information was obtained by a foreign government, it would compromise U.S. national security.

B. GONG's Background

18. According to my review of **GONG**'s U.S. and Chinese passports, applications for employment and PRC Talent Program funding, bank statements, and email communications, **GONG** was born in 1966 in Zhejiang province in China. Hangzhou is the capital and largest city of Zhejiang province. **GONG** first entered the United States in or around 1993 and became a United States citizen in 2011. After arriving in the United States, **GONG**'s resume states that he earned a Master of Science Degree in Electrical Engineering from Clemson University and completed some PhD work at Stanford University.

19. From the late 1990s to 2023, **GONG** worked for a number of prominent U.S. technology companies, as well as an international defense, aerospace, and security company, before joining the Victim Company in January 2023. As relevant here,

from approximately 2010 to May 2014, **GONG** worked as an integrated circuit design manager for a U.S. information technology company in Santa Clara, California ("Company 2").[3] From approximately May 2015 to October 2019, **GONG** was a CMOS[4] image sensor design manager for the U.S. subsidiary of an international defense, aerospace, and security company ("Company 3") in San Jose, California. After working for 10 months for a semiconductor company, **GONG** joined a U.S. technology company headquartered in Cupertino, California ("Company 4") in July 2020, where he worked as a silicon development product manager until October 2021. Then, from November 2021 to April 2023, **GONG** worked for a CMOS image sensor research, design, and manufacturing company headquartered in San Jose, California ("Company 5"). On January 30, 2023, **GONG** joined the Victim Company as an ASIC manager.[5]

---

[3] According to records obtained from Company 2, as well as a draft of **GONG**'s Application for Naturalization, **GONG** worked for a U.S. semiconductor manufacturer in Santa Clara, California, from approximately 2010 to 2011. Based on open-source research, Company 2 acquired the U.S. semiconductor company in 2011.

[4] Based on internet research, a complementary metal-oxide-semiconductor ("CMOS") sensor is an image sensor in which each pixel sensor unit has a photodetector and one or more active transistors. CMOS sensors are used to create images in digital cameras and other electronic devices, with both commercial and military applications.

[5] According to my review of **GONG**'s emails, **GONG** continued to work for Company 5 during at least the first month of his employment at the Victim Company. On January 13, 2023, after **GONG** had accepted a position at the Victim Company, he informed his supervisor at Company 5 via email that he planned to take vacation during the month of February 2023 to visit and care for his parents in China. Then, on February 26, 2023, after **GONG** had been working at the Victim Company for several weeks, **GONG** told his supervisor at Company 5 via email that he needed to be

(footnote cont'd on next page)

C. January 2023: The Victim Company Hires GONG to Develop Key Technology and Gives Him Access to Proprietary Technology

20. According to R.R., the Victim Company hired **GONG** in January 2023 to work at the Victim Laboratory as an ASIC manager responsible for the design, development, and verification of the Victim Laboratory's sensor assembly. **GONG**'s job functions focused on ASIC sensor design, not sensor manufacturing. At the Victim Laboratory, sensor ASIC design engineers rarely had any overlap or interaction with sensor ASIC manufacturing engineers.

21. According to R.R., **GONG** was given access to the Victim Laboratory's full data repository in light of **GONG**'s managerial role. The data repository contained, among other things, design details and records on how to develop and build the Victim Laboratory's products, testing data, roadmaps for future improvements to the Victim Laboratory's existing products, funding opportunities for the Victim Laboratory's current products, and information about new product opportunities. In other words, **GONG** had access to the full history, specifications, and roadmap of the Victim Laboratory's products.

22. According to R.R., at the Victim Company, engineers such as **GONG** used computer-assisted design programs to design and develop infrared sensors assemblies, including readout integrated circuits. The CAD programs and related files used to

---

present in China on February 28, 2023, for a medical examination for his father, and requested a leave of absence. At the time, **GONG** was working for the Victim Company in Camarillo, California, and DHS travel records do not show any travel for **GONG** to or from China during this time period. **GONG** only notified Company 5 on March 20, 2023, that he intended to give up his position at the company.

develop the Victim Company's sensor products reside in and can only be used on a UNIX computer operating system. The Victim Company's employees access the UNIX system using a virtual machine. Within the Victim Company's UNIX system, each product has a library, and within the product library, each user has a library. Exporting a product or user library from the UNIX system to the Microsoft Windows operating system, like the operating system on **GONG**'s work laptop, requires the user to first manually run scripts that save the design files in an archive file, such as a .bz2 file, which preserves the underlying library structure. The user then has to transfer the archive file from the UNIX environment to the Microsoft Windows environment using a file transfer protocol program. Only after the files are transferred from UNIX to the Microsoft Windows environment is the user able to copy or transfer the files from the Victim Company's systems to an external storage device.

23. According to R.R., there is no legitimate business purpose for an individual user, such as **GONG**, to move the CAD files and libraries from the UNIX system to the Microsoft Windows environment. The product and user libraries are not viewable without a UNIX server and specialized computer chip design tools, software, and models that only run in the UNIX environment. In addition, these chip design tools and software require licenses costing over $100,000. In an audio-recorded interview on May 10, 2023, **GONG** admitted that he did not have the software required to be able to view these files.

D. April 2023: GONG Removes Proprietary Information Belonging to the Victim Company Without Authorization and Unexpectedly Resigns

24. According to the Victim Company, on April 14, 2023, less than three months after he was hired, **GONG** notified the Victim Company that he was resigning from his position. **GONG**'s last day of employment was scheduled to be April 28, 2023. Although **GONG** had performed well, he told the Victim Company he was leaving because he felt he was not doing a good job and the Victim Company should hire someone better.

25. According to D.M., the Victim Company's Director of Security, the Victim Company began monitoring **GONG**'s network activity and discovered that beginning on March 30, 2023 -- two weeks before he submitted his resignation -- **GONG** had transferred thousands of files onto three personal storage devices, in violation of the Victim Company's policies. The three personal storage devices **GONG** used to export files from the Victim Company's system are: (1) a Verbatim Ltd. flash drive, bearing serial number 07010C5AB99B2F78 (the "Verbatim Flash Drive"); (2) a Western Digital Technologies, Inc. external hard drive, bearing serial number 57584D314539373450543055 (the "WD Drive 1"); and (3) a Western Digital Technologies, Inc. flash drive, bearing serial number 57583332444332523930 4C46 (the "WD Drive 2").

26. The files **GONG** transferred to his personal storage devices included documents marked as "[VICTIM COMPANY] PROPRIETARY," "EXPORT CONTROLLED," "FOR OFFICIAL USE ONLY," and "PROPRIETARY INFORMATION," among others. In addition, according

to the document markings, certain of the transferred files "contain technical data within the definition of the International Traffic in Arms Regulations and are subject to the export control laws of the U.S. Government." As indicated on the markings, the transfer of ITAR-controlled data "by any means to a foreign person, whether in the U.S. or abroad, without an export license or other approval from the U.S. Department of State, is prohibited."


RESTRICTION ON DISCLOSURE AND USE OF DATA

[redacted] PROPRIETARY

EXPORT CONTROLLED - This documents contain technical data within the definition of the International Traffic in Arms Regulations, and are subject to the export control laws of the U.S. Government. Transfer of this data by any means to a foreign person, whether in the U.S. or abroad, without an export license or other approval from the U.S. Department of State, is prohibited.

27. According to the Victim Company, as well as my review of records from the Victim Company (including reports of **GONG**'s file transfer activity), and my review of **GONG**'s digital devices, **GONG** transferred numerous files containing sensitive, proprietary, and trade secret information from his work laptop to his personal storage devices, including but not limited to the following:

a. On March 31, 2023, **GONG** transferred more than 760 files relating to several of the Victim Company's projects from his work laptop to WD Drive 1.[6] These files included approximately 185 .bz2 archive files, discussed above. According to the Victim Company, these .bz2 files, which **GONG**

[6] Unless otherwise stated, referenced file quantities include some .zip files that aggregate transferred files. Each .zip file is counted as a single file. Referenced file quantities also include files that appear to be transferred from the public domain.

exported from the Victim Company's UNIX system, contained the CAD blueprints for designing, testing, and manufacturing the Victim Company's sensors, including product and user libraries for various versions of the Anaheim and Serrano Readout Integrated Circuits. In conjunction, the product libraries contained the schematic information necessary to implement the architecture and circuit design for the Victim Company's integrated circuits, as well as the related physical and digital characteristics of the integrated circuits. They also included the information required to allow a semiconductor foundry to "print" all of the necessary layers to manufacture the circuits. The user libraries -- including the user libraries of **GONG**'s supervisor and other colleagues known to be successful within the Victim Company and the industry -- typically contained all the product design choices and simulations of the particular user. Based on the Victim Company's analysis and review of a selection of these files, these archive files contained some of the Victim Company's most valuable trade secrets, including the Serrano and Anaheim Trade Secrets. Additionally, **GONG** transferred dozens of presentations and other files containing testing results, progress summaries, specifications, and confidential client projects relating to the development of the Serrano and Anaheim Readout Integrated Circuits. The Victim Company confirmed that the disclosure of the information contained in these files would be extremely damaging to the Victim Company.

b. On April 6, 2023, **GONG** transferred approximately 939 files from his work laptop to WD Drive 2. These files included approximately 35 archive files (including .bz2 files, .gz files, and .tar files) containing design files and blueprints for the Serrano Readout Integrated Circuit.[7] Based on the Victim Company's analysis and review of a selection of these files, the Victim Company confirmed that they contained some of the Victim Company's most valuable trade secrets, including the Serrano Trade Secrets, and that the disclosure of the information contained in these files would be extremely damaging to the Victim Company. **GONG** also transferred at least two files containing the designs for the mechanical Integrated Dewar Cooler Assemblies, which, according to the Victim Company, were not relevant to **GONG**'s ASIC design role.

c. From March 30, 2023 and continuing until at least April 25, 2023, **GONG** transferred more than 1,900 files from his work laptop to the Verbatim Flash Drive, in violation of the Victim Company's policies. **GONG** transferred more than 1,800 of these files to the Verbatim Flash Drive on or after April 5, 2023, when **GONG** had already accepted a job at Company 1, one of the Victim Company's main competitors. On April 14, 2023, **GONG** notified the Victim Company of his intent to resign from his job by the end of the month. According to the Victim Company and my review of **GONG**'s file transfer activity, after submitting his

[7] The files also included hundreds of source code files relating to "Indium Electroplating," which according to the Victim Company pertained to the manufacturing process for integrated circuits and were not related to **GONG**'s role at the Victim Company.

resignation, **GONG** continued to transfer files from his work laptop to his personal storage devices, including files containing sensitive, proprietary, and trade secret information belonging to the Victim Company. These transfers included files and test results relating to a confidential client project known as "Pyramid," which involved the Serrano Readout Integrated Circuit; summaries of testing and issue identification, detailed product specifications, summaries of experiments, and implementation details for client review meetings regarding the Anaheim Readout Integrated Circuit; test results, issue logs, and trial probe results relating to the Serrano Readout Integrated Circuit; and troubleshooting, issue logs, and client review documents that outline product specifications, testing and implementation details regarding the Anaheim Readout Integrated Circuit; more than 100 CAD files (with .bz2, .dwg, .dxf, or .bak file extensions), mostly pertaining to the Anaheim Readout Integrated Circuit; and other files marked as "[VICTIM COMPANY] PROPRIETARY" relating to other technologies, including the Shasta program.

28. In total, **GONG** transferred more than 3,600 files from his work laptop onto three personal storage devices:

a. The Verbatim Flash Drive, to which **GONG** transferred approximately 1,900 files, including files that contain Serrano and Anaheim Trade Secrets, among others, was

recovered from **GONG**'s office at the Victim Company on April 26, 2023.[8]

b. WD Drives 1 and 2, to which **GONG** transferred approximately 1,700 files, including files that contain Serrano and Anaheim Trade Secrets, among others, have not yet been located by law enforcement. According to my review of the Victim Company's records and **GONG**'s personal laptop, which was seized on May 8, 2023,[9] **GONG** transferred proprietary files from his work laptop to WD Drive 1 on March 31, 2023, and last plugged WD Drive 1 into his personal laptop on April 6, 2023. Based on the same sources, **GONG** last transferred proprietary files belonging to the Victim Company from his work laptop to WD Drive 2 on April 10, 2023, and last plugged WD Drive 2 into his personal laptop on April 28, 2023 -- days after he was terminated by the Victim Company (discussed below).

29. From my review of **GONG**'s personal digital devices, including flash drives and external hard drives that were seized from **GONG**'s Thousand Oaks residence, I know that after **GONG** transferred files from his work laptop to his personal storage

---

[8] **GONG** had deleted or transferred many of these files from the Verbatim Flash Drive before the Victim Company recovered the drive on April 26, 2023.

[9] On May 5, 2023, the Honorable Maria A. Audero, United States Magistrate Judge, authorized the search of **GONG**'s Verbatim flash drive in Case No. 23-MJ-2242, which was reopened on January 5, 2024, by the Honorable Alicia G. Rosenberg in Case No. 24-MJ-00082. On May 5, 2023, the Honorable Maria A. Audero, United States Magistrate Judge, also authorized the search of **GONG**'s Thousand Oaks residence in Case No. 23-MJ-2243. That warrant was executed on May 8, 2023, and the government seized multiple digital devices. The search period was extended by the Honorable Margo A. Rocconi on September 7, 2023, and by the Honorable Alicia G. Rosenberg on January 4, 2023.

devices, he then transferred some of those files to other personal digital devices. For example, **GONG** transferred proprietary files pertaining to the Victim Company's Anaheim Readout Integrated Circuit from his work laptop to his personal storage devices, and then transferred those files to another personal external hard drive recovered from **GONG**'s Thousand Oaks residence. Additionally, **GONG** transferred proprietary testing and issue logs pertaining to the Victim Company's Serrano Readout Integrated Circuit and Anaheim Readout Integrated Circuit, and files containing other manufacturing parameters and specifications, from his work laptop to his personal storage devices, and then transferred those files to his personal laptop computer recovered from **GONG**'s Thousand Oaks residence. In my training and experience, because flash drives have limited storage capacities, individuals typically use flash drives as short-term storage and transfer those files to hard drives or other larger storage devices to preserve those files.

D. GONG Admits to Transferring Information Belonging to the Victim Company to His Personal Storage Devices

30. The Victim Company interviewed **GONG** on April 26, 2023, which was audio recorded. **GONG** admitted that he knew it would be wrong for him to take the Victim Company's proprietary information and that he had signed a form acknowledging that he would safeguard such information. **GONG** initially denied that he used a personal storage device to transfer files from his work laptop. When then confronted with evidence about his file transfers, **GONG** provided inconsistent explanations. **GONG**

initially denied having transferred any files to any personal storage devices, then admitted he transferred files but claimed he only moved three documents, then claimed he only transferred public documents, and finally stated that someone else had said something that made him "curious," which caused him to make the file transfers, and that he had transferred the files to read them at home. **GONG** refused to tell the Victim Company where he was renting a home. The Victim Company terminated **GONG**'s employment following the interview.

31. FBI agents interviewed **GONG** in recorded interviews on May 8, 2023 and May 10, 2023. Based on my review of those recordings, **GONG** was warned multiple times that making false statements to the FBI is illegal. During the interviews:

a. **GONG** admitted to transferring files onto the Verbatim Flash Drive and to accessing the transferred files at home but denied the full extent of his conduct, providing conflicting explanations as to why he transferred the files. **GONG** initially denied multiple times that he owned any personal drives other than the Verbatim Flash Drive. **GONG** then admitted that he had two hard drives at home, but said that he did not have any Western Digital hard drives. Based on my review of files obtained from the Victim Company and **GONG**'s digital devices seized from the Thousand Oaks residence, I know that **GONG** plugged the Verbatim Drive, WD Drive 1, and WD Drive 2 into his work laptop, and that **GONG** plugged the Verbatim Flash Drive into his personal laptop as recently as April 25, 2023, plugged the WD Drive 1 into his personal laptop as recently as April 6,

2023, and plugged the WD Drive 2 into his personal laptop as recently as April 28, 2023. Based on my review of Amazon records, I also know that **GONG** purchased multiple Western Digital hard drives and shipped them to his current primary residence in San Jose, California, as well as to his Thousand Oaks residence.

b. **GONG** also admitted to transferring files but first stated that he only transferred emails. He insisted that he did not transfer any data about the Victim Company's projects or technologies, or that if he did so it was a mistake. Based on my review of files obtained from the Victim Company, I know that **GONG** transferred more than 3,600 files (consisting of Word documents, PowerPoint presentations, PDFs, images, and other design files) over 16 days. More than 1,280 of those files were larger than one megabyte, and approximately 190 files were larger than 100 megabytes. It would also have required time and effort to export hundreds of CAD design files, which contained the technical blueprints for the Victim Company's products and technologies, from the Victim Company's UNIX system to a Microsoft Windows operating system.

E. The Victim Company Employed Reasonable Measures to Protect Its Trade Secrets

32. At all relevant times, the Victim Company employed reasonable measures to protect its trade secrets. The Victim Laboratory is located at the Victim Company's facility in Camarillo, California. According to D.M., the Victim Company's Director of Security, the Victim Company employs physical

security measures to protect its trade secret information. For instance:

a. Unauthorized visitors are not permitted to park on the Victim Company's property, and the Victim Company's employees who park at the facility must use window stickers provided by the Victim Company to identify their vehicles.

b. Clearly visible signs on the exterior of the building notify employees and visitors that all entrants to the facility are subject to inspection by authorized security representatives, including inspection of any and all packages, including lunch boxes, purses, briefcases, and other containers carried into or out of the facility. The signs also state that identification badges must be worn and visible at all times while on company premises and that unauthorized photography or recording is strictly prohibited.

c. CCTV surveillance covers the perimeter of the facility.

d. The doors to the he Victim Company's facility are locked at all times, even during normal business hours. Employees are required to use an access badge to enter the facility. Visitors are required to use an intercom on the front door to enter the building, which has a camera at the front door. Immediately inside the front door is a 24/7 manned security desk with a uniformed guard who processes and monitors all visitors to the facility.

e. Due to the Victim Company's "need to know" policy, employees at the Camarillo facility are not necessarily

granted access to all other facilities, nor are employees at the Victim Company's other campuses necessarily granted access to the facility in Camarillo.

33. The Victim Company also employs cyber-security measures to protect its trade secret information. For example:

a. Employees need a username and password to access their work computers, which have two-factor authentication for added security. Employees are not permitted to share their passwords with anyone, plug any personal electronic device into the Victim Company's computer networks, or conduct any work on personal laptops.

b. While on the Victim Company's network, and absent a need to know, employees lack access to areas of the network that are not connected with their work.

c. The Victim Company has an internal cyber team monitoring its networks for potential threats and to ensure compliance with national standards for economic security.

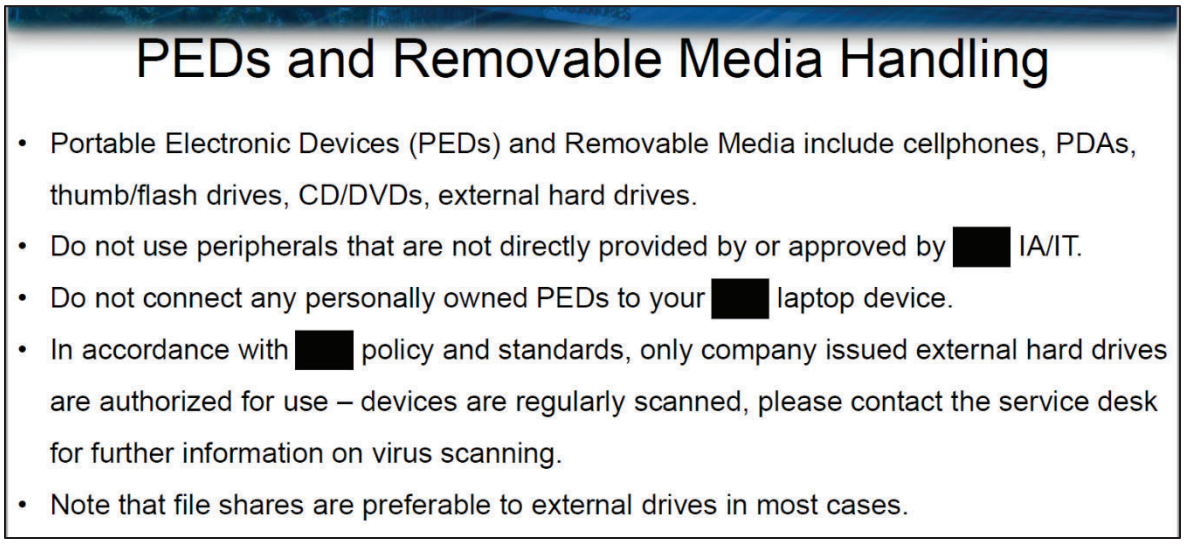
34. According to D.M. and my review of the Victim Company's records, the Victim Company also uses various company policies and trainings to notify and remind its employees that certain information owned by the company is proprietary trade secret information and that all employees have a duty to protect such information. For example:

a. The Victim Company requires new employees to read and sign a "Statements and Agreements" form, which requires employees to acknowledge that as part of their employment, they "will be exposed to trade secrets and other proprietary and

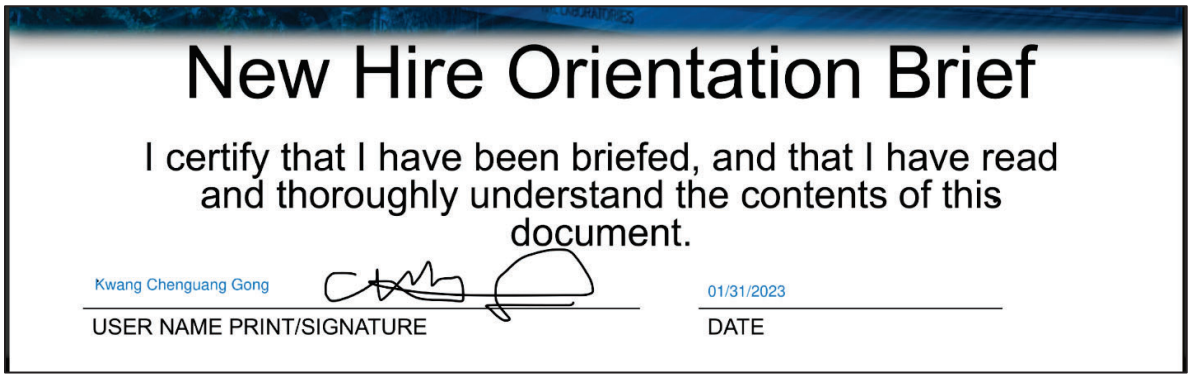
confidential information of [the Victim Company]" and that they will receive such information "under an obligation of confidentiality." Employees are required to acknowledge that the disclosure of such information to any future employer would be in violation of their agreement of confidentiality with the Victim Company and that transfer of such information would "amount to an unfair trade practice." The Statements and Agreements form further states that the success of the Victim Company depends, among other things, upon maintaining strictly confidential and secret information relating to the Victim Company's trade secrets, designs, products, methods, processes, research, development, and other competitive information, to which employees may have access. The form thus requires employees to agree that they will use their "best efforts to exercise utmost diligence to protect and guard the Proprietary Information of [the Victim Company]," to promise they will not disclose or use any proprietary information, except as required in connection with their employment, and to acknowledge they will not retain any copies, notes, or other documents relating directly or indirectly to any proprietary information, either during or after their employment. **GONG** signed the Statements and Agreements form on January 30, 2023.

b. All new employees must attend a Cybersecurity Orientation Briefing and sign an acknowledgment form. A copy of the training PowerPoint stated, among other things: "Proprietary Information, also known as trade secret, refers to any method, formula, device, process, or any information that gives the

business a unique competitive advantage in the marketplace. As [a Victim Company] employee you are obligated to protect this information." The training provided examples of proprietary information, including R&D (research and development) information, software algorithms, inventions and designs, formulas and ingredients, and devices. The training informed employees they were prohibited from a number of actions, including "[b]ypassing security mechanisms or architecture that have been put in place to prevent or isolate access or privileges"; "moving, relocating, or changing configuration of any software or hardware on or in [the Victim Company's] IT system" or storing such information improperly; and "using [work] devices for non-[Victim Company] work for personal gain or another job." The training also includes a slide on handling portable electronic devices and removable media, including "external hard drives," which instructs that employees must not "connect any personally owned [devices] to [their VICTIM COMPANY] laptop device":



Finally, the training states that employees have "an obligation to report any network activity that seems suspicious amongst their peers or other personnel on the [Victim Company] network," such as "[u]nauthorized access to systems or data" or "[a]ny attempt to transport data onto personal devices or unapproved cloud solutions." **GONG** attended this training on January 30, 2023, and signed the acknowledgment form on January 31, 2023:


New Hire Orientation Brief

I certify that I have been briefed, and that I have read and thoroughly understand the contents of this document.

Kwang Chenguang Gong

USER NAME PRINT/SIGNATURE

01/31/2023

DATE

c. Upon logging into their workstations, employees are presented with the Victim Company's "Notice and Consent" banner, which states that the system is "the property of [the Victim Company] and is for authorized company business use only." The banner reminds employees of their obligation to comply with all of the Victim Company's "policies, procedures, and guidelines for the protection of company information or information that the company has an obligation to protect, including but not limited to proprietary information, personally identifiable information, Controlled Unclassified Information (CUI), and export-controlled information."

F. GONG Begins Working at a Competitor of the Victim Company

35. According to my review of his email communications, **GONG** had accepted a position at Company 1 on or before April 5, 2023. As discussed above, **GONG** continued downloading files from the Victim Company until April 25, 2023. According to Company 1's website, the company is a leader in military, space, astronomy, and commercial applications of high-performance imaging systems, and its products also include "Read-Out Integrated Circuits," similar to the Serrano Circuit and Anaheim Circuit. According to the Victim Company, a "Report for Work" notice from Company 1, and FBI surveillance, Company 1 hired **GONG** as a Senior Manager, Digital & Analog Mixed Signal IC Design, to begin on May 1, 2023. On that day, FBI agents observed **GONG**'s car in the lot on Company 1's campus.[10]

G. Background on PRC Talent Programs

36. From my training and experience, my review of reports, and information received from other agents, 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

[10] According to records provided by Company 1, after learning from the Victim Company that **GONG** had transferred files onto personal storage devices, Company 1 terminated **GONG**'s employment on about May 10, 2023. In the termination letter, Company 1 stated that as "a cleared government facility," it "take[s] measures to assure [its] programs, including related confidential and proprietary information, are safeguarded to the best of [its] ability," and had concluded that "the risk to the company [was] too great to continue [**GONG**'s] employment." Based on my discussions with the President of Company 5 and my review of **GONG's** email communications, I believe that **GONG** currently works for Company 5 in San Jose, California.

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").

37. 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.

38. 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.

39. 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. Through the Talents Programs, the PRC government recruits Western-educated individuals to work and conduct technical and scientific research on behalf of the PRC and in furtherance of the PRC's strategic national development goals.

40. 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.

41. 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 certain 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.

42. 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.

H. GONG Applied for Talent Program Funding, Including to Produce High-Performance ADCs to Benefit China's Military and Defense Sector, from at Least 2014 to 2022

43. Based on my knowledge of the investigation and my review of **GONG**'s emails and documents obtained from his digital devices pursuant to federal search warrants, **GONG** submitted numerous applications to various Chinese Talent Programs between at least 2014 and 2022, as set forth in detail below.[11]

44. From approximately 2010 to May 2014, **GONG** was employed at Company 2, a U.S. information technology company headquartered in Dallas, Texas. According to its website, Company 2's business focused primarily on developing analog chips and embedded processors. **GONG** worked for a business unit based in Santa Clara, California, as a power management integrated circuit design manager. According to an April 2014 performance improvement plan, **GONG**'s manager at Company 2 had expressed concerns in several meetings about **GONG**'s performance, as **GONG** had not met expectations on a number of tasks. **GONG** left Company 2 the following month but retained hundreds of documents belonging to Company 2 that were marked as confidential or proprietary.

45. On November 2, 2013, while still employed by Company 2, **GONG** sent a business proposal to C.Y., who according to a

[11] Unless otherwise indicated, all communications described in this section occurred in Mandarin and have been translated into English using Google Translate, a multilingual neural machine translation service.

LinkedIn invite C.Y. later sent to **GONG** was an "Innovation Connector" between Hangzhou, China, and Silicon Valley, California.[12] In his email, **GONG** thanked C.Y. for speaking with him and providing input on his business proposal. The attached proposal described a plan to produce "high-throughput[,] high-performance" analog-to-digital converters ("ADCs") and digital-to-analog converters ("DACs") in China, and noted that the global market for 12-to-16 bit converters "is basically monopolized by several companies in the United States" and that the export of 14-bit and 16-bit ADCs and DACs from the United States requires a "government export license." **GONG** represented that he had formed a company called "Sailan Hi-tech (MII)," also known as MII, Magic Icfab Inc., or Seran Hi-tech,[13] and aimed to produce 14-bit 250 mega-samples per second ("MSPS") ADCs for evaluation by Huawei and other companies, and was developing 16-bit 100-370 MSPS ADCs.[14] On November 3, 2013, C.Y. responded

---

[12] According to a 2018 filing with the California Secretary of State, C.Y. was the Chief Executive Officer of the Hangzhou Silicon Valley Innovation Center LLC, a technology venture backed by Hangzhou, a city in eastern China. According to news reports, the Hangzhou Silicon Valley Innovation Center bought a two-story building in San Jose, California, in 2018 for $41.5 million in cash.

[13] According to records from the California Secretary of State, **GONG** registered "Magic Icfab, Inc." with the State of California in 2004. According to his filings, the company engaged in the business of "VLSI Design Service," which based on internet research refers to Very-Large-Scale Integration design, which is the process of creating an integrated circuit by combining millions or billions of transistors onto a single chip. **GONG** filed a notice of dissolution with the California Secretary of State on September 4, 2008.

[14] According to publicly available information, in data conversion, an analog signal is converted to a stream of

(footnote cont'd on next page)

with "a few more suggestions," and advised **GONG** that "government funding should not be mentioned," as "[t]his is not a financing channel, and even if it is, it should not be mentioned." Based on my review of product data sheets, Company 2, where **GONG** was employed at the time he sent this November 2013 email, released a 14-bit ADC with a sampling rate of 250 MSPS in May 2014 and 16-bit ADC with a sampling rate of 370 MSPS in April 2014.[15]

46. On March 23, 2014, **GONG** wrote to W.H. (at an email address with a @163.com domain),[16] who according to publicly available information was the contact person for the 38th Research Institute of China Electronics Technology Group Corporation, a high-tech research institute located in Hefei City, China, that focuses on both military and civilian products. In his email, **GONG** inquired whether W.H. would be interested in pursuing "such a project," referring to an attached business proposal titled "MII3b_to_38i.pdf." The business proposal is substantially the same as the proposal **GONG** sent to C.Y. in November 2013. **GONG** attached a copy of his

---

numbers, each representing the analog signal's amplitude at a moment in time. Each number is called a "sample," and the number of samples per second is called the sampling rate. Mega-samples per second ("MSPS") refers to millions of samples per second.

[15] In various versions of **GONG**'s project proposals regarding high-performance ADCs, **GONG** includes an image taken almost unaltered from a document entitled "High Speed ADC Catalog Roadmap," which appears to belong to Company 2 and is marked as "[Company 2] Confidential."

[16] Based on my training and experience, as well as my review of publicly available information, I know that the domain @163.com is hosted by the Chinese IT company NetEase, Inc., which is one of China's largest providers of free email services.

resume to the proposal, which noted that **GONG** had worked for the "Zhejiang Science and Technology Commission" as a government employee for approximately three years in the 1990s.[17]

47. On July 31, 2014, **GONG** received an email from F.X. (using an email address with a @163.com domain), who stated that he was with the "Hangzhou Qianjiang Economic Development Zone" and was "currently stationed in the United States." F.X. noted that **GONG** had previously submitted a "Sa[i]lan Hi-Tech Digital Integrated Circuit Design" project to a Hangzhou talent program and invited him to apply to several talent programs, including the Hangzhou Qianjiang Economic Development Zone "3615" Talent Introduction Plan. On August 2, 2014, **GONG** responded to F.X.'s email and stated that he would like to open a company in Hangzhou, and a few days later **GONG** provided his U.S. phone number to F.X. On August 10, 2014, **GONG** submitted to F.X. an application to the Hangzhou Qianjiang Economic Development Zone "3615" Talent Introduction Plan. In the application, which **GONG** noted was only partially completed, **GONG** described his proposed project to develop 16-bit 100-370 MSPS analog-to digital converters as follows:

> In fields such as national defense, military, and aerospace, high-performance analog-to-digital and digital-to-analog converters directly determine the

[17] Based on my training and experience, as well as internet research, I believe that **GONG** was likely referring to the Zhejiang Association for Science and Technology ("ZJAST"), which is an organization under the leadership of the CPC Zhejiang Provincial Committee and "serves as a bridge that links the Party and the provincial government to the science and technology community and plays an important role in promoting the development of science and technology in Zhejiang." See, e.g., http://fad.zj.gov.cn/art/2021/5/11/art_1229498540_58897344.html.

> accuracy and range of radar systems, of which 12[-bit] ADCs with 200 megabit or above . . are completely monopolized by major American manufacturers such as ADI and TI, and are regarded as high-end products [i]ncluded on the U.S. embargo list.
>
> [. . .]
>
> The completion of this project will bring domestic high-speed and high-precision analog-to-digital converter (ADC) development to the same highest level as that of international companies such as ADI/TI, far exceeding the embargo indicators. [This] will fill the domestic gap and lay a core foundation for high-end equipment and equipment manufacturing . . . and get rid of the United States blockade of China's product lines in this category.

GONG listed the export-controlled nature of the products as one of the "strengths" of his proposal and further noted that it was "almost impossible" for Chinese institutions to obtain such high-end products.

48. According to his resume, **GONG** worked as a CMOS image sensor design manager for Company 3, an international defense, aerospace, and security company, in San Diego, California, from approximately May 2015 to October 2019. According to its website, among other products, Company 3 develops visible and infrared imaging sensors for a wide variety of commercial and military applications, including for use in military weapons systems and satellites.

49. In January 2017, while employed at Company 3, **GONG** wrote to the human resources department of the 38th Research Institute of China Electronics Technology Group Corporation (at an email address with a @163.com), indicating that he "would like to apply for funding for entrepreneurial teams," and attached a copy of his resume and a summary of his proposed

project, which again centered around the development of "high-performance analog-to-digital (ADC) and digital-to-analog converters (DAC)," which appears to relate to technology **GONG** worked on at Company 2. **GONG** also reiterated the military utility of such products, explaining that for every one bit increase in accuracy, the "detection distance" of radar systems "can be increased by 10 kilometers." He further stated that "[m]issile navigation systems also often use radar front-end systems, and radar technology is also used in military radars." **GONG** also highlighted that there were "almost no" companies in China capable of developing and producing such products, which were subject to U.S. export controls, and that with the requested funding his startup company would "become the leader in the field of data converters in China, providing customization for the military and civilian fields."

50. **GONG** shifted focus later in 2017 and in 2018, working on business proposals while still employed at Company 3 to develop a technology for detecting defects in touchscreen displays. He also submitted several talent program applications proposing the development of a "quantum bioresonance chip" that would be integrated into wearable electronic products. Based on my review of **GONG**'s emails, it does not appear that those applications were accepted.

51. Throughout 2019, **GONG** applied for funding to various different talent programs, including the Hangzhou Xihu District 325 Talent Plan, the Hangzhou West Lake District 325 Talent Plan, and the "Maker World" Hangzhou Entrepreneurship

Competition. **GONG'** proposals in those applications included the development and production of high-performance ADCs and Gallium Nitride radio frequency power amplifiers.[18]

52. Based on my review of **GONG'**s emails and U.S. Department of Homeland Security ("DHS") travel records, **GONG** also traveled to China twice in 2019 to participate in talent program conferences in China at the invitation of the organizing committees, which each time subsidized **GONG'**s travel.[19] At the time of these trips, **GONG** was employed by Company 3.

a. **GONG** received an invitation in April 2019 for a paid trip to participate in the "12th Nanjing International Exchange and Cooperation Conference for Chinese Overseas Students" in Nanjing, China, on May 8 and 9, 2019. According to the invitation, the conference would pay for **GONG'**s accommodations and provide a travel subsidy. According to DHS travel records, **GONG** traveled to Peking, China, on May 3, 2019, and returned to the United States on May 19, 2019, and **GONG** later exchanged emails with the conference organizers about

[18] According to **GONG'**s proposals, "gallium nitride devices are currently widely used in military fields such as base stations, radars, and electronic warfare," and will become more widely used in telecommunications infrastructure with the expansion of 5G wireless technology.

[19] Based on my review of **GONG'**s emails, **GONG** also received an invitation in September 2018 to attend the 2018 Zhejiang Hangzhou International Talent Exchange and Project Cooperation Conference in Hangzhou, China, which was originally scheduled for November 7 to 9, 2018. The trip was to be subsidized by the organizers. **GONG** initially indicated that he planned to attend, but the conference dates were later postponed, and **GONG** did not participate.

receiving a wire transfer into a Bank of China account held in **GONG**'s name.

b. According to my review of emails and DHS travel records,[20] **GONG** traveled to China again in September 2019 to present his application to the Xihu District 325 Talent Plan in person in Hangzhou, China.[21] According to a copy of the presentation deck **GONG** sent to the program organizers, his proposal again sought funding to develop and produce 16 bits 100-370 MSPS ADCs, and **GONG** again underscored the military applications of high-performance ADCs.

c. In a November 12, 2019 email to a talent plan recruiter, **GONG** expressed frustration about the lack of a response to his September 2019 in-person presentation regarding his high-performance ADC proposal in Hangzhou, China: "I took a risk (because I worked for [Company 3], an American military industry company) and thought I could do something for the country's high-end military integrated circuits."

53. In 2020, **GONG** applied to the "Maker World-Hangxiang Future 2020" Hangzhou Overseas High-Level Talent Innovation and Entrepreneurship Competition, once again seeking funding for his high-performance ADC project.

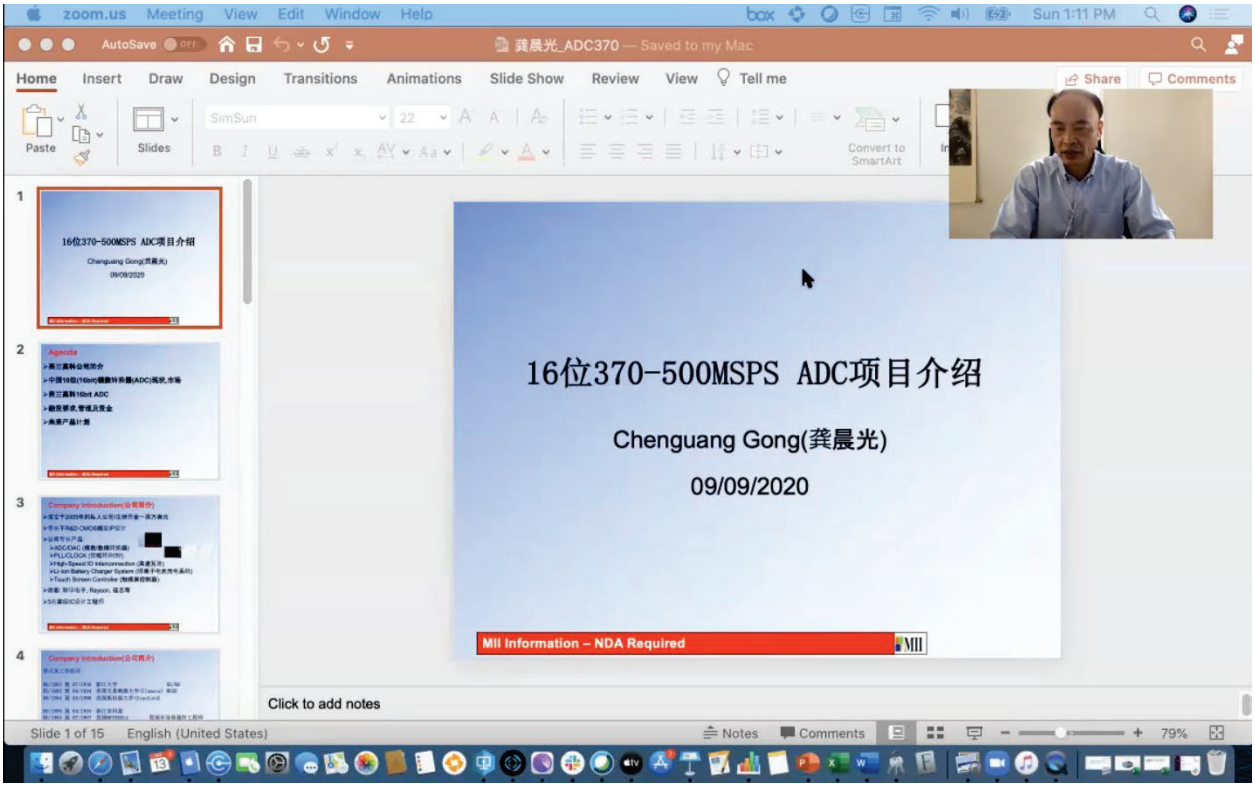
---

[20] The DHS travel records show that **GONG** traveled from San Francisco to Hong Kong on September 18, 2019, and returned from Hong Kong to San Francisco on September 23, 2019. Based on my review of **GONG**'s emails, **GONG** traveled onward from Hong Kong to Hangzhou, China.

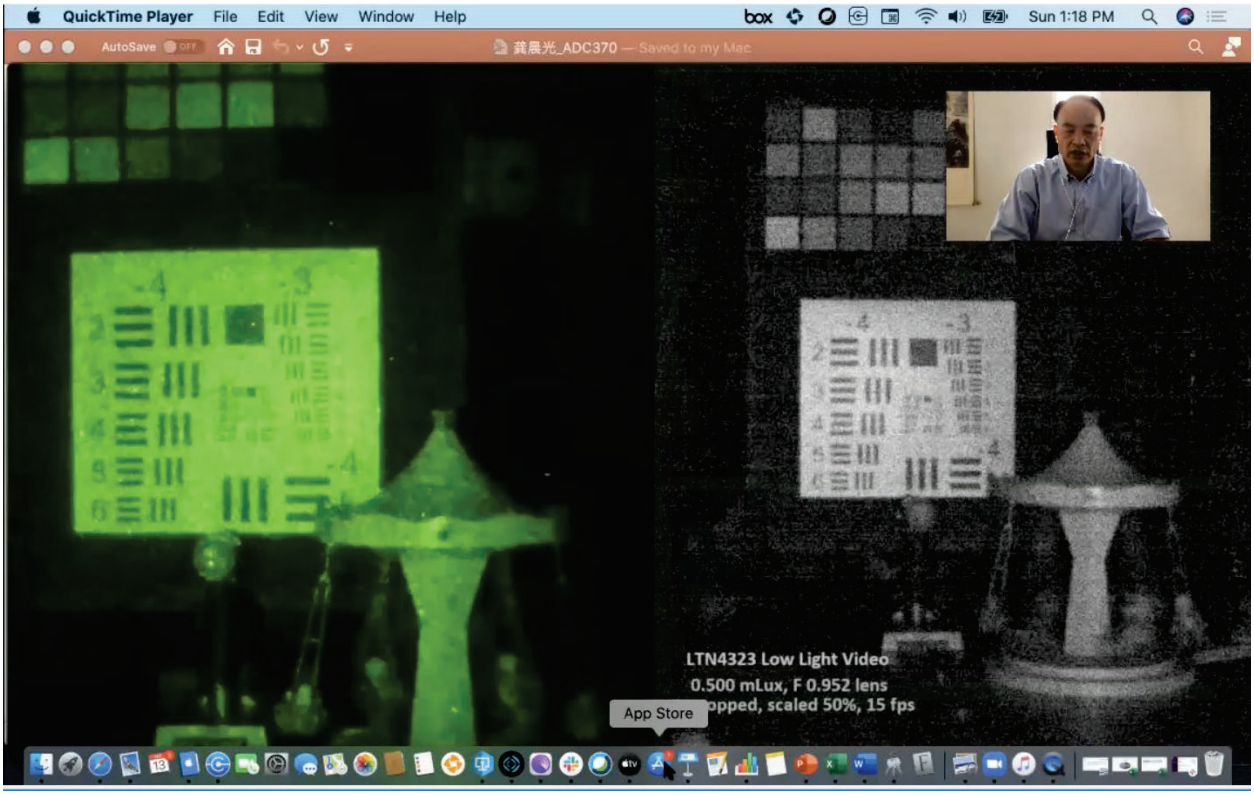
[21] On Augst 26, 2019, **GONG** sent a copy of his Chinese passport and his Company 3 employee ID card to a representative of the Xihu District Office of Talents.

a. On September 6, 2020, the "Organizing Committee" notified **GONG** via email that his project had been "officially recommended to enter the semi-finals of the competition," and that he would need to submit a video presentation explaining his project and to participate in a video conference via Zoom on September 24 or 25, 2020. **GONG** agreed.

b. **GONG** sent his pre-prepared video presentation to the competition organizers on September 13, 2020. In the image below, **GONG** can be seen explaining his 16-bit 370-500 MSPS ADC project proposal.



c. In another portion of the video, **GONG** can be seen explaining the functionality of a high-performance 4K resolution CMOS sensor. The model number of the sensor, LTN4323, is clearly visible in the bottom left portion of the image, and corresponds to a sensor developed by Company 3, where **GONG** had been employed until October 2019. In a copy of the presentation **GONG** sent to the competition organizers on October 3, 2020, **GONG** stated that his product extensions included a "low-light/night vision dual-use CMOS image sensor" for use in military night vision goggles and civilian applications.



d. On September 25, 2020, **GONG** received an email informing him that his project proposal had been "selected as a finalist," and **GONG** was asked to participate in an "online real-time project roadshow and to submit a "project roadshow"

PowerPoint presentation in advance of the "project defense" on October 28, 2020. According to my review of his emails, **GONG**'s selection as a semifinalist may have entitled him to a "winning bonus" of 20,000 RMB (approximately $2,800), but **GONG**'s project was not among the three projects selected for the grand final of the competition.[22]

e. On October 31, 2020, **GONG** submitted a substantially similar project proposal to an email address which, based on internet research, is listed as the point of contact for the Hangzhou Xihu West Lake Talent Plan.

54. **GONG** continued to seek funding from Chinese government programs through at least March 2022. For example, on March 13, 2022, **GONG** sent his project proposal to an email address with a @qq.com domain,[23] which, based on other emails, I believe is associated with the Shanghai Overseas Talent Plan.

55. When **GONG** was interviewed by the FBI on May 8 and 10, 2023, **GONG** acknowledged that he had heard of Chinese talent programs and may have received some invitations to participate

---

[22] On November 9, 2020, **GONG** provided remittance instructions to the Bank of China for a wire transfer to a Bank of China account held in **GONG**'s name, with an account number ending in x6684. In addition, in a January 5, 2021 email to the COO of the INNO-APAC Chuangtai Acceleration Workshop and Foreign Investment Network, **GONG** stated that although some organizations were interested in his project, "which could fill the gap in the country with specific strategic value," he did not "want to implement it yet because the support funds are not enough" to pay for one semiconductor photomask.

[23] Based on my training and experience, as well as my review of publicly available information, I know that the domain @qq.com is associated with the Chinese IT company Tencent, is and that QQ Mail is one of China's most popular free email platforms.

in talent programs in his Yahoo email account. **GONG** initially denied that he had ever submitted any talent plan applications, however. After being warned that the FBI would review his email account, **GONG** then admitted that he applied to talent programs before the COVID-19 pandemic but denied submitting any more recent applications, stated that he had never accepted any funding, and claimed that he did not offer to provide any technology that had military applications and that he had "no intention" to open his own company.

I. GONG Retained and Possessed Proprietary Documents Belonging to Several Prior Employers

56. Based on my review of **GONG**'s communications and his digital devices, **GONG** took and retained thousands of documents, stored on a variety of digital devices, that appear to belong to several of **GONG**'s former employers, including Company 2, Company 3, Company 4, and Company 5. Many of these documents bear confidentiality markings indicating their sensitive nature, including "Confidential," "Proprietary," "Confidential – Maximum Restrictions," "Strictly private and confidential," "Export Controlled," "ITAR Restricted," and "Distribution Statement C."[24]

57. Based on my review of the files and file types on **GONG**'s personal storage devices, his personal laptop, and his iPad, I believe that **GONG** also retained CAD files containing the technical designs and blueprints for integrated circuits or

[24] Based on my training and experience, I know that "Distribution Statement C" is a U.S. Department of Defense ("DoD") marking that means that distribution of the document is only authorized to U.S. Government Executive Branch departments and agencies and DoD Components, as well as their contractors if such distribution is in furtherance of that contractual purpose.

other products. Many of these CAD files are contained within .bz2, .gz, and .tar archive files. Based on my analysis of the file paths and file names, it appears that many of these files relate to products developed by several of **GONG**'s former employers, including Company 2 and Company 5.

58. In addition, based on my review of these files, **GONG** appears to have retained and continued to possess hundreds of files that relate to high-performance ADCs and CMOS sensors, which, based on my knowledge of this investigation, I know are product types that **GONG** included in his proposals to various Chinese Talent Programs between approximately 2014 and 2022 and relate to his work at Company 2, Company 3, and Company 5.

J. GONG's Travel History and Plans

59. Based on my review of DHS travel records, **GONG** often traveled to China before the onset of the COVID-19 pandemic. In addition to traveling to China in May and September 2019 -- each time at the invitation of PRC Talent Programs, as described above -- **GONG** traveled to China in December 2010, from December 2011 to January 2012, from November to December 2013, and from April to May 2017.

60. Based on my review of **GONG's** email communications, I know that **GONG** applied for a visa to travel to China in 2023. Based on my conversations with **GONG**, I believe that **GONG** intends to travel to China in February 2024, around the time of Chinese New Year, which falls this year on February 10, 2024.

V. CONCLUSION

61. For all of the reasons described above, there is probable cause to believe that **GONG** has committed a violation of Title 18, United States Code, Section 1832(a)(1) (Theft of Trade Secrets).

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 5th day of February, 2024.

HON. BRIANNA F. MIRCHEFF
UNITED STATES MAGISTRATE JUDGE