AO 91 (Rev. 11/82)

CRIMINAL COMPLAINT

COPY

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v. SU BIN, aka Stephen Su, aka Stephen Subin	DOCKET NO. MAGISTRATE'S CASE NO. 14-1318M

FILED
CLERK, U.S. DISTRICT COURT
JUN 27 2014
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

Complaint for violation of Title 18, United States Code, and Section 1030(b) (Conspiracy to Gain Unauthorized Access to a Protected Computer and Obtaining Information and Things of Value with Intent to Defraud), and Section 1030(a)(2)(C) (Unauthorized Access of a Protected Computer and Obtaining Information)

NAME OF MAGISTRATE JUDGE		LOCATION
HONORABLE RALPH ZAREFSKY	UNITED STATES MAGISTRATE JUDGE	Los Angeles, California

DATE OF OFFENSE	PLACE OF OFFENSE	ADDRESS OF ACCUSED (IF KNOWN)
January 10, 2010	Los Angeles County and Orange County	

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

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

Beginning in or about 2009 until 2013, in Los Angeles and Orange County, within the Central District of California, in a matter within the jurisdiction of the Federal Bureau of Investigation ("FBI"), defendant Su Bin, also known as Stephen Su, also known as Stephen Subin, conspired to gain unauthorized access to protected computers in the United States and to obtain information, and to obtain things of value with the intent to defraud, and did gain unauthorized access to protected computers in the United States and obtained information.

BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:

(See attached affidavit which is incorporated as part of this Complaint)

MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.	SIGNATURE OF COMPLAINANT **Noel A. Neeman** OFFICIAL TITLE Special Agent – Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

SIGNATURE OF MAGISTRATE JUDGE[1]	DATE
RALPH ZAREFSKY	June 27, 2014

[1] See Federal Rules of Criminal Procedure 3 and 54

AUSA Anthony J. Lewis x1786 REC: Detention

AM

A F F I D A V I T

I, Noel A. Neeman, being duly sworn, hereby declare and state as follows:

I.

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2006, where I have been assigned to the Los Angeles Field Office. I am currently assigned to conduct investigations related to computer intrusions and national security. Prior to becoming a Special Agent with the FBI, I was a law clerk for a federal judge, and prior to that I worked for a law firm and for an investment bank. I received an undergraduate degree in economics and a law degree. In my experience with the FBI, I have directed or otherwise been involved in investigating violations of federal law.

2. I am submitting this affidavit in support of a complaint against and arrest warrant for SU BIN ("SU") for a violation of Title 18, United States Code, Section 1030(a)(2)(C) (Unauthorized Access of a Computer and Obtaining Information), and for a conspiracy in violation of Title 18, United States Code, Section 1030(b) to violate both Title 18, United States Code, Sections 1030(a)(2)(C) and Section 1030(a)(4) (Accessing a Computer to Defraud and Obtain Value).

3. There is probable cause to believe that SU BIN, Uncharged Co-Conspirator 1 ("UC1"), and Uncharged Co-Conspirator 2 ("UC2") conspired with each other and others to gain unauthorized access to computers maintained by Boeing and other companies in the United States and obtain information, including data related to military projects, beginning on or about 2009 and continuing through about 2013. Specifically, as set forth below, SU, UC1, and UC2 gained remote access from China to information residing on the computer systems of U.S. companies, including cleared defense contractors.

4. While others remain under investigation for their roles in the offense, a summary of the scheme among these co-conspirators is as follows, and is set forth in further detail below:

a. UC1 and UC2 are citizens of and located in the Peoples' Republic of China ("PRC"). They are each affiliated with multiple organizations and entities in the PRC.

b. UC1 and UC2 have been engaged in clandestine computer and network reconnaissance and intrusion operations--i.e., gaining unauthorized access to business computers and networks--targeting the United States and other foreign countries and obtaining information from them. They have no known affiliation with any U.S. companies.

c. SU is a PRC Citizen and currently is in the process of attempting to obtain permanent resident status in Canada. SU is the owner and manager of Lode-Tech, a PRC-based company focused on aviation technology with an office in Canada, and is in contact with military and commercial entities involved in aerospace technology in the PRC. Starting at least by August of 2009, UC1 began working with SU. UC1 would e-mail SU file directories listing data on the computer systems of U.S. and foreign companies to which UC1 had gained access. SU would then advise UC1 and UC2 what technology to target from those companies. In some instances SU would also seek to sell stolen data obtained by UC1 to entities in the PRC, including to state-owned companies, for their personal profit.

d. The investigation has shown that SU has used multiple e-mail accounts, including subin@lode-tech.com, which is an e-mail account maintained at his business Lode Tech. He also uses e-mail addresses hosted in the United States, such as subinstsu@hotmail.com and stephensubin@gmail.com. SU has been identified as the user of these accounts in several ways. For example, he uses subin@lode-tech.com, where his name, telephone and facsimile numbers, and Skype username appear in the signature block. UC1 also wrote to SU at one of his e-mail accounts addressing him as "Su." SU sent e-mails to UC1 with attachments. The metadata associated with some of these

attachments indicated that they were written or revised by "Stephensu" or "Subin," both of which are derivations of his actual name. When SU crossed the U.S. border on December 31, 2012, he had documents with him identifying the stephensubin@gmail.com e-mail account.

e. UC1 and UC2 also use multiple e-mail accounts, including e-mail accounts hosted by U.S. companies, such as Gmail accounts. The investigation has shown that UC1 and UC2 use these particular e-mail accounts as both UC1 and UC2 sent multiple copies of their personal identification documents (passports, Hong Kong identification cards, and other government-issued identification) using these e-mail accounts.

5. As a part of that scheme, SU, UC1, and UC2 gained unauthorized access to computers maintained in Orange County, California by the Boeing Company ("Boeing") for the C-17 Strategic Transport Aircraft. Specifically:

a. In early 2009, UC1 and UC2 began targeting Boeing's computer network, with the objective of finding and gaining access to information related to Boeing's military projects, including the C-17 aircraft. Boeing is a cleared defense contractor that produces both military and commercial aircraft and other technology. The C-17 is an advanced strategic transport aircraft, which was developed over many years.

b. Beginning in January 2010, UC1 and SU began e-mailing each other about data on Boeing's computer systems. In one of those e-mails, SU highlighted certain file names within a C-17 directory listing that he believed had value and e-mailed the highlighted file listings back to UC1, as if to request that UC1 steal those select files.

c. In a report summarizing their work titled "C-17 Project Reconnaissance Summary," prepared by UC1 and UC2, and sent from UC1 to UC2 on August 13, 2012, UC1 and UC2 claimed to have exfiltrated 630,000 digital files related to the C-17 from Boeing, totaling 65 gigabytes of data.

d. The information sought as a part of the conspiracy included specific files related to parts and performance of the C-17 military cargo aircraft, as well as files related to other military aircraft, such as the F-22 and F-35 fighter jets.

6. The facts set forth in this affidavit are based upon (1) my personal involvement in this investigation; (2) my review of reports and other documents related to this investigation; (3) my training and experience; (4) court-authorized surveillance; and (5) information obtained from other law enforcement officers and witnesses.

7. This affidavit is intended to show that there is sufficient probable cause for the requested arrest warrant and

does not purport to set forth all of my knowledge of, or the government's investigation into, the matters described herein. I have set forth only those facts and circumstances that I believe are necessary to establish probable cause for the issuance of the requested arrest warrant. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. Further, all dates noted in this affidavit are on or about the date listed, and are specified in Greenwich Mean Time ("GMT"). The communications discussed below were originally in Chinese, English or a mix of both languages. In instances where Chinese language appeared in the original communication, I am including the summary of the English language translations or a translated quote of the communication that I received from a linguist who reviewed the original text in Chinese. In certain instances I have provided the original Chinese text in addition to including the corresponding English language translation. Unless stated otherwise, all e-mails referred to below were obtained pursuant to court-authorized surveillance or court-authorized disclosure of stored communications.

II.

LEGAL BACKGROUND

8. Title 18, United States Code, Section 1030 sets forth certain crimes involving unauthorized access of computers.

Specifically, Title 18, United States Code, Section 1030(a)(2) provides criminal punishment for whoever:

> intentionally accesses a computer without authorization . . . , and thereby obtains—
>
> . . .
>
> (C) information from any protected computer.

9. Section 1030(c)(2)(B) provides that a violation of Section 1030(a)(2)(C) is a felony if:

> (i) the offense was committed for purposes of commercial advantage or private financial gain;
>
> (ii) the offense was committed in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State; or
>
> (iii) the value of the information obtained exceeds $5,000 . . . .

10. Title 18, United States Code, Section 1030(a)(4) provides criminal punishment for whoever:

> knowingly and with intent to defraud, accesses a protected computer without authorization . . . , and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

11. For purposes of Sections 1030(a)(2) and 1030(a)(4), a "protected computer" is defined by Section 1030(e)(2) to mean a computer:

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

III.

FACTUAL SUMMARY

A. Definitions

12. For purposes of this affidavit, the following terms are defined as follows:

a. Defense Contractor: A defense contractor or a cleared contractor is a company that is authorized to perform work on projects or contracts, including classified projects, for the government, including the Department of Defense. Such companies typically have access to sensitive information necessary for the development and production of national defense technology and equipment.

b. Internet Protocol ("IP") Address: An Internet Protocol address, or IP address, is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Many companies control a range

or a block of IP addresses.

c. Hop Point: As described in some detail below, a hop point is a computer that is used as an intermediary between a computer used to conduct a computer intrusion and the victim computer. A hop point is used to obscure or conceal the true origin of commands being sent to a victim computer, or the true destination of files or information extracted from a victim computer. When a hop point is used, the only IP address that a victim's computer will "see" is the IP address of the hop point, not the IP address of the attacker (hence the term "hop," as the attack hops through the intermediary). This technique can help to conceal the IP address, location, and identity of the actor responsible for the computer intrusion. A hop point can either be a server that is rented by the person conducting the intrusion or by a complicit party, or a computer used by a legitimate business that has been compromised and used as a relay for information, commands, or data between the attacker and the victim. Sometimes multiple hop points may be used to shuttle information, commands, or data through multiple computers between an attacker and a victim computer.

d. .rar Files: A .rar extension on a file is an extension used for files that are compressed using a specific format that is capable of being encrypted as well, also known as a roshal archive. When a .rar file is encrypted, it is

generally protected with a password that, when entered, will decrypt and decompress the files into their original format (such as into Adobe .pdf files or Microsoft Word .doc files). Even an encrypted .rar file may sometimes reveal a directory or list of the files that it contains.

e. File Directory Listing: A file directory is a logical subdivision of a storage medium (such as a hard drive) that contains files or subdirectories, and it is often graphically represented in operating systems as a folder. A directory listing is a list of the files and subdirectories (or subfolders) that the directory contains, often including file extensions that show the type or format of each file, and sometimes the subfolders' contents as well. The listing displays both the contents of a folder and how those contents are organized within subfolders.

B. Background on Intrusions Originating in China

13. As set forth below, evidence shows that SU, UC1, and UC2 stole large quantities of data that relate to dozens of U.S. military projects. In addition to the evidence below, I have reviewed multiple private security reports, open source materials, and news articles detailing computer intrusions that originated in the PRC, that sought sensitive military technology and intellectual property, and that followed certain routine practices.

14. Based on my training and experience and my review of those open source materials and reports, I have learned that intrusions originating in the PRC often have certain characteristics, including:

a. The hackers send a phishing e-mail to an employee at their primary target or victim, that is designed to appear as if it came from a colleague or legitimate business contact. The phishing e-mail prompts the victim employee to click on a link or open an attachment. Doing either then causes the victim recipient's computer to initiate an outbound connection with a domain (e.g., as www.xxxx.org) that is under the control of the hackers. What is known as the Domain Name System ("DNS") works as a "phonebook," translating each domain into an IP address. By having control of the domain embedded in the link or attachment, the hackers can manipulate the IP address--i.e., the physical computer--to which the victim computer connects. That computer is often what is known as the C2, short for "command and control."

b. From the command and control computer, the hackers can install additional malware--or malicious software--onto the victim's computer, use that malware to access the victim's computer remotely using tools such as the remote desktop protocol, and can begin exploring the now-compromised computer and the network to which it is connected. The hackers

can also install malware that allows their presence to be persistent (for example, by calling back out to a domain that would lead to a command and control computer), they can escalate their privileges, and they can gain access to secure parts of an internal network.

c. Once the desired set of data is located, it can be compressed into a .rar file or other file compression format, and exfiltrated, or transmitted, from the victim's computer system to other computers controlled by the hackers.

d. The hackers use hop points both to enter the victim's computer system and exfiltrate data from it. The hop points are typically secondary victims, whose data is not necessarily being targeted but whose computer is being used as a relay--either to relay commands to the primary victim's computer or to relay the data from the victim as it is being exfiltrated. Sometimes multiple hop points or layers are used.

C. Subjects of the Investigation

15. Probable cause exists to believe that SU, UC1, and UC2 participated in a scheme to gain unauthorized access to computers in the United States, including computers and networks maintained by Boeing in Orange County, California, within the Central District of California, and to exfiltrate U.S. military technical data from those computers.

16. UC1, located in the PRC, is affiliated with multiple organizations and entities in the PRC. UC2, also located in the PRC, is UC1's supervisor or superior in the organizations and entities with which they are both affiliated. UC1 and UC2 are named as two of the three members of the implementation team that executed the Boeing C-17 exfiltration in a report titled "C-17 work summary" that UC1 e-mailed to UC2.

17. SU BIN, aka Stephen Subin, aka Stephen Su, is head of Lode Technology Co., Ltd., aka Lode Tech, aka Loade Tech, which maintains offices at an address in Beijing, People's Republic of China ("PRC"), and an address in Canada. Multiple e-mails SU sent contain a signature block showing SU is affiliated with Lode Tech. SU is a citizen of China, and a permanent resident of Canada. Nonetheless, based on my review of border crossing records, SU has continued to spend significant time in China. Based on a review of SU's Canadian permanent resident card, SU was born in 1965 and his Canadian permanent resident card number is XXXX6446. Based on a review of U.S. Customs and Border Protection border crossing records, SU traveled to the United States on December 31, 2012, using Chinese passport number XXXXX8293. The photograph below was taken during SU's entry into the United States on June 22, 2011.

PHOTOGRAPH OF SU BIN

18. Based on a review of the e-mail communications between SU and UC1, I believe they have a working relationship in which SU works with UC1 in the clandestine acquisition of military technology, as demonstrated by their exfiltration of data related to the C-17 aircraft discussed below in Section F, in which SU and UC1 coordinated which specific files to steal. They also worked together to sell exfiltrated military technology and technical data, as they did for example in connection with the C-17.

D. Background on Computer Intrusion Activities and Objectives of UC1 and UC2

19. On July 7, 2011, UC1 sent an e-mail with an attachment to UC2. The attachment was a report that identified the targets, objectives, and successes of an identified entity's computer intrusion activities. Specifically:

a. Included in the report's list of "Past Achievements" was surveillance involving "military technology," which named an identified U.S. defense contractor and claimed that the entity had controlled one of the company's FTP (or File Transfer Protocol) servers and obtained 20G, or gigabytes, of technology information from it. The report also identified a U.S. developed unmanned aerial vehicle ("UAV") and claimed that the entity had "acquired a list of targeted contractors and suppliers of that project and conducted reconnaissance of the targeted network structure. We have collected a large amount of information and mailboxes of the targeted relevant personnel. We have also obtained the password for the customer management system of the supplier [Identified U.S. Company] and controlled the customer information of that company." The report also claimed that "[t]hrough long-term reconnaissance and penetration, [we have] secured the authority to control the website of the . . . missile developed jointly by India and Russia and that they would "await the opportunity to conduct internal penetration."

b. Other "Past Achievements" listed were obtaining military technology in Taiwan and files held by various groups within China, including the "Democracy Movement," and the "Tibetan Independence Movement." The report concluded by noting

that it would keep "military technology intelligence as a main focus," among other targets.

20. On February 21, 2013, UC1 sent an e-mail with a document attachment to UC2. The e-mail attachment provided additional detail on the activities and methodologies of a specific entity in the PRC. Specifically, the report revealed that[1]:

(1) . . .

> First, we use the surveillance means which combines espionage work and technology(s) to accommodate the demands of S&T [likely Science and Technology] development. . . .
>
> Second, we have gradually established technology bases outside China for the sake of security/safety and stability. So far, jump servers [likely hop points] have been set up in the U.S., Korea, Singapore and etc. The rotations/switches/changes are made on them irregularly based on the security/safety variations of the environment.
>
> Third, machine rooms are set up in the surrounding areas/regions for work convenience. Our machine rooms have been set up in Hong Kong and Macao respectively with legal status. . . .
>
> Fourth, in order to avoid diplomatic and legal complications, surveillance work and intelligence collection are done outside China. The collected intelligence will be sent first by an intelligence officer via a pre-ordered temporary server placed outside China or via a jump server which is placed in a third country before it finally gets to the surrounding regions/areas or a work station located in Hong

[1] My interpretations of certain terms are indicated in brackets.

> Kong or Macao. The intelligence is always picked up and transferred to China in person. . . .
>
> . . .
>
> (3) . . . The focus on the U.S. is primarily on the military technologies but it also touches other areas whereas the focus on Taiwan is mainly on the military maneuvers and military construction. So far, we still have control on American companies like [identifying U.S. companies] and etc. and the focus is mainly on those American enterprises which belong to the top 50 arms companies in the world.
>
> (4) In recent years, we, with relentless work and through multiple channels, have obtains respectively a series of military industrial technology data including F-35, C-17, [additional identified U.S. military technologies] as well as the Taiwanese military maneuvers, warfare operation plans, strategic targets, espionage activities and so forth.

21. On February 27, 2012, UC1 sent an e-mail with an attachment to UC2. The subject of the e-mail was "Complete Listing" and the attachment listed 32 United States military projects and data amounts associated with each project. For example, next to "F-22," the table listed "220M," which I believe indicates that 220 megabytes of data had been stolen regarding the F-22. Many of the other thirty-one projects listed amounts of data followed by a "G," which I believe refers to gigabytes of data, including one project that listed "57G" next to it. Based on my training, experience, and a review of those e-mails, I believe the attachment was a list of

compromised projects and the amounts of exfiltrated data claimed to have been obtained by UC1, UC2, and others with whom they work.

22. For several of the projects listed in this chart I have seen additional correspondence exchanged between SU, UC1, and UC2, which includes corroborating material supporting the claim that these projects were compromised. This corroborating information includes file directory listings, technical schematics, and proprietary documents of the victim companies.

23. FBI Special Agents, including myself, have compared many of the exfiltrated technical documents and excerpts exchanged between SU, UC1, and UC2, to originals obtained directly from U.S. companies or U.S. government entities, as set forth below. Because many of the military projects compromised by SU, UC1, and UC2 involved multiple defense contractors and subcontractors, the specific locations and companies from which many of the documents were obtained remains under investigation. With respect to the compromise of C-17 data, however, as discussed below, UC1 sent UC2 a report stating they had stolen the C-17 data from Boeing directly, and describing the intrusion that acquired the C-17 data. Likewise, e-mails between SU and UC1 in January 2010 contain at least one lengthy C-17 directory file listing that matches in extensive detail the files and folders hosted on Boeing's computer systems. These facts show

that the C-17 data was exfiltrated directly from Boeing's computer systems.

E. SU's Relationship with UC1 and UC2

24. SU's relationship with UC1 and UC2 appears to have begun in the summer of 2009. At that time SU began sending a series of e-mails to UC1 and UC2 that--based on their content and my training and experience--appear to be targeting instructions for companies that SU recommended UC1 and UC2 evaluate for computer intrusions.

a. On August 5, 2009, SU sent an e-mail with an attachment from his stephensubin@gmail.com account to UC1. The subject of the e-mail was "2008 Aerospace Industries arranged listing" and the attachment listed multiple U.S. and foreign companies in a "[p]erformance ranking," including one company in China.

b. On August 6, 2009, SU sent an e-mail with an attachment from his subin@lode-tech.com account to UC1. The subject of the e-mail was "My cell phone number." At the bottom of the e-mail was SU's signature block including his mobile telephone number. Using this number as a password I was able to open the password-protected file attached to the e-mail. The attachment was an excel spreadsheet listing the e-mail addresses, telephone contact information, and program roles for 80 engineers and program personnel working on a military

development project. The individuals listed on the contact sheet included employees of U.S. companies and a branch of the U.S. armed services. The metadata of the document indicated the document was originally created at an identified U.S. company.

c. Approximately two and a half years after receiving this project contact sheet from SU, UC1 included the associated military project to which it relates in the list of compromised projects that he sent to UC2 on February 27, 2012 (see paragraph 21). The relevant entry read "57G" next to that project. Based on these e-mails and other similar exchanges set forth herein, I believe this sequence of events shows that SU directed UC1 on whom and what to target, and UC1 later claimed to have successfully exfiltrated data from that target.

d. Further showing that SU provided targeting instructions to UC1 and UC2, SU sent UC1 additional e-mails from his subin@lode-tech.com account. One e-mail was sent on December 14, 2009, with a subject line of "Target," which I believe was the purpose of the e-mail--to identify a target for UC1 to compromise. The attachment to the e-mail listed the names and positions of four individuals--including the President and Vice Presidents for Electronic Systems Division, Electronic Manufacturing Division, and Program Management, as well as the website and telephone number for a company that develops

military electronic systems, including weapons control and electronic warfare systems.

e. On December 17, 2009, SU sent another e-mail to UC1 with a subject line of "RE: Target." In that e-mail, SU identified other companies and e-mail accounts that were important, including the website, names, and e-mail addresses for four people at a European company that develops military navigation, guidance, and control systems. This second e-mail was carbon copied to one of UC2's e-mail addresses, demonstrating SU was in contact with both UC1 and UC2 at that time.

f. Based on a review of numerous e-mails collected in this investigation, SU and UC2 were in fact in contact with each other as early as September 4, 2009, when SU sent an e-mail to both UC1 and UC2, advising them that Boeing would be sharing space with Lode-Tech at the Beijing Aviation Expo. These e-mails demonstrate: (1) that SU was in contact with both UC1 and UC2 by September 2009; and (2) that SU was simultaneously communicating with UC1 and UC2 about targets of exfiltration. Based on the nature of their communications, I believe UC1, UC2, and SU were all participating in the conspiracy in 2009.

F. Exfiltration of C-17 Data

25. On August 13, 2012, UC1 sent an e-mail with an attachment to UC2. The subject of the e-mail was "c-17." The

attachment was a report titled "C-17 work summary." The report claimed that there had been a successful exfiltration of C-17-related data from Boeing. The report indicated that UC1, UC2, and a third individual were responsible for the implementation of the project. The report also referenced an attached "Sample File" and attached "Directory File" but those files were not attached to the e-mail. The report stated as follows:

> . . . In 2009, . . . [we] began reconnaissance of C-17 strategic transport aircraft, manufactured by the American Boeing Company and code named "Globemaster." . . . [W]e safely, smoothly accomplished the entrusted mission in one year, making important contributions to our national defense scientific research development and receiving unanimous favorable comments . . . .
>
> . . . The development of C-17 strategic transport aircraft is one of the most time-consuming projects in the American history of aviation research and manufacture: a total of 14 years from 1981 when the McDonnell Douglas Company won the development contract to 1995 when all test flights were completed. In development expenses, it is the third most expensive military aircraft in American history, costing $3.4 billion (U.S.) in research and development . . . .
>
> Thorough planning, meticulous preparations, seizing opportunity . . . , [we] initiated all human and material preparations for the reconnaissance in the beginning of 2009 . . . . After a few months' hard work and untiring efforts, through internal coordination [we] <u>for the first time broke through the internal network of the Boeing Company in January of 2010</u>. Through investigation of Boeing Company's internal network, we discovered that the Boeing Company's internal network structure is extremely complex. Its border deployment has FW and IPS,

the core network deployment has IDS, and the secret network has [ ] type isolation equipment as anti-invasion security equipment in huge quantities. Currently, we have discovered in its internal network 18 domains and about 10,000 machines. Our reconnaissance became extremely cautious because of the highly complex nature of Boeing's internal network. Through painstaking labor and slow groping, we finally discovered C-17 strategic transport aircraft-related materials stored in the secret network. Since the secret network is not open 24 hours and is normally physically isolated, it can be connected only when C-17 project related personnel have verified their secret code. Because we were well-prepared, we obtained in a short time that server's file list and downloaded a small number of documents. Experts have confirmed that the documents were truly C-17 related and the data scope involved the landing gear, flight control system, and airdrop system, etc. Experts inside China have a high opinion about them, expressing that the C-17 data were the first ever seen in the country and confirming the documents' value and their unique nature in China.

Scientific/technical support, safely procure, clear achievement. Since the Boeing Company's internal network structure is highly complex and strictly guarded, successful procurement of C-17 related data required meticulous planning and vigorous technical support. We were able to deal with them one by one in our work. (1) We raised the difficulty level of its counter-reconnaissance work to ensure the secure obtainment of intelligence. From breaking into its internal network to obtaining intelligence, we repeatedly skipped around in its internal network to make it harder to detect reconnaissance, and we also skipped around at suitable times in countries outside the U.S. In the process of skipping, we were supported by a prodigious quantity of tools, routes, and servers, which also ensured the smooth landing of intelligence data. (2) We used technology to exit the network securely. Because breaking into

Boeing's internal network was harder than we imagined, after obtaining intelligence we had to rely on technology to separate and bundle data, change the document formats, etc. Ultimately, we avoided the many internal automatic and manual auditing facilities to transfer data safely and smoothly out of the Boeing Company. (3) We repeatedly skipped around to retreat safely. To ensure obtaining intelligence safely and evading tracking by American law enforcement, we had planned for numerous skip routes in many countries. The routes went through at least three countries, and we ensured one of them did not have friendly relations with the U.S. To safely, smoothly accomplish this mission, we opened five special routes and servers outside the U.S. and shut them down after the mission concluded. (4) We made appropriate investment and reaped enormous achievement. Through our reconnaissance on the C-17 strategic transport aircraft, we obtained files amounting to 65G. Of these, there were 630,000 files and 85,000 file folders, containing the scans of C-17 strategic transport aircraft drawings, revisions, and group signatures, etc. The drawings include the aircraft front, middle, and back; wings; horizontal stabilizer; rudder; and engine pylon. The contents include assembly drawings, parts and spare parts. Some of the drawings contain measurement and allowance, as well as details of different pipelines, electric cable wiring, and equipment installation. Additionally, there were flight tests documents. This set of documents contains detailed contents and the file system is clear and detailed, considered topflight drawings by experts! This project took one year and 2.7 million RMB to execute, showing cost-effectiveness and enormous achievement. This reconnaissance job, because of the . . . sufficient preparations, meticulous planning, has accrued rich experience for our work in future. We are confident and able . . . to complete new mission. . . . August 6, 2012.

[emphasis added]

26. While the report discussed a successful exfiltration by UC1 and UC2, many of the details of the report have not been corroborated. The success and scope of the operation could have been exaggerated. For example, based on information I have received from other FBI agents who learned about Boeing's computer network, I have not discovered any evidence that any classified information has been accessed or exfiltrated. I have also learned that the servers and computers used by Boeing to store the data for the parts and design of the C-17 are in Orange County, California and in other locations, including Dover Air Force Base in Delaware and in McChord Air Force Base in Washington.

27. Nonetheless, there is independent evidence that an exfiltration of C-17 information was successful to some degree. On January 14, 2010, at 09:55:23 +800, UC1 sent SU an e-mail with a subject line of "C-17." In the body of the e-mail, UC1 wrote that he would send the unzip password to SU via text message. Attached to the e-mail was a file titled Desktop 22.rar. What followed this e-mail were a number of e-mails with explicit references to the C-17 in the subject line, in the names of files attached to e-mails, or in the contents of documents attached to e-mails. These e-mails are consistent with the claim in the report that the exfiltration of C-17 data began in January 2010.

28. On January 14, 2010, at 17:22:59, SU sent an e-mail to UC1 with a subject line of "RE: C-17." In the body of the e-mail, SU asked UC1 to give him the original password. Attached to that e-mail was a file titled 22.rar.

29. On January 21, 2010, UC1 sent an e-mail to SU with a subject line of "C-17 _2." Attached to that e-mail was a file titled "C-17_2.rar." In the body of the e-mail, UC1 wrote "The password remains unchanged. Please write me a document about which ones are important, which ones are not important and what they are."

30. On January 22, 2010, UC1 sent SU an e-mail with a subject line of "Re: C-17 _2." In the body of the e-mail, UC1 wrote that the 3.txt was the subdirectory and document of 3-jianhua.txt. UC1 wrote that some directory trees contained random codes. UC1 reminded SU to read the 3.txt.

31. On January 23, 2010, at 21:53:47 +800, SU sent an e-mail to UC1 with a subject line of "RE: C-17 _2." In the body of the e-mail, SU wrote that "judging from its name, the document looks fine." Attached to that e-mail was a .rar file titled "Appendix 3."

32. On January 23, 2010, at 21:57:38 +800, UC1 sent an e-mail to SU with a subject line of "Re: C-17 _2." In the body of the e-mail, UC1 wrote "3.txt is the list of these documents, pay

attention to it! There are some gibberish due to incorrect encoding."

33. On January 26, 2010, SU sent an e-mail to UC1 with a subject line of "Re: C-17 _2" in which SU wrote "There are many picture documents. The useful ones are marked in yellow. Many documents are for application. They should be the computer documents of a person who uses airplane, not the computer documents of a designer."

a. Attached to that e-mail was a Microsoft Word document titled "Appendix 3.docx." That document was 1,467 pages long, and contained what appeared to be a directory structure and list of approximately 50,000 files related to the production, performance, or testing of the C-17. Towards the top of the document there was a directory listing for "Shortcut to electrical-reference-files on [ ]boeing.com.lnk." On March 25, 2014, I learned from another FBI agent that Boeing had confirmed that "[ ]boeing.com.lnk" was an internal Boeing computer server that contained data related to the C-17. Also in the directory listing were approximately 142 files that had been highlighted in yellow, for example: "C17Hangar Requirements 112399.pdf"; "C-17 LOAD TESTINGRev.a.xls"; "C-17 Wiring Failures.ppt"; and what appeared to be a folder of files called "SUPPORT - HYDRAULIC, FIRE SHUT OFF VALVE, OUTBOARD C-

17." The first page of the 1,467 page directory list is displayed below (with redactions by the FBI).

Folder PATH listing for volume Shares L:
Volume serial number is 0006EE50 400A:F04F
Z:.
3 17P1B1172.pdf
3 17P8N1008-535.pdf
3 AC ASGN_Config 4 Aug 09.xls
3 Acronyms.xls
3 [redacted]_Retrofit_Configs_19 Feb 2007 - SW.ppt
3 SDS Link.txt
3 Shortcut to electrical-reference-files on [redacted]boeing.com.lnk
3
????02 -General Vehicle
3 3 AIRCRAFT IDENTIFICATION BY LOT-BLOCK 111709.xls
3 3 Antenna_[redacted].pdf
3 3 C-17 Demilitarization Plan (Draft)_Dec2005.msg
3 3 C-17 station guide.pdf
3 3 C-17A-brochure.pdf
3 3 C17 Aircraft names.xls
3 3 C17 TDPG.pdf
3 3 C17Hangar Requirements 112399.pdf
3 3 Critical Safety Item(CSI) Report_Sep2006.pdf
3 3 DEEP FREEZE.pdf
3 3 Design Handbook_Fastener Instll.pdf
3 3 ELT Compatability Test.pdf
3 3 Increased Gross Weight White Paper(may03).doc
3 3 McChord_new aircraft_FY2010.pdf
3 3 OATP List.xls
3 3 Over G Inspections.pdf
3 3 PCR for Brush Cad Plating.msg
3 3 [redacted] Jet in Comml Colors.bmp
3 3 RE Safty wire for cannon plugs.msg
3 3 [redacted] at March ARB providing APU Training.JPG
3 3 [redacted] at March ARB proving APU and Laptop Training.JPG
3 3
3 ????Box Car Seal
3 3 IMG_1278.jpg
3 3 IMG_1279.jpg
3 3 IMG_1280.jpg
3 3 IMG_1281.jpg
3 3 IMG_1282.jpg
3 3 IMG_1283.jpg
3 3 IMG_1284.jpg
3 3 IMG_1285.jpg
3 3
3 ????DEEP FREEZE_Cold Weather Ops & MX Info
3 3 DEEP FREEZE.pdf

b. Based on the communications above, specifically the e-mails where UC1 sought SU's guidance for which C-17 files to acquire, and SU's response that "[t]he useful ones are marked in yellow," I believe UC1 sent SU the C-17 directory he previously obtained from Boeing's network and SU sent the file back to UC1 adding the yellow highlights to identify the "useful" documents that UC1 should steal.

c. I have also reviewed several of the files received from Boeing on May 30, 2014, that correspond to file names highlighted by SU in the directory file listing that SU e-mailed to UC1. Those documents included a diagram with a label indicating that it contained technical data that is subject to the Arms Export Control Act or the Export Administration Act, PowerPoint presentations with photographs of parts of the C-17, and excel spreadsheets with certain data related to the C-17.

d. I learned from an FBI agent that file names contained in the directory file listing e-mailed by SU match the names of files on Boeing's network. Specifically, I learned that as of May 30, 2014, of the approximately 50,000 files listed in the 1,467-page directory, 38,886 matched files residing on one of Boeing's C-17 servers, or other servers on Boeing's computer systems. Each of the 38,886 files is unique

(i.e., not a duplicate), and the files were named using various naming conventions, examples of which include the following:

1c-17a-2-27jg-30-1.pdf
207200E34P03-317--a.pdf[2]
7383-00142 (EGT Harness MIP).ppt
C17 SDR Briefing.ppt
1780001.pdf
PL1B244172330001-.pdf
SRR-03 C17 Reqmts Use New.PPT
TC1B2441VF7254I00.pdf

34. On February 3, 2010, SU sent UC1 an e-mail attaching a file titled "document," which was a .rar file. The listing of the contents of the compressed .rar file contained a word document that included the characters "C-17" along with other Chinese characters.

35. On February 5, 2010, SU sent UC1 an e-mail attaching a file titled "System 20100206.rar." Compressed within the .rar file was a Microsoft Word Document titled "C-17ÏµÍ³20100206.docx."

36. On February 7, 2010, SU sent UC1 an e-mail attaching a file titled "System 20100207.rar." Compressed within the .rar file was a Microsoft Word document also called "C-17ÏµÍ³20100206.docx," the same name as the compressed file attached to SU's February 5, 2010 e-mail.

37. On March 2, 2010, at 10:40:57 +800, UC1 sent SU an e-mail asking about a "CAMAPROD." SU replied that he was not

---

[2] Over 5,000 of the files follow this format.

sure. UC1 wrote another e-mail that same day to SU and wrote "17 Keywords" in Chinese in the body of the e-mail.

38. On March 2, 2010, at 12:48:56 +800, UC1 sent an e-mail to SU with a subject line of "17." In the body of the e-mail, UC1 wrote "17's LIST. Read carefully." Attached to that e-mail was an attachment titled "17.rar."

39. On March 3, 2010, SU sent an e-mail back to UC1. Attached to that e-mail was an attachment, also titled "17.rar." The .rar file contained 11 .txt files, whose file names are 17/1.txt through 17/10.txt and an additional file titled 17/tools.txt.

40. On March 4, 2010, UC1 sent SU an e-mail attaching a .rar file, which file name translates to "Blueprint.rar." Based on the subject line and the timing of this e-mail and others sent in the same period of time, this may relate either to the C-17 or to a different project about which they also e-mailed during this period of time.

41. On March 20, 2010, UC1 wrote an e-mail to SU with a subject line of "View picture." In the body of the e-mail, UC1 wrote "Haha." Attached to the e-mail was an image titled C-17.jpg with a list of files. That attachment, which appears below this paragraph, is an image of a directory listing referencing the following files, whose names were partially translated from Chinese to English. All but the last one

contained C-17 in their title: 0-25-113-c17 Key alloy and metal parts list manual.pdf; 1c-17a-1-2 Task system manual.pdf; 1c-17a-2-12jg-24-1 Generator manual.pdf; 1c-17a-2-12jg-29-4 Hydraulic system manual.pdf; 1c-17a-2-47jg-20-1 Inertia gas system manual.pdf; 1c-17a-4-56 Cockpit glass manual.pdf; 33d7-50-1592-2 Fuel test computer.pdf. On the same day, SU replied "Got it." Although these exact file names did not appear in the Appendix 3.docx--the 1,467 page directory SU highlighted and sent back to UC1 on January 26, 2010--I recognize "1c-17a-1," "1c-17a-2," and "1c-17a-4" as a naming convention used internally by Boeing to name many of its C-17-related files. The fact that the files discussed above and depicted below are not included in the Appendix 3.docx indicates that UC1, UC2 and SU's intrusion into Boeing went beyond the 50,000 file names listed in the Appendix 3.docx document. Furthermore, the fact that these file names contain the English characters used commonly in Boeing's naming convention followed by Chinese characters suggests that they were likely saved by UC1 somewhere other than Boeing's network. None of the file names from Boeing's C-17 computers that I have seen to date in this investigation have any Chinese characters in them.

00-25-113-c17关键合金和金属零件清单手册.pdf
1c-17a-1-2任务系统手册.pdf
1c-17a-2-12jg-24-1发电机手册.pdf
1c-17a-2-12jg-29-4液压系统手册.pdf
1c-17a-2-47jg-20-1惰性气体系统手册.pdf
1c-17a-4-56座舱玻璃手册.pdf
33d7-50-1592-2油量测试计算机.pdf

42. UC1 used the same Gmail address to send and receive all of the e-mails with SU that referred to the C-17 set forth above in the preceding paragraphs. UC1 also used this same Gmail address to send UC2 the report on the completed intrusion described in paragraph 25.

43. On December 28, 2010, UC1 sent an e-mail to UC2 attaching a report. The report stated that the objective had been to acquire U.S. military technology, that it had done so successfully, and that those involved had established hop points in the United States, France, Japan, and Hong Kong.

44. The report stated that those involved had received funding in the amount of 2.2 million RMB to build up its team and infrastructure, to construct positions outside the border, and to purchase software and hardware. The report noted, however, that the actual expenditure had been 6.8 million RMB, and that the gap of 4.6 million RMB had been covered by a loan. This, the report stated, "has caused significant special project C-17 to miss the best opportunity." The report noted that for

2011, "[t]he C-17 Special Project funds will be approximately 3.5 million Renminbi."

45. Certain aspects of the intrusion described in paragraph 25 correspond to information I have learned about Boeing's network, but because of the complexity of the network's architecture, the review is still ongoing. As noted above, although certain aspects of the e-mail described in paragraph 25 are consistent with the network architecture employed by Boeing, other aspects are not. Nonetheless, based on the other contemporaneous e-mails sent at the time the intrusion was taking place, I believe that SU, UC1, and UC2 obtained unauthorized access to Boeing's network and obtained C-17 information from it.

46. The e-mails cited above regarding the C-17 intrusion occurred between January 14, 2010 and March 20, 2010. Based on copies of SU's passport and identifying documents obtained pursuant to a border search of SU and based upon my review of a database that records border-crossings across the U.S. border, I learned that SU was in the United States for part of this period. Specifically, SU flew from the PRC to the United States on January 13, 2010; then flew from the United States to the PRC on January 24, 2010; then flew from the PRC to the United States on February 11, 2010; then flew from the United States to the PRC on February 21, 2010; and then flew from the PRC to the

United States on May 26, 2010. These records showed when SU came in or out of the United States during that period of time, but did not show where else he traveled inside or outside of the United States.

G. Acquisition of Data for Profit or Economic Gain

47. In addition to e-mails about the content they were accessing and obtaining, SU and UC1 also e-mailed about selling C-17 data. On March 30, 2010, UC1 e-mailed SU and asked if SU had any good news. Then on April 5, 2010, at 9:58, UC1 sent an e-mail to SU with the subject "…". In the e-mail UC1 asked SU "How about giving you the sample of 17?" The e-mail included within its body UC1's March 20, 2010, e-mail to SU where UC1 attached the jpeg of the C-17 files (paragraph 41). Based on this e-mail and the following e-mails, I believe that UC1 was asking SU if it would be helpful to the sales and negotiation process if UC1 provided SU a C-17 document as a sample of the data they had exfiltrated.

48. On April 5, 2010, 10:52, SU sent a reply e-mail to UC1 stating "I understand that it's very urgent for you. It's not that easy to sell the information. If money is collected for the sample of 17, it won't be easy to collect your big money that would follow. Also, it's a long process to apply for the expenses."

49. On April 5, 2010, at 11:30, UC1 replied to SU by e-mail with the subject "Re: Reply: ..." In the body of the e-mail UC1 wrote "It's putting pressure on you, not selling for money. It's just a bargaining chip." I believe that in this e-mail UC1 was explaining that the sample document he referred to earlier was not itself intended to be for sale, but rather to be a bargaining chip to advance the overall negotiation and sale.

50. Thirteen minutes later, at 11:43, UC1 sent a new e-mail to SU with the subject "Thanks a lot." In the body of the e-mail UC1 wrote "OK, that is fine. Thanks a lot." This e-mail also contained in its body UC1's March 20, 2010, e-mail to SU where UC1 attached the jpeg picture file listing C-17 .pdf files.

51. This e-mail exchange shows that both SU and UC1 were seeking the "big money" that would result from selling the information they had acquired.

52. This discussion of value is consistent with other e-mails sent in February and March 2010, in which SU wrote to UC1, referring to a document related to another identified U.S. aircraft and noting that "[t]he value is decent. In China, this information is what the [identified Chinese aircraft corporation] needs. They are too stingy!" Based on this exchange, I believe that SU and UC1 were selling information they obtained to various customers, including PRC aircraft

corporations. This e-mail shows that SU and UC1 were seeking information that they could match to buyers or customers willing to pay a significant price for the information.

53. I have reviewed open source materials that described the corporation identified above as a PRC state-owned aircraft company.

54. Previously, on March 9, 2010, UC1 sent an e-mail to SU with a subject line "My account number." UC1 wrote "China Merchants Bank Shenzhen: [XXXX XXXX XXXX]4611 [UC1]; Industrial and Commercial Bank of China Shenzhen: [XXXX XXXX XXXX XXX]5369 [UC1]."

55. This evidence suggests that SU and UC1 were obtaining the information at least in part for commercial advantage and private financial gain. Given their own estimation of the value of the information obtained related to the C-17 alone (i.e., the "big money"), and my review of the data obtained from multiple military projects, I believe the value of the information they obtained is well in excess of $5,000.

H. Other Military Cargo Aircraft Data

56. As set forth above, I believe that UC1 sent SU file directory listings showing files and folders residing on Boeing's computer networks, and SU then sent back to UC1 a highlighted version of the file directory listing indicating the files of interest for UC1 to exfiltrate. As set forth below, I

believe that SU and UC1 similarly exfiltrated data from a competitor of Boeing regarding another military transport plane, which shows that one of their objectives was to acquire data related to military cargo aircraft.

57. On August 27, 2010, SU sent an e-mail with several attachments from his subin@lode-tech.com account to UC1. Both the subject of the e-mail and the .rar attached to it made reference to what I believe was the numerical model of a military cargo aircraft, and the .rar attached was a file with seven compressed files inside.

58. On October 24, 2010, SU sent an e-mail with several attachments from his subin@lode-tech.com account to UC1. The subject of the e-mail was "Document." The body of the e-mail stated "it remains the same." Attached to the e-mail was a .rar file with reference to the same numerical model. Compressed within that .rar file were five Microsoft Word documents, each of which contained computer file directory listings related to several military and civilian aircraft produced by a non-U.S. aircraft manufacturer. The metadata associated with each of these files identified "Stephen Subin" as the author.

59. In addition to file names related to military aircraft, the directories also included hundreds of file names related to commercial passenger aircraft, including four

specific models. There were over 200 files related to one such civilian aircraft alone.

60. One of the file directories attached to SU's October 24, 2010, e-mail was more than 6,000 pages long. Twenty-two folders and files were highlighted in yellow in this directory, in the same manner that SU had highlighted files of interest in the Boeing C-17 directory. One of these 22 highlighted items was a folder whose name made explicit reference to the model of the military cargo aircraft. That folder alone contained more than 2,000 individual files.

61. Another file directory attached to the e-mail was 137 pages long and contained another 17 yellow highlighted folders and files, covering more than 87 files related to the military cargo aircraft. Several of the yellow highlighted file names included Chinese language added to the end of the file name. Because SU is identified by metadata as the author of the document and SU e-mailed the attachment to UC1, I believe SU most likely added the Chinese language. One of the highlighted file names with added Chinese referred to "outlook" in the file name, which file was depicted in a file directory page. Based on my training and experience I know that a ".pst" file is a Microsoft Outlook Data File format which stores a user's e-mail messages. The English translation of the included Chinese is

"This is an outlook document, if this is from the chief engineer then we will do it."

62. As described above, UC1 and SU followed the same pattern of behavior in their scheme to exfiltrate data related to both the C-17 and this military cargo aircraft. Specifically, after UC1 e-mailed .rar files that I believe were likely file directory listings to SU, SU then e-mailed back to UC1 the uncompressed file directory listings with yellow highlighting on portions of them. I believe SU highlighted in yellow the folders and files that SU believed had value, and sent the directories back to UC1 to exfiltrate the highlighted items from the manufacturer's computer network.

I. Exfiltration of F-22 Information

63. Over the course of the investigation, I have also seen that SU and UC1 have targeted other military technology, including certain technology that relates to the F-22.

64. On April 4, 2010, at 21:42 UC1 sent an e-mail to SU with a subject line of "22." The body of the e-mail read "22." Attached to that document was a file titled "22.rar." Based on a review of e-mails exchanged by UC1 and SU that follow chronologically after this e-mail, and which are discussed below, I believe this .rar file related to the F-22 fighter aircraft.

65. Based on a review of websites belonging to companies that work on parts of the F-22, I know the F-22 "Raptor" was designed as a supersonic, super-maneuverable, stealthed air superiority fighter. According to one web site, the F-22 is the world's premier 5th generation fighter.

66. On April 4, 2010, at 22:33, SU responded to UC1. The subject of that e-mail was "RE: 22." In it, SU wrote that "[i]t's still the information related to the mount." Based on my review of this e-mail, the image attached to it, and the e-mails that UC1 sent SU immediately afterwards, I believe the "mount" SU is referring to is the particular F-22 component ("Component B") that is the subject of the presentation described below.

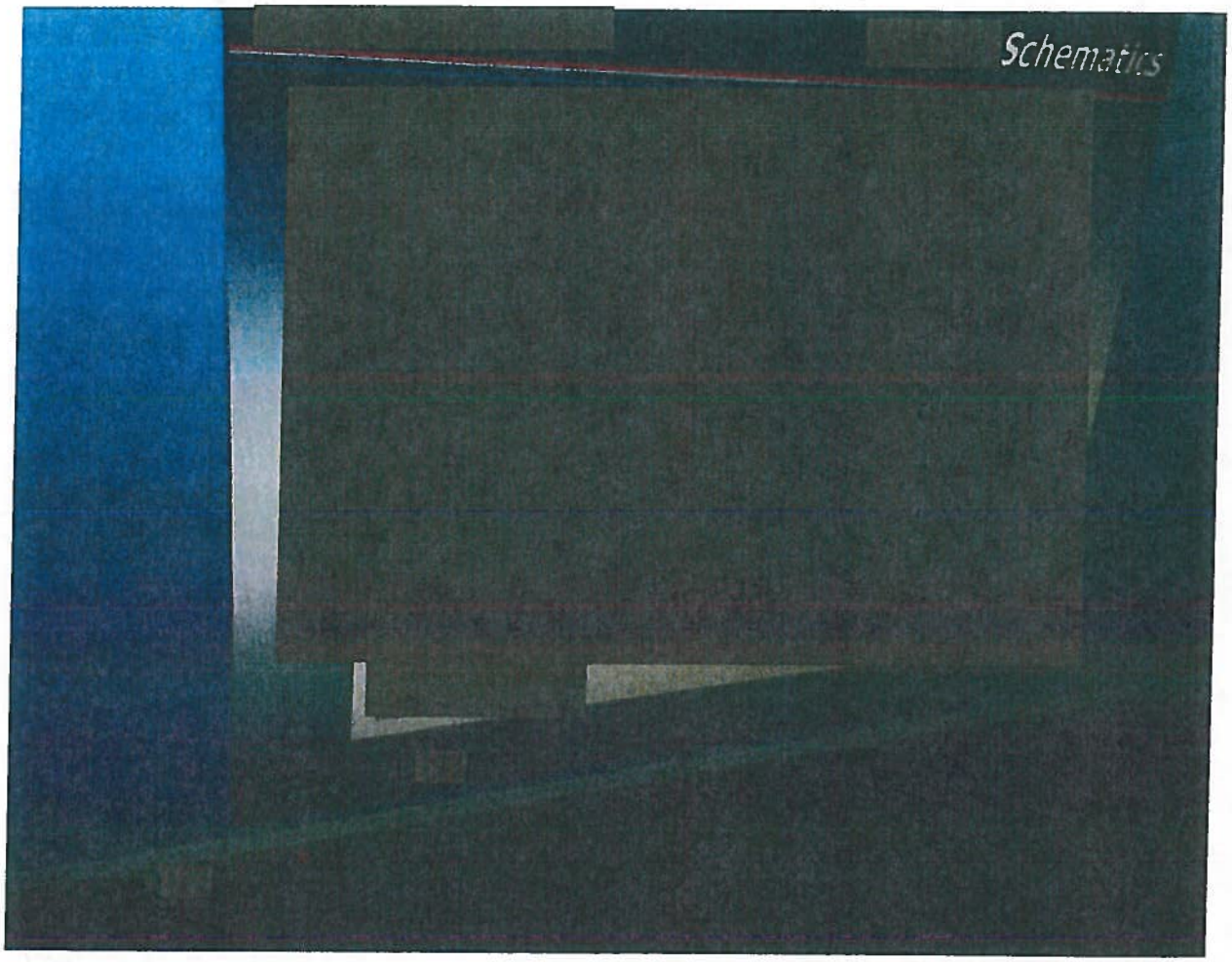
67. On April 4, 2010, at 22:42, SU sent an e-mail to UC1 again and wrote: "Take a look at the document" and then identified a specific PowerPoint file name, folder, and a subfolder with Component B's name. Based on the pattern of UC1 sending SU file directory listings and SU identifying files of interest for UC1 to obtain, I believe the 22.rar files UC1 sent SU likely contained a directory of files related to the F-22, and that the Component B file SU asked UC1 to look at was likely one of many files listed in that file directory. This also shows that SU was telling UC1 which files to access and obtain.

68. On April 4, 2010, at 22:53 UC1 responded by e-mail to SU and included an attachment. The subject line of the e-mail was "Re: Reply: 22." and the attachment was called IMG_0367.JPG. The attachment was a photo of a PowerPoint presentation slide displayed on a computer monitor. The slide was a technical schematic and at the bottom of the slide was written "[Identified Company] Proprietary Information Source Selection Sensitive. This Data is covered by IATR [sic] 22 CFR 120-130." (This means that it is a violation of AECA to export this information from the United States or to disclose it to foreign nationals without a license.)

69. Following this e-mail, UC1 sent SU four more e-mails in quick succession. He sent these e-mails to SU on April 4, 2010, at 22:55, 22:57, 23:06 and 23:12. Each e-mail had the subject line "Re: Reply: 22" and contained a photo attachment identified as IMG_0368.JPG, IMG_0370.JPG, IMG_0369.JPG, and IMG_0372.JPG, respectively.

70. IMG_0369.JPG, shown redacted below, is one of the photos of a computer monitor showing a PowerPoint slide. In this photo part of the task bar at the bottom of the computer screen can be seen. A folder labeled with the name of Component B is visible, as are a series of Chinese characters that say "Mandarin China." I believe the photos were likely taken by UC1 using his mobile phone in front of his computer monitor while he

was accessing the presentation. Based on a review of each of these images, I believe the PowerPoint slides are part of the Component B presentation SU asked UC1 to look at by providing the file path, and that UC1 had possession of the entire PowerPoint presentation. (The image below has had the content redacted by the FBI.)



71. As noted above in paragraph 21, the F-22 is on the list of compromised projects that UC1 and UC2 claimed they had obtained.

72. I have met with representatives of the U.S. company identified in the screenshots, and I have received from them a PowerPoint presentation with content that matches each of the screenshots from the PowerPoint referred to above. The document was dated May 30, 2014, the date on which I received it, and the date appeared to be automatically generated and displayed on the slide. This would be consistent with the date of April 4, 2010 appearing on the slides captured in the screenshots sent on April 4, 2010. Each of the pages captured in the screenshots sent to SU by UC1 matched a page in the document I obtained from the U.S. company.

J. Other Technology Acquired

73. Through my review of e-mails between SU, UC1, and UC2, I have learned that they were involved in acquiring information related to multiple other U.S. military projects, two examples of which are set forth below.

74. First, between November 2 and November 10, 2011, SU sent UC1 and UC2 three e-mails each with an attached report that discussed the PRC's acquisition of data related to an identified advanced United States military project (which I refer to herein as "Project A") and the value of that material. Based on the duplication of content in the reports and because each successive report sent by SU contained additional detail, I believe SU, UC1, and UC2 were preparing and editing the report.

The metadata associated with the first two reports lists one person's name, while the metadata of the most complete and final version of the report listed "Stephensu" as the author. As noted above, SU is also known as Stephen Subin and Stephen Su.

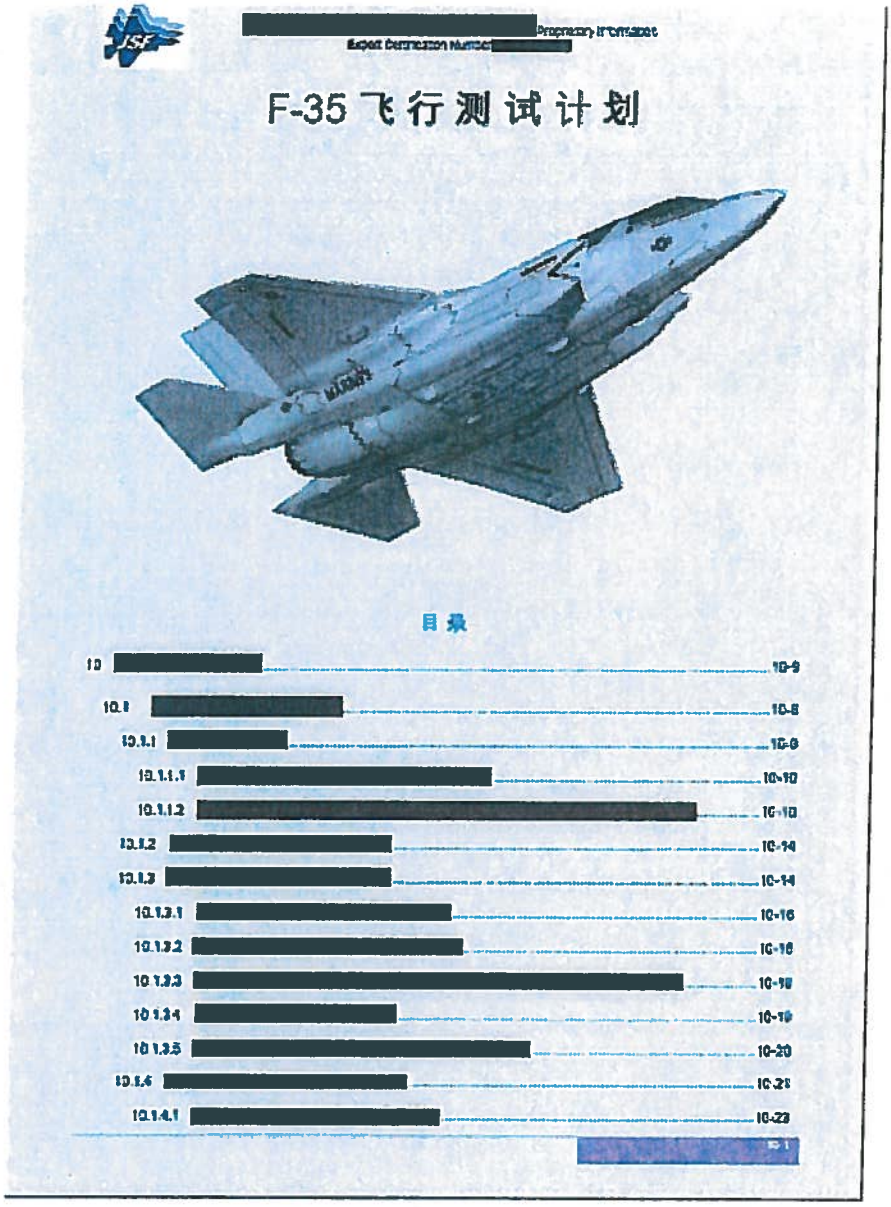
75. The 11-page final report was sent from SU to UC1 and UC2 on November 10, 2011, at 23:48:40 GMT. It included 14 graphics depicting diagrams, data tables, calculations and schematics related to Project A. These graphics are in English and relate to Project A. The report described in Chinese the value and importance of the underlying documents from which the graphics had been taken. The report made reference to obtaining U.S. military data related to the project, including blueprints and testing data. The report also claimed that the information would "allow us to rapidly catch up with U.S. levels," that the information was protected by U.S. export restrictions, and that the information would allow them to "stand easily on the giant's shoulders." While a couple of the slides incorporated into SU's report appear to be publicly available, I have spoken to two U.S. government entities with oversight over Project A, and they have told me that at least nine of the slides or images are not publicly available information about Project A.

76. Second, on May 3, 2012, SU sent UC1 an e-mail with the translated subject line "Plan." Attached to that e-mail was a 120-page Microsoft Word document containing the F-35 Joint

Strike Fighter Flight Test Plan. That document laid out the flight test protocol for the F-35, which, according to open-source materials I have reviewed, is the world's most advanced multi-role fighter, combining radar-evading stealth, supersonic speed, and extreme agility with the most powerful and comprehensive integrated sensor package of any fighter aircraft in history. I also learned that the F-35 was developed by a consortium of defense contractors from the United States and eight other countries at an estimated cost of $11 billion.

77. The "Flight Test Plan" is an English-language document that has Chinese translation incorporated throughout. The metadata of the document identifies an engineer at a U.S. company as the original author and "Subin" as the last person to save the document.

78. Based on the pattern of communication I have observed between SU and UC1 and that is documented in this complaint, I believe UC1 obtained this document and sent it to SU. SU in turn added the Chinese language to the document and sent it back to UC1. The first page of the document is shown below.



79. I visited one of the U.S. companies that works on the F-35 and I viewed the first page of a document that I was told by an employee was an earlier version of this same document. Subsequently, I spoke on the telephone with another employee who confirmed with one of the people believed to be an author of the document that it was a version of a document used in connection

with the F-35 and that it was not distributed publicly. That company also said it had conducted a thorough investigation and found no evidence that a version of this document had been obtained from its computer systems.

IV.

SEALING REQUEST

80. The criminal investigation into the activities of the subject of this affidavit is continuing. Disclosure of the contents of this affidavit would seriously impede the investigation by revealing details of the government's investigation and evidence gathered in connection herewith. It would alert the subjects of the investigation to the fact that the government had obtained their e-mails, which would cause them to stop using those e-mail accounts. It would also be likely to cause them to flee and destroy any evidence of these events, or potentially manufacture evidence that concealed the true nature of their conduct or that indicated that other persons were responsible. Further, the subjects of the investigation would be able to learn the extent of the government's investigation as set forth herein. Accordingly, I request that the Court issue an order sealing this affidavit, the complaint, and arrest warrant until further order of this Court.

V.

CONCLUSION

81. Based on the facts set forth above, I believe that there is probable cause to believe that SU BIN has committed a violation of Title 18, United States Code, Section 1030(a)(2)(C) (Unauthorized Access of a Computer and Obtaining Information), and a violation of Title 18, United States Code, Section 1030(b) by conspiring with UC1 and UC2 to violate both Title 18, United States Code, Sections 1030(a)(2)(C) and Section 1030(a)(4) (Accessing a Computer to Defraud and Obtain Value).

/s/

NOEL A. NEEMAN
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me
on this 27th day of June, 2014

RALPH ZAREFSKY

HONORABLE RALPH ZAREFSKY
UNITED STATES MAGISTRATE JUDGE