

FILED

Feb 04 2025

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

CRIMINAL COVER SHEET

Instructions: Effective November 1, 2016, this Criminal Cover Sheet must be completed and submitted, along with the Defendant Information Form, for each new criminal case.

CASE NAME:

USA v. Linwei Ding

CASE NUMBER:

CR 24-cr-00141 VC

Is This Case Under Seal?

Yes

No ☒

Total Number of Defendants:

1 ☒

2-7

8 or more

Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326?

Yes

No ☒

Venue (Per Crim. L.R. 18-1):

SF ☒

OAK

SJ

Is this a potential high-cost case?

Yes

No ☒

Is any defendant charged with a death-penalty-eligible crime?

Yes

No ☒

Is this a RICO Act gang case?

Yes

No ☒

Assigned AUSA

(Lead Attorney): Molly Priedeman & Casey Boome

Date Submitted: 2/4/2025

Comments:

RESET FORM

SAVE PDF

United States District Court
FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED

Feb 04 2025

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

LINWEI DING, a.k.a. Leon Ding,

DEFENDANT(S).

SUPERSEDING INDICTMENT

18 U.S.C. § 1832(a)(1), (2) and (3) – Theft of Trade Secrets;
18 U.S.C § 1831(a)(1).(2), and (3) – Economic Espionage
18 U.S.C. §§ 981(a)(1)(C), 1834, and 2323, and 28 U.S.C. §
2461(c) – Criminal Forfeiture.

A true bill.

/s/ Foreperson of the Grand Jury

Foreman

Filed in open court this 4th ____ day of
February 2025

Elaine Karling
Clerk

Laurel Beeler

Bail, \$ _____ no process

Hon. Laurel Beeler, U.S. Magistrate Judge

FILED

Feb 04 2025

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,	)	CASE NO. 24-cr-00141 VC
Plaintiff,	)	<u>VIOLATIONS:</u>
v.	)	18 U.S.C. § 1832(a)(1), (2) and (3) – Theft of Trade
LINWEI DING, a.k.a. Leon Ding,	)	Secrets;
Defendant.	)	18 U.S.C § 1831(a)(1).(2), and (3) – Economic
	)	Espionage
	)	18 U.S.C. §§ 981(a)(1)(C), 1834, and 2323, and 28
	)	U.S.C. § 2461(c) – Criminal Forfeiture.
	)	SAN FRANCISCO VENUE

SUPERSEDING INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Superseding Indictment:

Background on Google, LLC

1. Google, LLC (“Google”) was a technology company headquartered in Mountain View, California. Google was a subsidiary of Alphabet Inc., the world’s third-largest technology company by revenue with a market capitalization of approximately \$1.75 trillion. Google’s products and services included Google Search, Google Maps, YouTube, Android, Chrome, Google Play, and Google Cloud, among others. Google was integrating artificial intelligence (“AI”) and machine learning (“ML”) into its

SUPERSEDING INDICTMENT

1 products and services and conducting research to develop next generation AI technology. Among
2 Google's AI initiatives was the development of supercomputing data centers capable of training and
3 serving state of the art proprietary AI models, conducting AI research, and integrating AI into Google's
4 core products and services. Google Cloud also leased part of its supercomputing data centers to other
5 companies who used the infrastructure to train their own AI models and host AI applications.

6 2. Large AI models and the AI applications they supported could make predictions, find
7 patterns, classify data, understand nuanced language, and generate intelligent responses to prompts,
8 tasks, or queries. To achieve this capability, large AI models were created through a computation-
9 intensive process called "training," which involved processing an enormous volume of text, code,
10 images, video, and other data.

11 3. Google offered a range of products designed to accelerate ML tasks, including Graphics
12 Processing Unit ("GPU") and Tensor Processing Unit ("TPU") based products. GPUs and TPUs were
13 advanced computer chips with the extraordinary processing power required to train and serve large AI
14 models. Google's customers could access and use TPUs and GPUs for their own machine learning
15 workloads via Google Cloud. Google also used the chips for its own purposes, for example to train and
16 serve its own AI models, such as Gemini.

17 4. TPUs were developed in-house by Google to accelerate deep learning workloads. Deep
18 learning uses neural networks, a type of AI model trained to make decisions in a manner similar to the
19 human brain. Google built complex systems that combined thousands of interconnected TPU chips to
20 achieve high performance and support large AI models. Google designed its TPUs to contain four
21 primary components: (1) TensorCore; (2) BarnaCore/SparseCore; (3) high bandwidth memory (HBM)
22 access interface; and (4) inter-chip-interconnect (ICI). The TensorCore component was the main
23 processing component of the chip and was responsible for most of the acceleration. The
24 BarnaCore/SparseCore component was responsible for sparse computation, which provided substantial
25 acceleration on certain types of deep learning workloads. The HBM access provided a way for the chip
26 to access memory. ICI was a Google-developed technology that allowed TPU chips to communicate.
27 Google created custom designed machines to house multiple TPUs and to scale the processing power for
28 ML workloads. Each TPU machine had multiple components designed to optimize value, cost, and

1 efficiency. Multiple TPU machines were installed on a rack, and machines across multiple racks were
2 then connected. This large-scale proprietary system allowed Google to create a supercomputer and
3 accelerate ML tasks at scale. The hardware infrastructure for Google's TPUs was managed by several
4 layers of software. Google used custom designed software to manage the hardware and resources within
5 a TPU, to facilitate communication between TPUs, and to allocate and manage collections of
6 interconnected TPUs to complete different workloads.

7 5. GPUs were accelerators that could be also used for machine learning. Google purchased
8 the GPUs used in its data centers from another technology company. Google designed custom machines
9 intended to hold multiple GPUs, as a well as a system designed to connect thousands of GPUs and to
10 provide the necessary power, cooling, and networking for high-performance computing. Google's GPU
11 hardware infrastructure was managed by several layers of software. Google used custom designed
12 software to facilitate communication between GPUs and to allocate and manage collections of
13 interconnected GPUs.

14 6. To enhance the functions of its GPU products, Google used a custom designed
15 SmartNIC, a type of network interface card. A SmartNIC was a hardware device that offloaded
16 networking functions from a server's Central Processing Unit (CPU). Google's SmartNIC incorporated
17 a proprietary chip component designed to deliver low-latency and high-bandwidth transfers of data over
18 large-scale networks. Google also developed software and used its custom designed SmartNIC to
19 enhance its high performance and cloud networking products.

20 7. The hardware infrastructure in Google's network of data centers was managed by several
21 layers of software (the "software platform"). The software platform provided instructions, in the form
22 of code, which communicated tasks to the hardware infrastructure for execution. One component of the
23 software platform was the Cluster Management System ("CMS"), which functioned as the "brain" of
24 Google's supercomputing data centers in that the CMS organized, prioritized, and assigned tasks to the
25 hardware infrastructure, allowing the hardware to function efficiently when executing machine learning
26 workloads or hosting AI applications.

27 Google's Proprietary Information Protection Policies

28 8. Google took reasonable measures to safeguard its proprietary technology, information,

1 and trade secrets. For instance, Google secured its physical space by deploying campus-wide security
2 guards and installing cameras on most building entry points. Google restricted access to its buildings by
3 requiring employees to badge in at front entrances. Certain floors or areas within buildings were further
4 restricted to a subset of employees by badge access. Advance registration was required for guests, and
5 Google employees were required to escort their guests at all times.

6 9. Google also took measures to secure its network. One method was a data loss prevention
7 system that monitored and logged certain data transfers to and from Google's network. Google also
8 required each device to be uniquely identified and authenticated before accessing the Google corporate
9 network. All Google employees were required to use two-factor authentication for their work-related
10 Google accounts. Employee activity on Google's network was logged, including file transfers to
11 platforms such as Google Drive or DropBox.

12 10. Google collected physical and network access information, including badge access times
13 and locations, Internet Protocol (IP) addresses for employee logins, and two-factor authentication logs,
14 and gathered this information in a database to analyze potential risks. This data was regularly assessed
15 both by automated tools and human analysts to detect potential malicious activity. For example, if a
16 Google employee's account were used to access the network through an IP address registered in a
17 different location from a door access badge-in for the same employee, an "Impossible Location Signal"
18 would be generated, and Google's security team would be notified. Google employees were instructed
19 to report remote work from foreign locations, and Google automatically limited the network access of
20 employees traveling to certain countries, such as the People's Republic of China (PRC), the Democratic
21 People's Republic of Korea (DPRK), and Iran.

22 11. Within the Google network, access to certain sensitive information, including the trade
23 secrets identified below in Trade Secret Categories One through Seven, was further restricted to a subset
24 of employees whose job duties related to the subject matter.

25 12. Every Google employee was required to sign an Employment Agreement through which
26 the employee agreed:

- 27 a) To hold all Google Confidential Information, which included Google trade
28 secrets, "in strict confidence;"

- b) Not to use Google Confidential Information “for any purpose other than for the benefit of Google in the scope of [their] employment;”
- c) Not to “retain any documents or materials or copies thereof containing any Google Confidential Information” upon termination from Google; and
- d) Not to engage in other employment or business activity that “directly relates to the business in which Google is now involved, becomes involved, or has plans to become involved,” or “otherwise conflicts with Google’s business interest.”

13. Every new Google employee was required to sign Google’s Code of Conduct, which stated, in part, that every Google employee must “take steps to keep our trade secrets and other confidential intellectual property secret.” Additional supplementary security training was often provided for employees working on sensitive technology projects.

14. All employees were trained on the importance of protecting Google’s intellectual property. For instance, Google employees were required to complete “Privacy and Information Security” training while onboarding with Google and periodically thereafter. This training included modules about the importance of protecting Google’s trade secrets.

Linwei DING’s Employment with Google

15. Google hired Linwei DING as a software engineer in 2019. DING signed Google’s Employment Agreement on February 20, 2019, and began working for Google on May 13, 2019. The following day, May 14, 2019, DING signed Google’s Code of Conduct.

16. The focus of DING’s work was the software platform deployed in Google’s network of supercomputing data centers. DING’s job responsibilities included development of software that allowed GPUs to function efficiently for machine learning, AI applications, or other purposes required by Google or Google Cloud clients. Due to DING’s job responsibilities, he was authorized to access Google Confidential Information related to Google’s supercomputing data centers, including the hardware infrastructure, the software platform, and the AI models and applications they supported.

Without Informing Google, DING Affiliated with PRC-Based Companies in the AI Industry While Secretly Exfiltrating Google’s Trade Secrets and Other Confidential Information

17. DING began uploading Google Confidential Information from Google’s network into a

1 personal Google Cloud account (“DING Account 1”) on May 21, 2022, and continued periodic uploads
2 until May 2, 2023. In total, DING uploaded more than 1,000 unique files containing Google
3 Confidential Information, including the trade secrets alleged in Trade Secret Categories One through
4 Seven. DING exfiltrated these files by copying data from the Google source files into the Apple Notes
5 application on his Google-issued MacBook laptop. DING then converted the Apple Notes into PDF
6 files and uploaded them from the Google network into DING Account 1. This method helped DING
7 evade immediate detection by Google.

8 18. Beginning on or about June 13, 2022, less than one month after DING’s unauthorized and
9 secret upload activity started, DING received several emails from the Chief Executive Officer (CEO) of
10 Beijing Rongshu Lianzhi Technology Co., Ltd. (“Rongshu”), an early-stage technology company based
11 in the PRC. The emails indicated that the CEO had offered DING the position of Chief Technology
12 Officer (CTO), with a monthly salary of 100,000 RMB (approximately \$14,800 in June 2022), plus an
13 annual bonus and company stock. Rongshu’s business objectives included the development of
14 acceleration software designed for ML on GPU chips. Rongshu touted its development of AI federated
15 learning platforms, which were systems for training AI models using decentralized data sources for
16 greater data privacy.

17 19. DING traveled to the PRC on October 29, 2022, and remained there until March 25,
18 2023. Beginning in or about December 2022, while in the PRC, DING participated in investor meetings
19 to raise capital for Rongshu. Rongshu’s CEO informed potential investors during an April 17, 2023
20 meeting that DING was Rongshu’s CTO.

21 20. DING never informed Google about his affiliation with Rongshu.

22 21. By no later than May 30, 2023, DING had founded Shanghai Zhisuan Technology Co.
23 Ltd. (“Zhisuan”) and was acting as its CEO. Zhisuan was a PRC-based startup company that proposed
24 to develop a Cluster Management System (CMS) that could accelerate ML workloads, including training
25 large AI models powered by supercomputing chips.

26 22. On or about May 30, 2023, DING applied on behalf of Zhisuan to a PRC-based startup
27 incubation program known as MiraclePlus. Zhisuan was accepted to the program, and on or about
28 November 20, 2023, DING signed an agreement granting a seven percent ownership interest in Zhisuan

1 to a MiraclePlus affiliated company in exchange for investment capital for Zhisuan. DING traveled to
2 the PRC and pitched Zhisuan to investors at the MiraclePlus venture capital investor conference in
3 Beijing on or about November 24, 2023. A Zhisuan document, which DING circulated on November
4 29, 2023 to the members of a Zhisuan WeChat group, stated in part, “we have experience with Google’s
5 ten-thousand-card computational power platform; we just need to replicate and upgrade it – and then
6 further develop a computational power platform suited to China’s national conditions.”

7 23. DING never informed Google about his affiliation with Zhisuan.

8 *DING Intended to Benefit the PRC Government and Instrumentalities*

9 24. On or about November 17, 2023, Ding circulated a PowerPoint presentation to other
10 Zhisuan employees citing PRC national policies encouraging the development of the domestic AI
11 industry. The presentation, which was circulated to potential Zhisuan investors, pointed to the State
12 Council’s 2017 “Notice on the Development of the New Generation of Artificial Intelligence,” which
13 called for the development of high-performance computing infrastructure. The PRC State Council is the
14 chief administrative authority in the PRC, and it functions as the executive branch of the central
15 government. The presentation also cited a policy document titled “Interim Measures for the
16 Management of Generative AI Services,” which was published and sponsored by seven PRC
17 government agencies, including the Cyberspace Administration of China (CAC). The CAC, also known
18 as the State Internet Information Office, is a PRC government agency responsible for regulating and
19 managing the PRC’s internet and cyberspace. The presentation quoted Article 6 of the Interim Measures
20 document, which seeks to “Encourage independent innovation in basic technologies such as generative
21 ratification intelligence algorithms, chips, and supporting software platforms”

22 25. In or about December 2023, Ding created a PowerPoint presentation containing an
23 application to a PRC talent program based in Shanghai. Talent programs are sponsored by the PRC to
24 incentivize individuals engaged in research and development outside of the PRC to transmit that
25 knowledge and research to the PRC in exchange for salaries, research funds, lab space, or other
26 incentives. Ding’s application stated that his product “will help China to have computing power
27 infrastructure capabilities that are on par with the international level.”

28 26. An internal Zhisuan memo dated December 14, 2023, indicates that Zhisuan intended to

1 market itself to and provide services to multiple PRC-controlled entities, including government agencies
2 and universities.

3 Google Detects DING's Exfiltration of Google Confidential Information

4 27. On or about December 2, 2023, DING uploaded additional files from the Google network
5 to another personal Google Drive account controlled by DING ("DING Account 2") while DING was in
6 the PRC. On December 8, 2023, after Google detected this activity, DING told a Google investigator
7 that he had uploaded the files to his personal account to use the information as evidence of the work that
8 he had conducted at Google. DING assured the investigator that he had no intention of leaving Google.
9 DING signed a Self-Deletion Affidavit (SDA), dated December 8, 2023, that stated in part:

10 I have searched my personal possessions, including all devices, accounts,
11 and documents in my custody or control for any non-public information
12 originating from my job at Google . . . I have permanently deleted and/or
destroyed all copies of such information . . . As a result, I no longer have
access to such information outside the scope of my employment.

13 DING did not tell Google that he had previously uploaded more than 1,000 confidential files, including
14 Google trade secrets, between May 2022 and May 2023, nor that he was affiliated with Rongshu and
15 Zhisuan.

16 28. Unbeknownst to Google, on December 14, 2023, DING booked a one-way ticket from
17 San Francisco to Beijing on a China Southern Airlines flight scheduled to depart on January 7, 2024.

18 29. On December 26, 2023, DING sent an email to his manager resigning from Google and
19 stating that his last day would be January 5, 2024.

20 30. On or about December 29, 2023, Google learned that DING had presented as the CEO of
21 Zhisuan at the MiraclePlus investor conference in Beijing on November 24, 2023. Google then
22 suspended DING's network access and remotely locked his Google laptop. Google searched DING's
23 network activity history and discovered DING's unauthorized uploads from May 2022 through May
24 2023.

25 31. Also on or about December 29, 2023, Google investigators reviewed surveillance footage
26 from the entrance to the Google building where DING worked. Google observed another employee scan
27 DING's access badge on December 4, 6, and 8, 2023, making it appear as though DING had been
28 working from his U.S. Google office on those dates when in fact DING was in the PRC. The employee

1 who scanned DING's badge stated to Google that DING had asked him/her to periodically scan his
2 badge while he was traveling to make it appear as though he was working from his office.

3 32. On January 4, 2024, Google security personnel retrieved DING's Google laptop and
4 mobile device from DING's residence.

5 FBI Investigation of DING

6 33. On January 6, 2024, the Federal Bureau of Investigation (FBI) executed a search warrant
7 at DING's residence, seizing his electronic devices and other evidence.

8 34. On January 13, 2024, the FBI executed an additional search warrant for the contents of
9 DING Accounts 1 and 2. DING Account 1 contained more than 1,000 unique files containing Google
10 Confidential Information, including the trade secrets in Trade Secret Categories One through Seven.

11 General Description of Stolen Trade Secrets

12 35. In general, the trade secrets described in Trade Secret Categories One through Seven
13 pertain to the hardware infrastructure and software platform that allowed Google's supercomputing data
14 centers to train and serve large AI models. The trade secrets contain detailed information about the
15 architecture and functionality of TPU chips and systems and GPU systems, the software that allowed the
16 chips to communicate and execute tasks, and the software that orchestrated thousands of chips into a
17 supercomputer capable of training and executing cutting-edge AI workloads. The trade secrets also
18 pertain to Google's custom designed SmartNIC and related software.

19 **Trade Secret Category 1:**

20 36. Instruction sets, protocols, internal specifications, and implementation level details
21 related to the four primary components of Google's custom designed TPU chip: (1) TensorCore; (2)
22 BarnaCore/SparseCore; (3) high bandwidth memory (HBM) access interface; and (4) inter-chip-
23 interconnect (ICI).

24 **Trade Secret Category 2:**

25 37. Documents including details of the design, performance, and operation of Google's
26 custom designed TPU chips, TPU machines, and TPU systems.

27 **Trade Secret Category 3:**

28 38. Design documents for Google's TPU software that managed the hardware and resources

1 within a TPU, facilitated communication between TPUs, and allocated and managed collections of
2 interconnected TPUs to different workloads.

3 **Trade Secret Category 4:**

4 39. Documents including details of the design, performance, and operation of Google's
5 custom GPU machines and GPU systems.

6 **Trade Secret Category 5:**

7 40. Design documents for Google's GPU software that facilitated communication between
8 GPUs and allocated and managed collections of interconnected GPUs to different workloads.

9 **Trade Secret Category 6:**

10 41. Design specifications to implement Google's proprietary chip component designed to
11 deliver low-latency and high-bandwidth transfers of data over large-scale networks on Google's
12 SmartNIC.

13 **Trade Secret Category 7:**

14 42. Design documents for Google's software to implement its high performance and cloud
15 networking on its SmartNIC.

16 COUNTS ONE THROUGH SEVEN: (18 U.S.C. § 1832(a)(1), (2), & (3) – Theft of Trade Secrets)

17 43. The allegations contained in Paragraphs 1 through 42 are realleged and incorporated as if
18 fully set forth herein.

19 44. On or about the dates set forth in the separate counts below, in the Northern District of
20 California and elsewhere, the defendant,

21 LINWEI DING,

22 intending to convert a trade secret that was related to a product and service used in and intended for use
23 in interstate and foreign commerce to the economic benefit of anyone other than the owner of that trade
24 secret, and knowing and intending that the offense would injure the owner of that trade secret, as
25 specifically alleged in each of Counts One through Seven below:

- 26 a. knowingly stole, and without authorization appropriated, took, carried away, concealed,
27 and by fraud, artifice, and deception obtained trade secrets belonging to Google;
28 b. knowingly and without authorization copied, duplicated, sketched, drew, downloaded,

uploaded, altered, photocopied, replicated, transmitted, delivered, sent, communicated, and conveyed trade secrets belonging to Google; and

c. knowingly and without authorization received, bought, and possessed trade secrets belonging to Google, and attempted to do so, knowing the same to have been stolen and appropriated, obtained, and converted without authorization:

Count	Date	Item Description
One	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category One
Two	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Two
Three	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Three
Four	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Four
Five	On or about and between June 3, 2022 and April 17, 2023	Trade Secret Category Five
Six	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Six
Seven	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Seven

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

COUNTS EIGHT THROUGH FOURTEEN: (18 U.S.C. § 1831(a)(1), (2), & (3) – Economic Espionage

45. The allegations contained in Paragraphs 1 through 42 are realleged and incorporated as if fully set forth herein.

46. On or about the dates set forth in the separate counts below, in the Northern District of California and elsewhere, the defendant,

LINWEI DING,

intending or knowing that the offense would benefit any foreign government, foreign instrumentality, or foreign agent:

- a. knowingly stole, and without authorization appropriated, took, carried away, concealed, and by fraud, artifice, and deception obtained trade secrets alleged in each of Counts Eight through Fourteen below belonging to Google;
- b. knowingly and without authorization copied, duplicated, sketched, drew, downloaded, uploaded, altered, photocopied, replicated, transmitted, delivered, sent, communicated, and conveyed trade secrets alleged in each of Counts Eight through Fourteen below belonging to Google; and
- c. knowingly and without authorization received, bought, and possessed trade secrets alleged in each of Counts Eight through Fourteen below belonging to Google, and attempted to do so, knowing the same to have been stolen and appropriated, obtained, and converted without authorization:

Count	Date	Item Description
Eight	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category One
Nine	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Two

Ten	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Three
Eleven	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Four
Twelve	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Five
Thirteen	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Six
Fourteen	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Seven

Each in violation of Title 18, United States Code, Sections 1831(a)(1), (2), and (3).

FORFEITURE ALLEGATION: (18 U.S.C. §§ 981(a)(1)(C), 1834, and 2323, and 28 U.S.C. § 2461(c) – Proceeds and Property Involved in Theft of Trade Secrets)

47. The factual allegations contained in Paragraphs 1 through 46 of this Superseding Indictment are realleged and by this reference fully incorporated herein for the purposes of alleging forfeiture. Upon conviction of any of those offenses, the defendant,

LINWEI DING,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 1834, and 2323, and Title 28, United States Code, Section 2461(c), any property used, or intended to be used, in any manner or part to commit or facilitate the commission of the offenses, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, including, but not limited to, a sum of money equal to the total amount of proceeds defendant obtained or derived, directly or indirectly, from the violations, or the value of the property used to commit or to

1 facilitate the commission of said violations.

2 48. If any of the property described above, as a result of any act or omission of the defendant:

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

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

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

6 d. has been substantially diminished in value; or

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

8 the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21,
9 United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 2323(b).

10 All pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 1834, and 2323, Title 28,
11 United States Code, Section 2461(c), and Federal Rule of Criminal Procedure 32.2.

12
13 DATED: February 4, 2025

A TRUE BILL.

14 */s/ Foreperson*

15 _____
16 FOREPERSON
San Francisco, California

17 ISMAIL J. RAMSEY
18 United States Attorney

19
20 */s/* _____
21 CASEY BOOME
22 MOLLY K. PRIEDEMAN
Assistant United States Attorneys

23 STEPHEN MARZEN
24 YIFEI ZHENG
Trial Attorneys
25 National Security Division
26
27
28

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT
 BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT
☒ SUPERSEDING
OFFENSE CHARGED

Counts 1-7: 18 U.S.C. § 1832(a)(1), (2), & 3) - Theft of Trade Secrets

☐ Petty☐ Minor

Counts 8-14: 18 U.S.C. § 1831(a) - Economic Espionage

☐ Misdemeanor☒ Felony

PENALTY: 18 U.S.C. § 1832(a)(1), (2), & 3): 10 years imprisonment, \$250,000 fine, \$100 special assessment, 3 years supervised release

18 U.S.C. § 1831(a): 15 years imprisonment, \$250,000 fine, \$100 special assessment, 3 years supervised release

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT - U.S.

▶ Linwei Ding

DISTRICT COURT NUMBER

24-cr-00141 VC

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

FBI

☐ person is awaiting trial in another Federal or State Court, give name of court☐ this person/proceeding is transferred from another district per (circle one) FRCrP 20, 21, or 40. Show District☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:☐ U.S. ATTORNEY ☐ DEFENSESHOW
DOCKET NO.☐ this prosecution relates to a pending case involving this same defendantMAGISTRATE
CASE NO.☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person

Furnishing Information on this form Ismail Ramsey

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S.

Attorney (if assigned)

Molly Priedeman & Casey Boon

IS NOT IN CUSTODY

Has not been arrested, pending outcome this proceeding.

1) ☐ If not detained give date any prior summons was served on above charges ▶2) ☐ Is a Fugitive3) ☒ Is on Bail or Release from (show District)**IS IN CUSTODY**4) ☐ On this charge5) ☐ On another conviction☐ Federal ☐ State6) ☐ Awaiting trial on other charges

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

Has detainer been filed? ☐ Yes ☐ No

If "Yes" give date filed

DATE OF ARREST ▶

Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY ▶

Month/Day/Year

☐ This report amends AO 257 previously submitted**ADDITIONAL INFORMATION OR COMMENTS****PROCESS:**☐ SUMMONS ☒ NO PROCESS* ☐ WARRANT

Bail Amount: _____

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address:

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

Date/Time: _____ Before Judge: _____

Comments: