

FILED

2014 AUG 14 PM 1:43

CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES

BY: _____

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2014 Grand Jury

CR 14 00131

UNITED STATES OF AMERICA,

SA CR No. 14-

Plaintiff,

I N D I C T M E N T

v.

SU BIN,
aka "Stephen Su,"
aka "Stephen Subin,"
aka "Steven Subin,"

[18 U.S.C. §§ 1030(a)(2)(C),
(c)(2)(B)(i)-(iii), §§ 1030(a)(4),
(c)(3)(A), §§ 1030(b),
(c)(2)(B)(i)-(iii), (c)(3)(A):
Unauthorized Computer Access; 18
U.S.C. § 371: Conspiracy; 18
U.S.C. § 1832(a)(5): Conspiracy to
Commit Theft of Trade Secrets; 18
U.S.C. § 2(a): Aiding and
Abetting]

Defendant.

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

At all times relevant to this Indictment:

1. Defendant SU BIN, also known as ("aka") "Stephen Su," aka
"Stephen Subin," aka "Steven Subin" ("defendant SU"), was a citizen
of the People's Republic of China (hereinafter "China").

2. Unindicted Co-conspirator 1 was a citizen of China and
resided in China.

1 3. Unindicted Co-conspirator 2 was a citizen of China and
2 resided in China.

3 4. Defendant SU, Unindicted Co-conspirator 1, and Unindicted
4 Co-conspirator 2 e-mailed each other both in Chinese and English.

5 5. Between in or about October 2008 and in or about May 2014,
6 defendant SU traveled to the United States multiple times, including
7 specifically:

8 a. between on or about January 13, 2010, and on or about
9 January 24, 2010;

10 b. between on or about February 11, 2010, and on or about
11 February 21, 2010;

12 c. between on or about May 26, 2010, and on or about June
13 8, 2010;

14 d. between on or about June 20, 2010, and on or about
15 June 27, 2010;

16 e. between on or about September 8, 2010, and on or about
17 September 11, 2010;

18 f. between on or about December 18, 2010, and on or about
19 December 28, 2010;

20 g. between on or about June 30, 2011, and on or about
21 June 22, 2011;

22 h. between on or about September 28, 2012, and on or
23 about October 3, 2012;

24 i. between in or about October 2012 and on or about
25 November 3, 2012; and,

26 j. between on or about December 31, 2012, and on or about
27 January 2, 2013.

28

1 6. The Boeing Company (hereinafter "Boeing"), headquartered in
2 Chicago, Illinois, was a company with offices throughout the United
3 States that developed and sold military and commercial aircraft,
4 among other goods; technologies; and related support services.
5 Boeing had facilities in many locations, including Seal Beach and
6 Long Beach, California. The goods and technologies Boeing sold to
7 its customers were sold and shipped, and were intended to be sold and
8 shipped, in interstate and foreign commerce.

9 7. One of the aircraft models that Boeing manufactured was the
10 C-17 military transport aircraft ("the C-17"), including variants of
11 the C-17, which was manufactured in Los Angeles County, California,
12 located in the Central District of California. The C-17 was
13 developed over multiple years and produced by Boeing and its
14 predecessor and subcontractors pursuant to contracts with the United
15 States Air Force at a cost of billions of dollars. Developing and
16 producing the C-17 required the use of trade secrets and the use of
17 export-controlled technical data. Boeing maintained multiple
18 computer servers containing files relating to the C-17, including
19 servers in Orange County, California, containing detailed files
20 necessary to make the component parts of the C-17.

21 8. The F-35 "Lightning" was a fifth-generation fighter jet
22 aircraft capable of supersonic speed and equipped with "stealth"
23 capabilities that allowed it to evade radar ("the F-35"). The F-35
24 was developed over multiple years by multiple companies performing
25 contracts with the United States Department of Defense ("defense
26 contractors") in the United States and other countries at a cost of
27 billions of dollars. Developing and producing the F-35 required the
28 use of those defense contractors' trade secrets and the use of

1 export-controlled technical data. Variants of the aircraft were made
2 for different services of different countries' armed forces.

3 9. The F-22 "Raptor" was a fifth-generation fighter jet
4 aircraft capable of supersonic speed and equipped with "stealth"
5 capabilities that allowed it to evade radar ("the F-22"). The F-22
6 was developed over multiple years by defense contractors in the
7 United States at a cost of billions of dollars. Developing and
8 producing the F-22 required the use of those defense contractors'
9 trade secrets and the use of export-controlled technical data.

10 10. In developing, testing, producing, and maintaining the C-
11 17, F-35, F-22, and other military technology, defense contractors
12 generated documents, files, and information, including computer
13 files, that contained trade secrets that were the product of research
14 and development and that were proprietary information belonging to
15 those defense contractors. Those trade secrets related to various
16 facets of the aircraft, its development, design, testing, production,
17 components, and ongoing maintenance. Those trade secrets also
18 related to the ways in which those defense contractors competed to
19 win government contracts to build and service military aircraft and
20 other military technology. Those trade secrets existed in a single
21 document and record at times, and at other times as compilations and
22 collections of documents and files that related to the entire
23 aircraft and to portions or components of the aircraft.

24 11. The Arms Export Control Act, Title 22, United States Code,
25 Section 2778 ("AECA"), authorized the President of the United States
26 to control the export of "defense articles" and "technical data"
27 related to such defense articles by designating those items and that
28

1 data as defense articles and by promulgating regulations for the
2 import and export of such articles and data.

3 12. Defense articles and technical data subject to such
4 licensing requirements were designated on the United States Munitions
5 List ("USML"). Those designations were made by the United States
6 Department of State ("Department of State") with the concurrence of
7 the United States Department of Defense ("Department of Defense").
8 (22 U.S.C. § 2778(a)(1); 22 C.F.R. § 120.2.)

9 13. Category VIII of the USML, among others, included aircraft
10 and aircraft-related equipment. (22 C.F.R. § 121.1.)

11 14. The AECA and its attendant regulations, the International
12 Traffic in Arms Regulations, Title 22, Code of Federal Regulations,
13 Parts 120-130 ("ITAR"), required a person to apply for and obtain an
14 export license from the Directorate of Defense Trade Controls
15 ("DDTC") of the Department of State before exporting from the United
16 States defense articles or related technical data by any means,
17 including by disclosing technical data on the USML to a foreign
18 person. (22 U.S.C. § 2778(b)(2); 22 C.F.R. §§ 120.1, 120.10,
19 120.17.)

20 15. At no time did defendant SU apply for, receive, or possess
21 a license to export defense articles or technical data from the
22 United States.

23 16. The factual allegations in paragraphs 1 through 15 are
24 incorporated in all counts of this Indictment by reference and are
25 re-alleged as though fully set forth therein.

26 17. In the course of their conduct, defendant SU, Unindicted
27 Co-conspirator 1, and Unindicted Co-conspirator 2 committed the
28 following acts on or about the following dates:

1 18. On October 23, 2008, Unindicted Co-conspirator 1 wrote an
2 e-mail to another person asking: "Hey there, Do you sell the
3 Poisonivy Program? How much do you sell it for? i wish to buy one
4 which can not be detect [sic] and killed by the Anti-Virus software."

5 19. On July 22, 2009, defendant SU forwarded an e-mail that he
6 had received from Unindicted Co-conspirator 1. Attached to that
7 e-mail was a draft contract for the purchase of a "System for
8 Unidirectional Secure Delivery of Files Over the Internet," from an
9 identified company located in China that advertised its expertise in
10 the fields of computer network attack and defense and communication
11 security.

12 20. On July 23, 2009, defendant SU caused one of his company's
13 employees to e-mail defendant SU and Unindicted Co-conspirator 1 a
14 signed version of the contract described in paragraph 19 that
15 defendant SU had executed on behalf of his company.

16 21. On December 14, 2009, defendant SU sent an e-mail to
17 Unindicted Co-conspirator 1 with a subject line of "Target."
18 Attached to the e-mail was a file containing the names and positions
19 of U.S. executives as well as a website and telephone number.

20 22. On December 17, 2009, defendant SU sent an e-mail to
21 Unindicted Co-conspirator 1 and copied Unindicted Co-conspirator 2
22 with a subject line of "RE: Target." In that e-mail defendant SU
23 identified e-mail addresses, a website, and four individuals
24 associated with a European company.

25 23. On January 13, 2010, Unindicted Co-conspirator 1 sent
26 defendant SU an e-mail with a subject line of "C-17," attached a file
27 titled "Desktop 22.rar," and wrote that he would send defendant SU
28 the password for the file.

1 24. On January 14, 2010, defendant SU sent an e-mail to
2 Unindicted Co-conspirator 1 with a subject line of "RE: C-17,"
3 attached a file titled "Desktop 22.rar," and asked Unindicted Co-
4 conspirator 1 to give defendant SU the password for the file.

5 25. On January 21, 2010, Unindicted Co-conspirator 1 sent
6 defendant SU a file titled "C-17_2.rar" and asked defendant SU to
7 write Unindicted Co-conspirator 1 a document about which files were
8 important, which ones were not important, and what they were.

9 26. On January 22, 2010, Unindicted Co-conspirator 1 sent an e-
10 mail to defendant SU with a subject line of "Re: C-17 _2," and wrote
11 that 3.txt was the subdirectory and document of 3-jianua.txt, added
12 that some directory trees contained random codes, and reminded
13 defendant SU to read 3.txt.

14 27. On January 23, 2010, defendant SU sent an e-mail to
15 Unindicted Co-conspirator 1 with a subject line of "RE: C-17 _2,"
16 attached a document titled "Appendix 3.rar," and wrote that, judging
17 from its name, the document looked fine.

18 28. On January 23, 2010, Unindicted Co-conspirator 1 sent an e-
19 mail to defendant SU with a subject line of "Re: C-17 _2," and wrote
20 that 3.txt was the list of documents, added that defendant SU should
21 pay attention to it, and noted that there was some gibberish due to
22 incorrect encoding.

23 29. On January 25, 2010, defendant SU sent an e-mail to
24 Unindicted Co-conspirator 1 with a subject line of "Re: C-17 _2" and
25 attached a document titled "Appendix-3.docx," which was a list
26 approximately 1,467 pages long of files and folders related to the C-
27 17, with some files and folders highlighted in yellow. In the e-mail
28 defendant SU wrote that the useful ones were marked in yellow and

1 that they should be the computer documents of a person who used an
2 airplane as opposed to a designer.

3 30. On February 2, 2010, defendant SU sent an e-mail to
4 Unindicted Co-conspirator 1 with a subject line of "Document No. 17,"
5 and defendant SU attached to this e-mail a compressed file, the
6 contents of which included a file with the characters "C-17" in the
7 filename.

8 31. On February 4, 2010, defendant SU sent Unindicted Co-
9 conspirator 1 an e-mail attaching a file titled "System
10 20100206.rar." Compressed within the .rar file was a file with the
11 characters "C-17" in the filename.

12 32. On February 7, 2010, defendant SU sent Unindicted Co-
13 conspirator 1 an e-mail attaching a file titled "20100207.rar."
14 Compressed within the .rar file was a document with the characters
15 "C-17" in the filename.

16 33. On February 28, 2010, defendant SU sent Unindicted Co-
17 conspirator 1 an e-mail in which defendant SU wrote that the value
18 was decent for a document related to a specific military aircraft,
19 and that it was information needed by an identified state-owned
20 aircraft company in China, but that the company was too stingy.

21 34. On March 1, 2010, Unindicted Co-conspirator 1 sent
22 defendant SU an e-mail and wrote only "17 keywords" in the body of
23 the e-mail.

24 35. On March 1, 2010, Unindicted Co-conspirator 1 sent
25 defendant SU an e-mail and wrote "17's LIST. Read Carefully."
26 Unindicted Co-conspirator 1 attached a file to that e-mail titled
27 "17.rar."
28

1 36. On March 3, 2010, defendant SU sent Unindicted Co-
2 conspirator 1 an e-mail and attached a file titled "17.rar."
3 Compressed within the .rar file were 11 .txt files, whose file names
4 were 17/1.txt through 17/10.txt and an additional file titled
5 17/tools.txt.

6 37. On March 4, 2010, defendant SU sent Unindicted Co-
7 conspirator 1 an e-mail attaching a file titled "blueprint.rar."

8 38. On March 7, 2010, Unindicted Co-conspirator 1 sent an e-
9 mail to another co-conspirator attaching several reports about the
10 expenses and activities of certain Chinese entities. One report
11 described how one of the entities identified targets and sought
12 foreign technologies to advance research and development cost-
13 effectively.

14 39. On March 19, 2010, Unindicted Co-conspirator 1 sent
15 defendant SU an e-mail with a subject line of "View picture" and
16 wrote in the body of the e-mail "Haha." Unindicted Co-conspirator 1
17 attached to that e-mail an image of a list of seven filenames that
18 had English characters followed by Chinese characters describing
19 their contents, six of which files contained "c-17" or "c17" in the
20 name of the file.

21 40. On April 4, 2010, Unindicted Co-conspirator 1 sent
22 defendant SU an e-mail with a subject line of "22" and wrote "22" in
23 the body of the e-mail. Attached to the e-mail was a document titled
24 "22.rar."

25 41. On April 4, 2010, defendant SU sent Unindicted Co-
26 conspirator 1 an e-mail with a subject line of "RE: 22."

27 42. On April 4, 2010, defendant SU sent Unindicted Co-
28 conspirator 1 an e-mail with a subject line of "RE: 22" and

1 instructed Unindicted Co-conspirator 1 to take a look at the file
2 "avel\Training\AVEL Familiarization Course 7-28-08 .ppt."

3 43. On April 4, 2010, Unindicted Co-conspirator 1 sent
4 defendant SU an e-mail with a subject line of "Re: Reply: 22" and
5 attached an image file named "IMG_0367.JPG." That image showed a
6 computer monitor displaying a presentation related to training on an
7 F-22 component used in launching missiles, which was marked
8 proprietary and with the warning, "Proprietary Information Source
9 Selection Sensitive. This Data is Covered by IATR [sic] 22 CFR 120-
10 130."

11 44. On April 4, 2010, Unindicted Co-conspirator 1 sent
12 defendant SU an e-mail and asked defendant SU about providing a
13 sample of the data they had acquired relating to the C-17.

14 45. On April 5, 2010, defendant SU sent Unindicted Co-
15 conspirator 1 an e-mail concerning the sale of data and expenses.

16 46. On April 5, 2010, Unindicted Co-conspirator 1 sent
17 defendant SU an e-mail and wrote that the sample of C-17 data was not
18 intended for sale, but rather for use as a bargaining chip.

19 47. On August 27, 2010, defendant SU sent Unindicted Co-
20 conspirator 1 an e-mail attaching a .rar file.

21 48. On October 24, 2010, defendant SU sent Unindicted Co-
22 conspirator 1 an e-mail. Attached to that e-mail was a .rar file,
23 and compressed within the .rar were five documents containing
24 filenames that corresponded to military and civilian aircraft. These
25 documents listed some files and folders that were highlighted in
26 yellow.

27 49. On December 27, 2010, Unindicted Co-conspirator 1 e-mailed
28 to Unindicted Co-conspirator 2 a report that described meeting the

1 objective of an identified Chinese company to acquire U.S. military
2 technology but sought additional funds to complete the "C-17 Special
3 Project."

4 50. On August 11, 2011, Unindicted Co-conspirator 1 sent an e-
5 mail to defendant SU that included a screenshot image of a document
6 and asked defendant SU what the document was.

7 51. On November 10, 2011, defendant SU drafted and modified a
8 report that discussed how an identified Chinese entity had acquired
9 research and development information that related to a specific
10 military project that was subject to export restrictions and was
11 restricted by the U.S. Department of Defense, explained why that
12 information was valuable, and sought support to complete its work in
13 acquiring more information.

14 52. On November 10, 2011, defendant SU sent an e-mail to
15 Unindicted Co-conspirator 1 and Unindicted Co-conspirator 2.
16 Attached to that e-mail was the report described in paragraph 51.

17 53. On December 8, 2011, Unindicted Co-conspirator 2 sent an e-
18 mail to Unindicted Co-conspirator 1 with a list of e-mail addresses,
19 names, and affiliations or roles in U.S. and other governments as
20 well as how the e-mail addresses were compromised.

21 54. On February 26, 2012, Unindicted Co-conspirator 1 sent
22 Unindicted Co-conspirator 2 an e-mail attaching a list of thirty-two
23 U.S. military projects and corresponding amounts of data.

24 55. On March 23, 2012, defendant SU modified a document related
25 to a flight test plan for the F-35 aircraft with different portions
26 written in English and in Chinese that bore notations that it was
27 proprietary information and subject to export restrictions.

28

1 56. On May 3, 2012, defendant SU sent an e-mail to Unindicted
2 Co-conspirator 1 with a subject line of "Plan." Attached to that e-
3 mail was the document described in paragraph 55.

4 57. On August 6, 2012, Unindicted Co-conspirator 1 drafted and
5 edited a document that described the acquisition of 65 gigabytes of
6 data in 630,000 files and 85,000 file folders that included scans,
7 drawings, and technical details related to the C-17 obtained by
8 gaining access to the Boeing network in January 2010, and noted that
9 the C-17 had been developed at a cost of \$3.4 billion in research and
10 development expenses.

11 58. On August 13, 2012, Unindicted Co-conspirator 1 sent
12 Unindicted Co-conspirator 2 an e-mail with a subject line of "c17."
13 Attached to that e-mail was the document described in paragraph 57.

14 59. On February 21, 2013, Unindicted Co-conspirator 1 sent an
15 e-mail to Unindicted Co-conspirator 2 that attached a report. The
16 attached report described how the entity with which they were
17 affiliated in China used servers in multiple countries, transferred
18 data to Hong Kong or Macau, and then carried the data to China by
19 hand. The report described how the entity focused in the United
20 States on military technologies, among other topics, and had acquired
21 data related to the F-35 and C-17.

22 60. On May 21, 2014, Unindicted Co-conspirator 1 forwarded an
23 e-mail to a co-conspirator attaching a report describing how a
24 company had been targeted, how its network had been infiltrated, how
25 the computer data stored at the company had been downloaded and
26 transmitted to Macau after going through jumps overseas and before
27 being physically delivered, and how future computer intrusions of the
28 company in a second phase were being designed to address security

1 measures that had prevented acquisition of the information they
2 sought.

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

COUNT ONE

[18 U.S.C. §§ 1030(b), (c)(2)(B)(i)-(iii), (c)(3)(A)]

A. OBJECTS OF THE CONSPIRACY

61. Beginning in or about October 2008, and continuing up to and including at least in or about May 2014, in Orange County, within the Central District of California, and elsewhere, including outside the United States, defendant SU BIN, also known as ("aka") "Stephen Su," aka "Stephen Subin," aka "Steven Subin" ("defendant SU"), Unindicted Co-conspirator 1, Unindicted Co-conspirator 2, and others known and unknown to the Grand Jury, knowingly combined, conspired, and agreed with each other knowingly and intentionally to commit offenses against the United States, namely:

a. To intentionally access a computer without authorization, and exceed authorized access, and thereby obtain information from a protected computer, as that term is defined at Title 18, United States Code, Section 1030(e)(2), (1) where the offense was committed for purposes of commercial advantage and private financial gain; (2) where the offense was committed in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, (a) conspiring to export defense articles, in violation of Title 18, United States Code, Section 371, and Title 22, United States Code, Sections 2778(b)(2) and (c), and Title 22, Code of Federal Regulations, Sections 121.1, 123.1, 127.1(a)(1), 127.1(a)(3), 127.1(a)(4), 127.1(d), and 127.1(e), as alleged in Count Four of this Indictment; and (b) conspiring to commit theft of trade secrets, in violation of Title 18, United States Code, Section 1832(a)(5), as alleged in Count Five of this Indictment; and (3) where the value of

1 the information obtained and sought exceeded \$5,000, all in violation
2 of Title 18, United States Code, Sections 1030(a)(2)(C) and
3 (c)(2)(B)(i)-(iii); and

4 b. To knowingly, and with intent to defraud, access a
5 protected computer, as that term is defined at Title 18, United
6 States Code, Section 1030(e)(2), without authorization, and exceed
7 authorized access, and by means of such conduct further the intended
8 fraud and obtain a thing of value, specifically, information related
9 to military and aviation technology, in violation of Title 18, United
10 States Code, Sections 1030(a)(4) and (c)(3)(A).

11 B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE
12 ACCOMPLISHED

13 62. The objects of the conspiracy were to be accomplished in
14 substance as follows:

15 63. Defendant SU would e-mail Unindicted Co-Conspirators 1 and
16 2 with guidance on what persons, companies, and technologies to
17 target for unlawful computer intrusions.

18 64. Unindicted Co-Conspirator 1 would e-mail defendant SU
19 information and files showing defendant SU the information and files
20 to which Unindicted Co-conspirator 1 had gained access through
21 unlawful computer intrusions. Defendant SU would then provide
22 direction to Unindicted Co-conspirator 1 as to which information and
23 files Unindicted Co-conspirator 1 should steal and obtain via
24 unlawful computer intrusions. After gaining unauthorized access into
25 various protected computers, Unindicted Co-conspirator 1 would then
26 steal, copy, download, transmit, possess, and send the information
27 and files that defendant SU had directed him to obtain.

1 65. Defendant SU, Unindicted Co-conspirator 1, and Unindicted
2 Co-conspirator 2 would then write, revise, and circulate reports that
3 described the information they and others had obtained by engaging in
4 such computer hacking, the value of that information, the
5 significance of the information in developing similar technologies,
6 their progress, and their need to continue their computer intrusions.

7 66. Defendant SU and Unindicted Co-conspirator 1 would
8 communicate about selling some of the information that they had
9 obtained as a result of their unlawful computer intrusions.

10 C. OVERT ACTS

11 67. On or about the relevant dates listed herein, in
12 furtherance of the conspiracy and to accomplish the objects of the
13 conspiracy, defendant SU, Unindicted Co-conspirator 1, Unindicted Co-
14 conspirator 2, and others known and unknown to the Grand Jury,
15 committed various overt acts within the Central District of
16 California and elsewhere. These overt acts included sending e-mails,
17 drafting and revising reports and other documents, and other overt
18 acts, including but not limited to the allegations contained in
19 paragraphs 18 through 60 of the Introductory Allegations, which are
20 incorporated herein by reference.

COUNT TWO

[18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i)-(iii);

18 U.S.C. § 2(a)]

1
2
3
4 Between on or about January 1, 2010 and on or about April 30,
5 2010, in Orange County, within the Central District of California,
6 and elsewhere, including outside the United States, defendant SU BIN,
7 also known as ("aka") "Stephen Su," aka "Stephen Subin," aka "Steven
8 Subin" ("defendant SU") intentionally accessed and attempted to
9 access a computer without authorization, and exceeded authorized
10 access, and aided and abetted Unindicted Co-conspirator 1 and other
11 persons known and unknown to the Grand Jury in doing so, and thereby
12 obtained information and attempted to obtain information, including
13 information related to the C-17, from a protected computer, as that
14 term is defined at Title 18, United States Code, Section 1030(e)(2).

15 The offense was committed by defendant SU (1) for purposes of
16 commercial advantage and private financial gain; (2) in furtherance
17 of a criminal and tortious act in violation of the Constitution and
18 the laws of the United States, specifically, (a) conspiring to export
19 defense articles, in violation of Title 18, United States Code,
20 Section 371, and Title 22, United States Code, Sections 2778(b)(2)
21 and (c), and Title 22, Code of Federal Regulations, Sections 121.1,
22 123.1, 127.1(a)(1), 127.1(a)(3), 127.1(a)(4), 127.1(d), and 127.1(e),
23 as alleged in Count Four of this Indictment; and (b) conspiring to
24 commit theft of trade secrets, in violation of Title 18, United
25 States Code, Section 1832(a)(5), as alleged in Count Five of this
26 Indictment; and (3) the value of the information obtained and that
27 defendant SU attempted to obtain exceeded \$5,000.

COUNT THREE

[18 U.S.C. §§ 1030(a)(4), (c)(3)(A); 18 U.S.C. § 2(a)]

Between on or about January 1, 2010 and on or about April 30, 2010, in Orange County, within the Central District of California, and elsewhere, including outside the United States, defendant SU BIN, also known as ("aka") "Stephen Su," aka "Stephen Subin," aka "Steven Subin" ("defendant SU") knowingly and with intent to defraud accessed and attempted to access a protected computer, as that term is defined at Title 18, United States Code, Section 1030(e)(2), without authorization, and exceeded authorized access, and aided and abetted Unindicted Co-conspirator 1 and other persons known and unknown to the Grand Jury in doing so, and by means of such conduct furthered defendant SU's intended fraud and obtained a thing of value, including specifically information related to military and other technology and including specifically information related to the C-17.

COUNT FOUR

[18 U.S.C. § 371]

A. OBJECT OF THE CONSPIRACY

68. Beginning in or about October 2008, and continuing up to and including at least in or about May 2014, in Orange County, within the Central District of California, and elsewhere, including outside the United States, defendant SU BIN, also known as ("aka") "Stephen Su," aka "Stephen Subin," aka "Steven Subin" ("defendant SU"), Unindicted Co-conspirator 1, Unindicted Co-conspirator 2, and others known and unknown to the Grand Jury, knowingly combined, conspired, and agreed with each other knowingly and intentionally to commit an offense against the United States, namely:

a. To willfully export and cause to be exported from the United States items designated as defense articles on the USML, namely technical data, including by means of disclosing such technical data to foreign nationals, without having first obtained from the DDTC the required export license or authorization for such export, in violation of Title 22, United States Code, Sections 2778(b) and (c), and Title 22, Code of Federal Regulations, Sections 121.1, 123.1, 127.1(a)(1), 127.1(a)(3), 127.1(a)(4), 127.1(d), and 127.1(e).

B. MEANS BY WHICH THE OBJECT OF THE CONSPIRACY WAS TO BE ACCOMPLISHED

69. The object of the conspiracy was to be accomplished in substance as follows:

70. Defendant SU would e-mail Unindicted Co-Conspirators 1 and 2 with guidance on what persons, companies, and technologies to

1 target in order to obtain export-controlled technical data and other
2 information through unlawful computer intrusions.

3 71. Unindicted Co-Conspirator 1 would e-mail defendant SU
4 information and files showing defendant SU the export-controlled
5 technical data and other information and files to which Unindicted
6 Co-conspirator 1 had gained access through unlawful computer
7 intrusions. Defendant SU would then provide direction to Unindicted
8 Co-conspirator 1 as to which information and files Unindicted Co-
9 conspirator 1 should steal and obtain via unlawful computer
10 intrusions. After gaining unauthorized access into various protected
11 computers, Unindicted Co-conspirator 1 would then steal, copy,
12 download, transmit, possess, and send the information and files that
13 defendant SU had directed him to obtain, without having obtained
14 permission or authorization to export technical data out of the
15 United States or to disclose it to foreign persons.

16 72. Defendant SU, Unindicted Co-conspirator 1, and Unindicted
17 Co-conspirator 2 would then write, revise, and circulate reports that
18 described the export-controlled technical data and other information
19 they and others had obtained by engaging in such computer hacking,
20 the value of that information, the significance of the information in
21 developing similar technologies, their progress, and their need to
22 continue their computer intrusions. The reports would also explain
23 that the information was protected by U.S. export restrictions.

24 C. OVERT ACTS

25 73. On or about the relevant dates listed herein, in
26 furtherance of the conspiracy and to accomplish the object of the
27 conspiracy, defendant SU, Unindicted Co-conspirator 1, Unindicted Co-
28 conspirator 2, and others known and unknown to the Grand Jury,

1 committed various overt acts within the Central District of
2 California and elsewhere. Those overt acts included sending e-mails,
3 drafting and revising reports and other documents, and other overt
4 acts, and include, but are not limited to, the allegations contained
5 in paragraphs 29, 39, 41, 42, 43, 49, 51, 52, 55, 56, and 59 of the
6 Introductory Allegations, which are incorporated herein by reference.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

COUNT FIVE

[18 U.S.C. § 1832(a)(5)]

A. OBJECTS OF THE CONSPIRACY

74. Beginning in or about October 2008, and continuing up to and including at least in or about May 2014, in Orange County, within the Central District of California, and elsewhere, including outside the United States, defendant SU BIN, also known as ("aka") "Stephen Su," aka "Stephen Subin," aka "Steven Subin" ("defendant SU"), Unindicted Co-conspirator 1, Unindicted Co-conspirator 2, and others known and unknown to the Grand Jury, knowingly combined, conspired, and agreed with each other knowingly and intentionally to commit offenses against the United States, namely:

a. To knowingly steal and without authorization appropriate, take, and conceal, and by fraud, artifice, and deception obtain a trade secret that is related to and included in a product that is produced for, used in, and placed in and intended for use in interstate and foreign commerce, with the intent to convert the trade secret to the economic benefit of someone other than the owner of the trade secret, and intending and knowing that doing so would injure any owner of that trade secret, in violation of Title 18, United States Code, Section 1832(a)(1);

b. To knowingly and without authorization copy, duplicate, photograph, download, upload, replicate, transmit, deliver, send, communicate, and convey a trade secret that is related to and included in a product that is produced for, used in, and placed in and intended for use in interstate and foreign commerce, with the intent to convert the trade secret to the economic benefit of someone other than the owner of the trade secret, and intending

1 and knowing that doing so would injure any owner of that trade
2 secret, in violation of Title 18, United States Code, Section
3 1832(a)(2); and

4 c. To knowingly receive, buy, and possess a trade secret
5 that is related to and included in a product that is produced for,
6 used in, and placed in and intended for use in interstate and foreign
7 commerce, knowing the same to have been stolen and appropriated,
8 obtained, and converted without authorization, with the intent to
9 convert the trade secret, to the economic benefit of someone other
10 than the owner of the trade secret, and intending and knowing that
11 doing so would injure any owner of that trade secret, in violation of
12 Title 18, United States Code, Section 1832(a)(3).

13 B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE
14 ACCOMPLISHED

15 75. The objects of the conspiracy were to be accomplished in
16 substance as follows:

17 76. Defendant SU would e-mail Unindicted Co-Conspirators 1 and
18 2 with guidance on what persons, companies, and technologies to
19 target for unlawful computer intrusions in order to obtain trade
20 secrets and other information, intending to convert such trade
21 secrets and other information to the economic benefit of persons and
22 entities other than their owners and intending and knowing that doing
23 so would injure the owners of the trade secrets and other
24 information.

25 77. Unindicted Co-Conspirator 1 would e-mail defendant SU
26 information and files showing defendant SU the trade secrets and
27 other information and files to which Unindicted Co-conspirator 1 had
28 gained access through unlawful computer intrusions. Defendant SU

1 would then provide direction to Unindicted Co-conspirator 1 as to
2 which information and files, including which trade secrets,
3 Unindicted Co-conspirator 1 should steal and obtain via unlawful
4 computer intrusions. After gaining unauthorized access to various
5 protected computers, Unindicted Co-conspirator 1 would then steal,
6 copy, download, transmit, possess, and send the information and
7 files, including the trade secrets, that defendant SU had directed
8 him to obtain. Defendant SU would then receive and possess the
9 information and files, including the unlawfully obtained trade
10 secrets, knowing they had been stolen and obtained without
11 authorization.

12 78. Defendant SU, Unindicted Co-conspirator 1, and Unindicted
13 Co-conspirator 2 would then write, revise, and circulate reports that
14 described the trade secrets and other information they and others had
15 obtained by engaging in such computer hacking, the value of that
16 information, the significance of the information in developing
17 similar technologies, their progress, and their need to continue
18 their computer intrusions.

19 79. Defendant SU and Unindicted Co-conspirator 1 would
20 communicate about selling some of the trade secrets and other
21 information that they had obtained as a result of their unlawful
22 computer intrusions.

23 C. OVERT ACTS

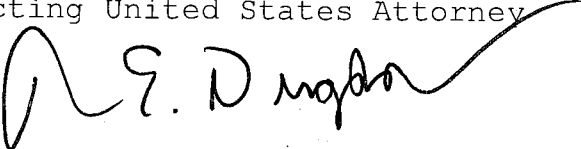
24 80. On or about the relevant dates listed herein, in
25 furtherance of the conspiracy and to accomplish the object of the
26 conspiracy, defendant SU, Unindicted Co-conspirator 1, Unindicted Co-
27 conspirator 2, and others known and unknown to the Grand Jury,
28 committed various overt acts within the Central District of

1 California and elsewhere. Those overt acts included sending e-mails,
2 drafting and revising reports and other documents, and other overt
3 acts, and include, but are not limited to, the allegations contained
4 in paragraphs 19, 33, 42, 43, 44, 45, 46, 48, 51, 52, 55, 56, 57, and
5 58 of the Introductory Allegations, which are incorporated herein by
6 reference.

7
8
9
10 A TRUE BILL

11
12 151
Foreperson

13 STEPHANIE YONEKURA
14 Acting United States Attorney

15 
16 ROBERT E. DUGDALE
17 Assistant United States Attorney
Chief, Criminal Division

18 PATRICK R. FITZGERALD
19 Assistant United States Attorney
Chief, National Security Section

20 ANTHONY J. LEWIS
21 Assistant United States Attorney
National Security Section

22 AARON LEWIS
23 Assistant United States Attorney
National Security Section