No. 16-50339

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

KEITH PRESTON GARTENLAUB,
Defendant-Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
DISTRICT COURT NO. CR 14-173-CAS

EXHIBIT C TO DEFENDANT'S MOTION FOR BAIL PENDING APPEAL—PUBLIC REDACTED VERSION

EILEEN M. DECKER
United States Attorney

PATRICK R. FITZGERALD
Assistant United States Attorney
Chief, National Security Division

ANTHONY J. LEWIS
VICKI CHOU
Assistant United States Attorneys

1500 United States Courthouse
312 North Spring Street
Los Angeles, CA 90012
Telephone: (213) 894-1786
Email: anthony.lewis@usdoj.gov
vicki.chou@usdoj.gov

Attorneys for Plaintiff-Appellee
UNITED STATES OF AMERICA

COPY AUSA

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with the accounts identified as kgartenlaub@yahoo.com and [redacted] that is stored at premises controlled by Yahoo!, Inc.

Case No. 13-1666M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	*Offense Description*
18 U.S.C. § 1030(a)(2)(C), (a)(2)(4) (Unauthorized Computer Access); 22 U.S.C. § 2778 (AECA), 22 C.F.R. Parts 120-130 (ITAR)	See attached Affidavit

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

FBI Special Agent Wesley K. Harris
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/12/13

ANDREW J. WISTRICH
Judge's signature

City and state: Los Angeles, California

Hon. Andrew J. Wistrich, U.S. Magistrate Judge
Printed name and title

AUSA: Anthony J. Lewis AJL

A F F I D A V I T

I, Wesley K. Harris, 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 July 2009. I am a graduate of the FBI Academy. I am currently assigned to conduct investigations related to cyber intrusions and national security, and have been working on this investigation since fall 2012. Prior to working Cyber intrusion investigations, I worked Chinese Counterintelligence since January 2010. Prior to becoming a Special Agent with the FBI, I was a professional services consultant for TMA Systems in Tulsa, Oklahoma. As a Professional Services consultant, I managed network of servers (that included a Storage Area Network (SAN) device) that hosted client databases. In addition to managing this network, I performed custom database integration and design. Lastly, I was also a traveling consultant that performed onsite implementation and training for the larger clients of TMA Systems. In my experience with the FBI, I have directed or otherwise been involved in investigating violations of federal law.

2. I make this affidavit in support of an application for a search warrant for information associated with the accounts identified as:

a. kgartenlaub@yahoo.com (the "GARTENLAUB SUBJECT ACCOUNT," believed to be used by Keith Gartenlaub), and [redacted] (the "[redacted]" believed to be used by Tess Yi, also known as Tess Gartenlaub), which shall be referred to collectively as the "YAHOO SUBJECT ACCOUNTS" that are stored at premises controlled by Yahoo! Inc., (the "YAHOO PROVIDER"), a provider of electronic communication and remote computing services, headquartered at 701 First Avenue, Sunnyvale, California 94089.[1]

b. [redacted] which shall be referred to as the [redacted] believed to be used by [redacted] that is stored at premises controlled by Google, Inc., (the

[1] Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

"GMAIL PROVIDER"), a provider of electronic communication and remote computing services, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The YAHOO SUBJECT ACCOUNTS and GMAIL SUBJECT ACCOUNT, shall be collectively referred to as the "SUBJECT ACCOUNTS," and the YAHOO PROVIDER and the GMAIL PROVIDER shall be referred to as the "PROVIDERS" or as a "PROVIDER."

3. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the PROVIDER to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B.

4. As described in more detail below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNTS constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of Title 18, United States Code, Section 1030(a)(2)(C)

(Unauthorized Access of a Computer and Obtaining Information), Section 1030(a)(2)(4) (Accessing a Computer to Defraud and Obtain Value), Title 22, United States Code, Section 2778 (Arms Export Control Act), and Title 22, Code of Federal Regulations, Parts 120-130 (International Traffic in Arms Regulations). As set forth below, the FBI is investigating a possible compromise of the Boeing C-17 aircraft. As reported by an article in Wired.com in January 2013, a Chinese aircraft named the Y-20 was recently demonstrated, appears to be very similar to the Boeing C-17, and its designs may be attributed to a "spy working at Boeing." The investigation to date has yielded one engineer at Boeing (Keith Gartenlaub) that has the combination of access to the C-17 data, knowledge of the computer network and systems, suspicious behavior and concerns by security personnel who worked with him, and connections and travel to China, and as set forth below there is probable cause to believe that there is evidence of the crimes set forth above on the SUBJECT ACCOUNTS, which include accounts used by his wife and used to communicate about aircraft equipment.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to

set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II.

LEGAL BACKGROUND

A. AECA and ITAR: Regulations on the Export of Munitions

6. The Arms Export Control Act ("AECA"), 22 U.S.C. § 2778, regulates the export of defense articles from the United States that are covered by the United States Munitions List (hereafter the "USML"). The implementing regulations for the AECA are the International Traffic in Arms Regulations ("ITAR"), codified at 22 C.F.R. Parts 120-130.

7. The USML is included in the ITAR at § 121.1. Under the AECA, the President of the United States is authorized to designate those items considered to be "defense articles" covered by the USML. Section 120.1 of the ITAR describes the President's delegation of this authority to the Secretary of State by Executive Order 11958, as amended. The Directorate of Defense Trade Controls ("DDTC"), an agency within the Department of State, is charged with controlling the export and temporary import of defense articles and defense services covered by the USML.

8. Pursuant to § 127.1(a)(1) of the ITAR, it is unlawful to export or attempt to export from the United States, or to re-export or attempt to re-export from one foreign destination to another foreign destination, defense articles, without first obtaining the required license or written approval from the DDTC. Specifically, § 127.1(a) provides:

> Without first obtaining the required license or other written approval from the Directorate of Defense Trade Controls, it is unlawful:
>
> (1) To export or attempt to export from the United States any defense article or technical data or to furnish or attempt to furnish any defense service for which a license or written approval is required by this subchapter;
>
> . . .
>
> (4) To conspire to export, import, reexport, retransfer, furnish or cause to be exported, imported, reexported, retransferred or furnished, any defense article, technical data, or defense service for which a license or written approval is required by this subchapter.

9. Section 120.17 defines "export" to mean:

> . . .
>
> (4) Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; or
>
> (5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.

B. Computer Intrusion Offenses

10. 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.

11. 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.

12. 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.

SUMMARY OF INVESTIGATION

A. Background

13. Probable cause exists to believe that the SUBJECT ACCOUNTS were utilized to and contain evidence of the removal of information, including export controlled technical data, from Boeing's computer networks to China.

14. On January 28, 2013, Wired Magazine published an article titled China's Great Transport Plane Takes Flight. I have reviewed that article, which states the following:

a. The article discussed the flight of the Chinese military's "first homegrown long-range transport plane." The plane, the Xian Y-20, is in roughly the same class as the U.S. C-17 or the Russian Il-76, and is still not fully operational or militarily effective.

b. The government-run Xinhua news service announced that the flight was "significant in promoting China's economic and national defense buildup as well as bettering its emergency handling such as disaster relief and humanitarian aid." The article in Wired magazine noted that the development of the plane may have been spurred in part by the massive earthquake that killed tens of thousands in Sichuan in 2008. In the aftermath of the earthquake, the People's Liberation Army Air Force was equipped with fighter jets, but had only a handful of

small cargo planes carrying relief supplies. The United States sent two Boeing C-17 airplanes, which the Wired Magazine article noted was "welcome assistance but also embarrassing for the Chinese Communist Party."

c. The Wired Magazine article noted that the Y-20 is at least as capacious as Russia's Il-76 cargo plane, which China possesses and which seems to be the basis of the Y-20's design. It then said: "Beijing may also have acquired some of the C-17's blueprints from a spy working at Boeing."

15. I have learned from communications with personnel at Boeing that the C-17 is a military cargo plane. Although complete C-17s have been sold to certain other countries, those sales only take place after government approvals, including export licenses, have been obtained. Because the C-17 is a military cargo plane, I learned from Boeing personnel that a large portion of the project is export controlled, and requires a license for export.

16. On May 31, 2013, ainonline.com published an article called "List of Hacked US Defense System Is Long." The article states that there is a long list of major US aerospace and missile defense systems that have been compromised by hackers that was obtained by the Washington Post. The list includes the F-35, Bell-Boeing V-22 Osprey, Boeing C-17, Boeing P-8 Poseidon, Boeing F/A-18 Super Hornet and Growler, and the Aegis Missile

Defense System. I know, based on my training and experience, that network intrusions are sometimes carried out completely from without, by gaining access through a vulnerability in the victim's computer systems, or by being given access through an insider who agrees to provide direction, guidance, or direct access to the target data.

17. Recent prosecutions demonstrate the aggressive collection of sensitive and military technology by persons and entities in China. [redacted] These prosecutions show that persons and entities in China have sought and acquired classified, sensitive, and proprietary information and technology from the United States. The technology involved in those cases involve military development, including propulsion [redacted] Based on my training and experience, and the facts of those cases, I have learned that some of these compromises of sensitive technology have resulted from exploiting persons who can use their insider access to

obtain information or technology that can be transmitted by removable media devices, e-mail, or other means of electronic transmission.

18. I know, based on my training and experience, that the security measures that are in place to protect sensitive and classified information are significant. [redacted]

B. **Investigation Related to Keith Gartenlaub**

19. On February 5, 2013, Keith Gartenlaub was contacted to setup an interview. Gartenlaub stated that he needed to do a background check to verify that it was in fact the FBI that was contacting him.

20. On February 7, 2013, I and another FBI agent interviewed Keith Gartenlaub at his office at Boeing in Huntington Beach, California. During the course of that interview, I learned the following from Gartenlaub:

a. Gartenlaub provided information concerning the structure of Boeing's database of files related to the C-17

aircraft and the applications that use and access them. Currently, Gartenlaub is the administrator of a set of software application tools called [redacted]. Gartenlaub works on a lot of Boeing projects but mainly focuses on the C-17. Prior to being the [redacted] supervisor, Gartenlaub was an engineer on the [redacted] team. For the C-17 project, Boeing uses a teamcenter database in conjunction with a Storage Area Network ("SAN") device to maintain all the part files for the C-17 project. [redacted]. (A subsequent interview of [redacted] confirmed that she is the database administrator, but she also said that she does not have a login[1] that has access to the C-17 part files.)

[1] As used herein, "login" refers to a username and corresponding password that can be used as credentials to "log in" to an application or database or network. It does not refer to a specific instance of logging in.

The internal department at Boeing called Information Technology Infrastructure ("ITI") administers all the hardware for the servers and SAN for the C-17 network, but most of the service and maintenance for work on that hardware is performed by a subcontractor that has root level access to the servers and SAN. Root level access has complete access to the entire file system. The team Gartenlaub supervises has copy/export access to the files on the SAN.

b. Gartenlaub said that Boeing allows information stored on its internal networks to be accessed externally by using Virtual Private Networking ("VPN"). In order to access the internal Boeing networks from a location outside of Boeing, one has to create a successful VPN connection to the Boeing network.

c. Gartenlaub said that in previous years, Boeing only required one form (username and password) of authentication to create a successful VPN connection. (It was later determined that the way Gartenlaub describes the VPN process is inaccurate. Subsequent interview of other employees revealed that it was much more difficult to create a successful VPN connection, and that Boeing has always required two forms of authentication to create a VPN connection. A second form of authentication may be a token that periodically changes or a card that must be inserted into a computer.)

d. From later interviews with other Boeing employees--[redacted] discussed below in paragraphs 30-34--I learned that with a successful VPN connection using a Boeing administrator's login credentials, one could remotely access every database for every Boeing project administrated by those credentials. In the course of those later interviews, I learned that Gartenlaub is the nationwide Unix military administrator for Boeing, and that if, for example, a military server in Virginia goes down, Gartenlaub would be called. Based on that and my training and experience and the information I learned, I believe that Gartenlaub's credentials would permit him access to Unix servers for all military projects, including the Unix server that houses the C-17 files.

21. I learned from records provided by Bank of America ("BOA") that Gartenlaub has been a customer of BOA since 1998. On February 7, 2013, the day that he was interviewed by the FBI regarding the C-17 and network structure, Gartenlaub enrolled in a wire transfer program at BOA called Safe Pass. Safe Pass is a BOA program used to send wire transfers internationally in excess of $1,000.

22. On February 8, 2013, I and another FBI agent interviewed Keith Gartenlaub again at his office at Boeing in

Huntington Beach, California. During the course of that interview, I learned the following from Gartenlaub:

a. Gartenlaub said that Boeing stores all of the part information for the C-17 and various amounts of data for the P-8, C-130, DC-10 and KC-767 aerospace projects in teamcenter databases. The architectural related information about the C-17 project is stored [redacted] database contains the blueprint architecture on how each part is connected to other parts. Teamcenter does not illustrate which part connects to which part, rather only what each individual part is and how to build each of those parts.)

i. The May 31, 2013 ainonline.com article described above in paragraph 16 referred to not only the C-17 but also the P-8 and other Boeing military projects were compromised.

b. Gartenlaub advised that the C-17 project contains approximately 112,910 unique parts and a total of 265,801 total parts. Each part has approximately 6 associated documents with each part. These associated files are CAD drawings, part blue

prints, revised part blue prints, engineering notes, and sign offs, which are effectively an engineer's assessment that the part will operate effectively.

c. As Gartenlaub had described the previous day, [redacted]. The [redacted] application is an Internet based tool that allows the Air Force, Boeing, and selected suppliers and contractors to access all of the C-17 data in both the Teamcenter and [redacted] databases.

d. [redacted]

i. Given the speed of development of the Y-20, vast amounts of part-specific designs as well as technical blueprints illustrating how the parts relate to each other would be necessary to build the Y-20. These detailed blueprints and part specific designs are housed in compartmented databases supervised by Gartenlaub. I know based on my training and experience and knowledge of this investigation that detailed knowledge of the network would be needed to be able to

exfiltrate that data without alerting computer intrusion personnel or software.

e. Gartenlaub said that his wife is Chinese and that he travels to China, although not for work. Gartenlaub agreed to meet again to help build a profile of the person who would have access to and knowledge of the Boeing systems in order to compromise the C-17 aircraft's data.

23. On Feburary, 8, 2013, approximately 4 hours after the conclusion of the interview, Gartenlaub provided a lead to me by e-mail that he claimed could have been responsible for compromising the C-17 aircraft's files. The information Gartenlaub provided involved an internal Boeing employee and subcontractor and indicated that the subcontractor was downloading part information out of the [redacted] application without Boeing's permission with the help of a Boeing employee. This incident was later determined to not be related after speaking with Boeing internal investigators that had detailed knowledge because the incident began in 2007, but at least according to the Wired article, the PRC became interested in the C-17 after the 2008 earthquake and the need for military cargo aircraft became acute. Additionally, when interviewed, Gartenlaub said there are an estimated 112,910 unique parts and 265,801 total parts. The person who discovered and first reported this other incident said that an estimated 22,400 parts were downloaded in

total. It does not appear that 22,400 out of either 112,910 or 265,801 would be sufficient information to recreate the entire aircraft.

24. On February 11, 2013, Gartenlaub sent an e-mail to me stating that a potential theft of the C-17 part files would most likely have occurred through the [redacted] application. It was later determined that it is unlikely that an intrusion resulting in the compromise of the entire C-17 project would have happened using the [redacted] application. [redacted]. I learned that from [redacted] when he was interviewed, and I have also reviewed some of those logs which begin with the inception of the [redacted] application in Long Beach. It was later determined that unlike the Unix SAN server that contained the C-17 part files, Gartenlaub does not have a login to [redacted] currently.

25. On February 19, 2013, Gartenlaub received an e-mail from Boeing employee [redacted] stating that there were over 900 part files missing on the C-17 SAN, or Storage Area Network.

26. Three days later, on February 22, 2013, another FBI agent and I interviewed Keith Gartenlaub again at his office at Boeing in Huntington Beach, California. Gartenlaub did not bring up the e-mail he had received from [redacted] three days

before, discussed in the previous paragraph. Based on my experiences and training as an FBI Agent, Gartenlaub made many statements which were suspicious in nature and which are set forth in this affidavit.

a. Gartenlaub stated he never had to worry about his security while traveling in China because his wife's family is "well connected." Gartenlaub did not elaborate on what connections she has. Gartenlaub spontaneously stated on numerous occasions that he was loyal to the United States.

b. Gartenlaub said was not happy working on classified projects for Boeing. Gartenlaub was displeased with the way supervision was structured at Boeing. Specifically, it was often the case people who worked on classified projects would have a supervisor that did not have a security clearance. Due to this arrangement, the day-to-day job responsibilities would not be fully understood and documented in the employee's performance evaluations. This caused a number of talented workers who work on classified projects to get laid off by Boeing.

c. Additionally, Gartenlaub did not enjoy working on classified projects because his wife is Chinese. Initially when Gartenlaub and his Chinese wife, Tess Yi, began their relationship in or around 2008, Boeing security did not have a problem Gartenlaub traveling to China. After the second trip to

China, Boeing security recommended that Gartenlaub not travel to China anymore. According to Gartenlaub, Boeing security was concerned that he would be a target of recruitment. Based on the context of this discussion, I understood Gartenlaub to mean recruitment by a Chinese Intelligence Service.

d. Moreover, Gartenlaub said it was a burden to report to Boeing the security-related incidents that occurred while traveling in China. Gartenlaub recalled once such incident in which he and his wife were touring the Great Wall of China. During this trip, someone approached Gartenlaub with a camera. Gartenlaub assumed that this person wanted Gartenlaub to take his picture, but unexpectedly, this person grabbed Gartenlaub and took a picture of them both. Gartenlaub's wife, Tess Yi, dismissed this incident, saying that the person probably has never seen a "white" person before.

e. Gartenlaub also described the approximately twelve employees that report to him, and their current and previous roles, responsibilities, and access to C-17 data. Gartenlaub is the only person on his team who maintains a security clearance (Top Secret). Gartenlaub previously helped set up classified networks for other projects. At no time did Gartenlaub tell investigators about the missing files referred to above in paragraph 25, even though potential infiltration of the C-17 program had been discussed in detail.

f. Gartenlaub also said that there are very few people in Boeing that know how many devices or machines are on the Boeing domains, i.e., its network. In order for someone to know that, they would need to understand Boeing security, which Gartenlaub did.

C. Boeing's Security Files Related to Gartenlaub and Gartenlaub's Travel

27. As set forth above in paragraphs 26.c and 26.d, Gartenlaub expressed his frustration with the limitations Boeing placed on his foreign travel, in particular because his wife is Chinese. I have reviewed records provided by security personal at Boeing, and another FBI SA and I have had conversations with security personnel at Boeing regarding Gartenlaub, and from that I have learned the following:

a. The project security officer ("PSO") who was responsible for all security related to a sensitive project on which Gartenlaub worked had interacted with Gartenlaub. That PSO wrote the following about Gartenlaub:

> Keith was always a concern for us. My impression when dealing with him was that he always felt he was above the rules. He married someone from China and would travel there to visit family. He also owned property in China (an apartment, as I recall). When the rules changed about travel to China, we told him he could no longer go there. He had already bought tickets and told us he was going anyway. His manager told him something along the lines of "this is a career limiting decision" meaning there might not be a job for him when he returned. Gartenlaub told us that he

canceled the trip but I always suspected he went anyway, but had no proof.

b. The PSO also wrote that nobody trusted him, that his transfer off of a sensitive project and onto the C-17 was the C-17's loss and the sensitive project's gain.

c. I also learned that Gartenlaub was required to report any foreign travel since at least 2003 until 2011. I have reviewed the pre-travel notification and post-travel questionnaires that Gartenlaub submitted before and after his foreign travel during that time. I did not see any notification regarding the April 2010 trip that was the subject of the PSO's suspicion, and I have reviewed the results of a government database showing U.S. border crossings and did not see evidence of Gartenlaub traveling abroad in April 2010, although I did learn that Gartenlaub took as leave the same time he had planned as vacation.

d. I have also compared documentation Gartenlaub submitted regarding his foreign travel to Boeing against the records of that government database showing when persons have crossed the U.S. border. Those are for the most part consistent, with the following exception. In June 2008, four months after getting married to Tess Yi, Gartenlaub and Yi traveled to China. Gartenlaub explained in Boeing documentation that he and his wife completed the purchase of a home on which

she had put a down payment before they were married. That travel appears in both the Gartenlaub travel reported to Boeing and in the database. In November 2008, Gartenlaub traveled to Canada for Thanksgiving for one week. That travel also appears in both the travel Gartenlaub reported to Boeing and in the database. Between those two trips, the database shows that Gartenlaub crossed the border into the United States on September 21, 2008, at the same border crossing where he returned to the United States after Thanksgiving of that year. There is no record of his travel departing from the United States (although the database is more effective at capturing inbound border-crossings), and this did not appear in the documentation provided by Boeing with all of Gartenlaub's reported travel.

28. That government database shows that Gartenlaub and his wife have traveled internationally together on multiple occasions, including the June 2008 trip in which Gartenlaub reported to Boeing that he and his wife traveled to China. On October 9, 2009, Gartenlaub departed LAX on a flight bound for Tokyo, Japan, returning from Seoul, South Korea (not Tokyo) on October 22, 2009. On May 22, 2011, Gartenlaub again left LAX on a flight for Tokyo, Japan, returning from Shanghai, China (not Tokyo) on June 3, 2011.

a. Similar to Gartenlaub, Tess Yi, has also made multiple international trips reflected on that database, some of which correspond with Gartenlaub's travel. Specifically, Yi made the following international trips:

05/16/2008, departed LAX arriving in Toyko, Japan;

06/13/2008, returned to LAX from Toyko, Japan.

01/22/2009, departed LAX arriving in Hong Kong;

02/12/2009, returned to LAX from Hong Kong.

08/13/2009, departed LAX arriving in Shanghai, China;

11/11/2009, returned to LAX from Shanghai, China.

04/22/2010, departed LAX arriving in Shanghai, China;

05/06/2010, returned to LAX from Shanghai, China.

12/01/2010, departed LAX arriving in Shanghai, China;

12/16/2010, returned to LAX from Shanghai, China.

05/06/2011, approximately one month after Gartenlaub became the PDM supervisor, Yi departed LAX arriving in Toyko, Japan;

06/03/2011, Gartenlaub and Yi both returned to LAX from international trips. As noted above, Gartenlaub returned to LAX from Shanghai; Yi, however, returned to LAX from Toyko, Japan.

11/07/2011, departed LAX arriving in Shanghai, China;

11/20/2011, returned to LAX from Shanghai, China.

09/25/2012, 20 days after Gartenlaub became the Infrastructure manager for all Unix military servers nationwide, Yi departs LAX arriving in Shanghai, China.

11/04/2012, Yi returned to LAX from Shanghai, China.

i. Given that Gartenlaub's wife was in Shanghai during Gartenlaub's October 2009 and May/June 2011 flights from LAX to Toyko, Japan, I believe that Toyko, Japan was not the final destination for Gartenlaub, and that Gartenlaub traveled to China to meet his wife, through Toyko, Japan. This is consistent with the travel that Gartenlaub reported to Boeing.

D. Gartenlaub's Recent Use of His Boeing E-mail and Boeing Computer

29. I and other FBI investigators have reviewed information provided by Boeing concerning Gartenlaub's activity while accessing Boeing computers. From that, I learned that on March 9, 2013, e-mail address [redacted], the [redacted], emailed Tess Gartenlaub at [redacted] the [redacted] The e-mail subject was in Chinese and has been translated into English and reads: Forward: Fish Fork Patent Pending. The email contained five images of a metal block with a hole in the center and a screen through the center. The email was then forwarded to Keith.P.Gartenlaub@Boeing.com (which is not a SUBJECT

ACCOUNT) the same day. Tess Gartenlaub's message to Keith was "Please advise."

a. An open source search was conducted of the term "Fish Fork" and according to ip.com this term refers to a "harpoon device which is installed on a helicopter for landing on warships." Aviation Industry Corporation of China ("AVIC"), which is owned by the PRC government, has applied for a Chinese patent for this product. Currently, the United States, Australia and Great Britain are using this device. The metadata for the five images were extracted and show that the photos were taken on September 12, 2012, and GPS latitude and longitude coordinates embedded in EXIF data in the photograph show that it was taken in Beijing, China. Based on my training and experience and my knowledge of this investigation, I believe that someone who works on aircraft equipment and technology in China was seeking Gartenlaub's advice in trying to construct their "Fish Fork."

b. I learned from another FBI Special Agent who spoke to a security representative at Boeing that Boeing makes a part that appears similar to the photos in this e-mail, and that the part Boeing makes is for landing unmanned aircraft on warships.

c. In the material provided by Boeing, which according to Boeing contained a complete set of Gartenlaub's e-

mail messages surrounding the period of time in which this e-mail was sent, Gartenlaub did not respond to this e-mail using his Boeing e-mail account or otherwise using his Boeing computer. In the course of my conversations with Gartenlaub, other personnel who work at Boeing on related matters, and with security personnel at Boeing, I have not learned of any information indicating that Gartenlaub's duties and responsibilities include advising anyone in China or anyone at the Chinese aerospace company AVIC regarding Fish Fork or other equipment used to land aircraft on warships.

d. Although Gartenlaub is currently employed as an administrator of various computer systems, I have learned that he is an engineer by training. According to a resume provided by Boeing internal investigator in May 2013, Gartenlaub has a degree from the University of Cincinnati in Aerospace Engineering. Additionally, the resume states that Gartenlaub was awarded a full fellowship at the Von Karmen Institute for Fluid Dynamics in Belgium in 1989. The same resume states that Gartenlaub finished second place in the American Institute of Aeronautics and Astronautics in team engine design competition.

30. On April 25, 2013, I and another FBI agent interviewed [redacted] at his office at Boeing in Huntington Beach, California. During the course of that interview, I learned the following from [redacted]:

a. [redacted] stated that he and Gartenlaub previously worked on classified projects at Boeing. While working on these projects, [redacted] and Gartenlaub's cubicles were next to each other. [redacted] declined to discuss the nature of the classified project but did state that it involved setting up classified networks. [redacted] stated that Gartenlaub is an expert and knows more than him about setting up classified networks. In addition to setting up classified network, Gartenlaub also has experience setting up teamcenter databases, the databases that store the location of the specific part files that are accessed by various Boeing applications. [redacted] was not certain why Gartenlaub wanted to stop working on classified projects at Boeing. [redacted] suspects that it is due to issues with Gartenlaub's wife being Chinese. [redacted] recalled an incident in which Gartenlaub wanted to travel to China to see his wife's family but Boeing denied this travel request.

31. Following the interview, [redacted] was in frequent contact with interviewing agents to clarify some technical facts discussed in the interview. Specifically on May 6, 2013, at 12:58 pm, I received an e-mail from [redacted] identifying exactly who has access to the folders that contain the C-17 part data (i.e., not the applications that access them, and not the database that stores the directories or folders where they are located, but the actual data for the files that describe the

individual parts). [redacted] confirmed a list of 24 total logins. Of the 24 logins, 23 were logins that were each specific to an individual person. [redacted] Additional information pertaining to this login was discussed in a May 21, 2013 interview of [redacted], discussed below in paragraph 34. I also learned from [redacted] that the team Gartenlaub supervises in Long Beach know the [redacted] log in, and I know that there are approximately twelve people on that team.

32. On May 6, 2013, approximately two hours after it was determined which logins at Boeing have access to the C-17 part files on the SAN device, [redacted] initiated an instant message chat with Gartenlaub on their work computers. I reviewed data provided by Boeing that show the content of this chat, which was the following:

Chat Activity

[redacted]
Title: [redacted]
Date: Mon, May 06, 2013 2:26 PM

[2:26:49 PM] [redacted] > are you in HB today?
[2:27:08 PM] keith [redacted] yes.
[2:27:14 PM] [redacted] can we talk?
[2:27:16 PM] keith [redacted] Im in 12-3 interviewing people....
[2:27:20 PM] keith [redacted] yeah
[2:27:23 PM] keith [redacted] sure
[2:27:26 PM] [redacted] when?
[2:27:29 PM] keith [redacted] but it will have to be later.
[2:27:36 PM] keith [redacted] is it quick?
[2:27:59 PM] [redacted] maybe not. its about the c-17 investigation
[2:30:45 PM] keith [redacted] Oh. I know nothing.
[2:30:47 PM] keith [redacted] :)
[2:31:20 PM] keith [redacted] I have 3 interviews this afternoon with a 1/2 hour in between. I can call you when Im done....5:30
[2:31:22 PM] [redacted] I know. :) But, I'd still like to talk abou it.
[2:31:34 PM] [redacted] ok. that's fine.
[2:32:05 PM] keith [redacted] I will call when Im dont.
[2:32:07 PM] keith [redacted] done
[2:32:12 PM] [redacted] ok thx

a. As reflected in the data provided by Boeing, all of the individual chat messages were sent within seconds of each other, with the exception of Gartenlaub's reply to [redacted] when [redacted] wrote that he wanted to discuss the C-17 investigation. Gartenlaub did not respond to that message until approximately three minutes later with the message "Oh. I know nothing. :)" I understand the "emoticon" or "smiley face" of ":)" to mean Gartenlaub was being sarcastic or kidding when he wrote that he did not know anything. Based on that, I believe that he did in fact know something, and that this alluded to prior communications about the C-17 investigation.

b. During each of the interviews on February 7, 8, and 22, 2013, Gartenlaub was advised to not discuss this investigation, as was [redacted].

33. On May 10, 2013, [redacted] sent another e-mail to Gartenlaub which stated that there was additional C-17 data missing and asked: "who do we notify that released data is being compromised." [redacted] also wrote: "Someone is moving data around and causing problems." Gartenlaub forwarded the e-mail from [redacted] to [redacted] requesting he look into the compromise instead of reporting it to Boeing security. Gartenlaub has not reported this information to me or the other FBI Special Agent who interviewed him regarding this evidence of C-17 files being compromised.

E. Investigation of Technical and Forensic Evidence

34. On May 21, 2013, another FBI agent and I interviewed [redacted], at his office at Boeing in Long Beach, California. During the course of that interview, I learned the following from [redacted]:

a. [redacted] is a software developer on the [redacted]. [redacted] stated that certain personal on the [redacted] have access to the Unix servers, which in turn access the SAN device that contains the part files for the C-17. (The Unix servers are the computers that access the SAN. The SAN is a large set of disk arrays or groups of hard drives,

and the Unix computers access the SAN similar to the way a desktop computer accesses a hard drive.) [redacted] personal use the [redacted] to access the C-17 part files. [redacted]

b. [redacted] stated that Gartenlaub had been the application team administrator since 2011 but is currently the infrastructure manger for all Unix military servers nationwide. [redacted] stated that since Gartenlaub is the Unix military infrastructure manager, he would know about the [redacted] and most likely know the password. If Gartenlaub did not know the current [redacted] password for a particular server, it would be part of his normal day to day job to ask for the current password. Additionally, Gartenlaub would know how to log into the C-17 Unix servers to view the C-17 part data but that is not part of his day to day job description. (Additionally, according a resume of Gartenlaub provided by Boeing Internal Investigators, one of Gartenlaubs job responsibilities since 1998 is Unix/Linux/Windows system administration.)

35. The May 31, 2013 ainonline.com article described above in paragraph 16 referred to the C-17, as well as the P-8, the V-22, and the F/A-18 Super Hornet/Growler, and Boeing performs at

least some work on each of those projects, and they are all military projects. Based on the information provided during the interview of [redacted], Gartenlaub would have access to the servers containing the files regarding how to build these military projects.

36. Based on this information, the user of the [redacted] may be by different persons who need access to the Unix databases to perform their duties. Therefore, if there were records of the [redacted]

37. I have also requested logs of the [redacted] application. Although Gartenlaub currently does not administer that application, he previously developed the application and had access to it in connection with those responsibilities. I learned that Boeing does not maintain logs of that device for more than 90 days, and that Gartenlaub did not have an active login for the [redacted] application during that period of time.

38. Although the Unix server for the C-17 files (which could be accessed using the [redacted]) have access logs, I know from my training, experience, and education that the logs of access and activity on [redacted]. Therefore, anyone with a working knowledge of Unix who

wanted to conceal which files have been accessed and when he or she did what would be able to erase the evidence of that access and activity. Furthermore, someone that knew the [redacted] login was used by multiple people--which Gartenlaub knows--would also know that it was difficult to attribute any activity while logged into the [redacted] account.

39. I have requested information from Boeing regarding the logs reflecting activity and access surrounding the February 19, 2013 e-mail and the May 10, 2013 [redacted] e-mails to Gartenlaub regarding compromise and movement of C-17 files that were brought to Gartenlaub's attention.

40. There is one other person, [redacted] who works on Gartenlaub's team and has similar access, travels to China, and does not have a security clearance. He does not, however, based on his current employment at Boeing, his day-to-day job responsibilities involve administering databases, not setting up network infrastructure and architecture. Based on that difference in responsibility and expertise, and Gartenlaub's behavior discussed herein and summarized below in paragraphs 56-57, Gartenlaub remains the primary subject of this investigation.

F. Gartenlaub's Associations with the PRC

41. On May 6, 2013, Yi at [redacted] sent an email with an attached photo to Gartenlaub at keith.p.gartenlaub@boeing.com. The attached photo depicted Keith and Tess Gartenlaub sitting around a table at a party subsequently identified associate's house, named [redacted] The metadata contained on the photo indicated it was taken on March 13, 2013. In the photograph, Gartenlaub is dressed in a white collared shirt, red scarf, red arm sash with Chinese characters, and a black cross-body strap. Tess Yi is wearing a red scarf and a white arm patch with two red "bars" within it. Both Keith Gartenlaub and Tess Yi are smiling.

42. Based on open source materials I have reviewed, I learned that the red scarf, white shirt, and black pants are typical dress uniforms of the Young Pioneers of China and worn by children commemorating various nationalistic holidays in the PRC. The scarf is the color red to commemorate the blood of the revolutionaries who fought for China's freedom in pre-1949. The triangular shape represents a corner of the Chinese flag. In the Young Pioneers constitution, it explains that the scarf corresponds to the missing triangle on the medium detachment flag. The constitution also explains that the red of the scarf comes from the blood sacrificed by martyrs of the Revolution, and that all members should therefore wear the scarf with

reverence. The young pioneers of China are run by the Communist Youth League, an organization of older youth that comes under the Communist Party of China. The white patch with red bars signifies rank within the Communist Youth League. The young pioneers group is a starting point which can lead to full communist party member status as an adult. According to a Wall Street Journal posting, three bars are traditionally the most that the organization's highest ranking leaders are allowed to wear. Below is a copy of the photo received by Gartenlaub, which shows Tess Yi wearing a badge with two stripes.

G. Financial Investigation

43. Keith Gartenlaub and Tess Yi have joint or individual bank accounts at the following financial institutions: Industrial Bank of China, Bank of America (BOA), Navy Federal Credit Union, First Bank, and TD Ameritrade. Analysis of bank statements for Gartenlaub and Yi's joint BOA account from August 2009 to December 2012 showed that there were 61 ATM deposits totaling $58,628.26. The BOA analysis also revealed 6 non-ATM deposits totaling $14,374.63. Additionally, a BOA bank statement from November 2009 revealed a $25,000 international wire transfer from Tess Yi at Industrial Bank of China to Gartenlaub and Yi's BOA account. Additionally, analysis of statements for Gartenlaub and Yi's TD Ameritrade accounts revealed $18,500 in additional deposits in their TD Ameritrade accounts during the same date range.

44. FBI LA believes that Gartenlaub and Yi were compensated for assisting in the intrusion via cash payments. FBILA believes Gartenlaub and Yi have been slowly depositing the cash into multiple bank accounts and transferring the money to other accounts in order to hide the source of the funds.

45. According to Yi's resume, which I obtained from a Boeing Internal Investigator in May 2013, between September 2005 and March 2006 Yi worked for Commercial Capital Bank as a customer service representative. Between April 2006 and July

2008, Yi worked for East West Bank as a personal banker. Through her employment, Yi would have been familiarized with bank reporting requirements and how to hide her banking activity.

46. Based on information received from Bank of America (BOA), on August 31, 2006, Tess Yi requested to purchase a $5,000 cashier check with cash. When Yi was told of the monetary instrument sales log form that would need to be filled out, she requested not to fill out the form and changed the check amount to $2,999. BOA also provided documents showing that between December 1, 2005 and January 17, 2007, Yi negotiated approximately 329 transactions for a total o $190,803 in combined debit and credit activity. In that period of time, Yi also deposited approximately $23,855 in cash and 32 checks and/or debits for a total of $40,159.

47. In May 2013, Boeing Internal Investigator provided an e-mail and attachment sent by a real estate broker to Tess Yi at [redacted], the [redacted]. Tess Yi forwarded it to Gartenlaub's Boeing email account. Attached to the e-mail to Tess Yi was a real estate purchase contract for a house in Las Vegas, Nevada on May 6, 2013 for $85,000. Tess Yi is the only listed buyer. It listed the purchase in cash. According to a recent resume, Tess Gartenlaub has been unemployed since 2008. In an e-mail obtained from Boeing,

Gartenlaub wrote his wife Tess Yi regarding "paperwork," and wrote that he wanted to talk to her about two things: "What should I list your occupation as? And your employer?" and ""Should we put in the China property as an asset since we still have some payments left on the loan?"

48. I also know from Boeing internal investigations that Tess Yi recently opened an antique store located at 1968 South Coast Highway, Laguna Beach, California. I have also learned that the storefront where she has the store is rented, not owned by her. Information I have received from Boeing regarding Gartenlaub's use of his Boeing computer showed that on a California Board of Equalization document, Gartenlaub listed the antique store's supplier of inventory as the business right next door. This business next door's name is Khyber Pass and is located at 1970 South Coast Highway, Laguna Beach, California.

49. Based on the fact that Keith Gartenlaub and Tess Yi are arranging to sell real estate in the United States, and Keith Gartenlaub specifically set up the ability to wire transfer funds online internationally from his Bank of America account, I believe Keith Gartenlaub and Tess Yi may be liquidating their assets in order to be able to leave the United States. Based on chats that Gartenlaub had with his supervisor in Washington State, I learned that Gartenlaub indicated he was interested in moving to Boeing's facility in South Carolina,

although he was equivocal regarding expressing preference for southern California based on what he believed his wife's preference was.

H. Use of the GARTENLAUB SUBJECT ACCOUNT

50. The GARTENLAUB SUBJECT ACCOUNT, kgartenlaub@yahoo.com, is used by Keith Gartenlaub at work and at home based on information provided by Boeing regarding the use of his Boeing-issued laptop computer. Information obtained from a court-authorized pen register and trap and trace device shows that he is in contact with a China based email account using a Shanghai IP address seven times since March 2013. The GARTENLAUB SUBJECT ACCOUNT is also used to communicate with his wife, as reflected in the results of a pen register and trap and trace device. E-mails are also forwarded from Gartenlaub's Boeing e-mail account to the GARTENLAUB SUBJECT ACCOUNT, evidence of which exists on the results of the data pen and trap and trace device.

51. I have also reviewed the records provided by Skype for the account subscribed to Keith Gartenlaub. Those records showed that in the period of April 2011 to March 2013, the account contacted other accounts based in China approximately once every three days, on average. (Gartenlaub was interviewed on February 7, 8, and 22, 2013). After Gartenlaub was contacted by the FBI to set up an interview, the Skype account subscribed

to Gartenlaub contacted accounts based in China approximately three times per day, on average.

I. Use of the [redacted]

52. Subscriber records for the [redacted], shows that it is subscribed to Tess Yi (her maiden name). Tess Gartenlaub's cell phone voicemail states that "You have reached Tess Treasures." The [redacted] received the Fish Fork email discussed above in paragraph 29, and then forwarded it to Gartenlaub's Boeing e-mail account. The [redacted] is in frequent contact with Gartenlaub's e-mail accounts and with Chinese e-mail addresses (such e-mail addresses ending in 163.com or .cn, which I know based on my training and experience to be domains used in China) [redacted].

J. Use of the [redacted]

53. The [redacted], was used to email the Fish fork part pictures to Tess Gartenlaub, as described above in paragraph 29. Based on the fact that the user of this account e-mailed the photographs to Tess Gartenlaub, I believe that the user of the account knew that

Tess Gartenlaub would be able to consult with her husband, Keith Gartenlaub, in order to gain additional information or technical details regarding the Fish Fork. Nothing in Tess Yi's resume indicates that she has any training, experience, or education that would equip her to provide any helpful insight into the operation or details of the Fish Fork.

54. In addition to the March 9, 2013 e-mail regarding the Fish Fork, Tess Yi and [redacted] have been in email communications 3 other times: twice on March 13, 2013, and once on April 27, 2013). Also, since February 8, 2013, Tess Yi, using her cell phone on which a pen register and trap and trace device has been used, has been in telephonic contact with the user of this e-mail account, which was connected to [redacted] by means of both searches on Facebook and on Choicepoint/Clear. They have been in telephone contact 21 times since February 8, 2013.

K. Summary of Evidence

55. For the reasons set forth above, I believe that there is evidence of a conspiracy to gain or provide unauthorized access to Boeing's computer systems housing an export-controlled military cargo plane and other military technology residing there on the SUBJECT ACCOUNTS. Keith Gartenlaub is positioned with unique access to an knowledge of the C-17 and other projects, and his communications with his wife Tess Yi, and in

turn her communications with the user of the GMAIL SUBJECT ACCOUNT (subscribed to [redacted]), show their knowledge of his position as a Boeing engineer willing to consult on Chinese military projects.

56. Specifically, Gartenlaub is the Unix administrator for all Boeing military projects, has access to the [redacted], has a technical knowledge of the network structure, and is familiar with the files, parts, and structure of the C-17 materials:

a. For example, although above in paragraph 22.c it states that the [redacted] allows "the Air Force, Boeing, and selected suppliers and contractors to access all of the C-17 data in both the Teamcenter and [redacted] databases," those do not allow direct access into the Unix servers that manage the SAN device where the actual part files with descriptive information about how to build them is contained;

b. The [redacted] application that can access the C-17 files has extensive logging and data retention of those logs, [redacted]. The Unix server has generic logins shared by multiple people which makes it difficult to attribute user activity, all of which I believe Gartenlaub is aware, based on his experience, education, and my conversations with him;

c. [redacted]

d. Furthermore, the number of people who have access to the full set of actual files that are needed to build the C-17 is limited to 23 people plus the approximately 12 people who [redacted]. Although other personnel work on other aspects of the network, even [redacted], the administrator for the database that is used to locate those files, does not even have access to the files themselves, as set forth above in paragraph 20.a;

e. As the person who developed the [redacted] application, Gartenlaub has a detailed familiarity of the network architecture because the application is used to access the C-17 parts by users who are granted access to particular parts on which they are authorized to work and given access; and

f. Gartenlaub stated that there are less than five people at Boeing that understand how the C-17 network is setup and also has administrative access to access the data. Gartenlaub stated that his position is unique.

57. Significant for this investigation, Gartenlaub has avoided providing information that is salient for the investigation, has not followed instructions not to discuss the

investigation, and has exhibited behavior consistent with concealment or possibly flight:

a. The day he was interviewed by FBI, he established the ability to send international wire transfers in excess of $1,000;

b. His contact with Chinese-based Skype accounts spiked as soon as he was contacted by the FBI about the C-17 investigation;

c. He received a request for advice on the Fish Fork, a device used for landing helicopters on warships, from a Chinese-based e-mail account through his wife, an area squarely outside his duties and responsibilities;

d. Although he had been questioned three times about the C-17 project and a potential compromise of the data, he did not bring to my or the other FBI Special Agent's attention instances in February 2013 (three days before he was interviewed the third time) and May 2013 regarding the "compromise" of C-17 files that had gone missing or were not where they belonged. This is particularly significant because based on my conversations with Gartenlaub, I know he is technically very proficient, and he understood the nature of the investigation, and that information regarding missing or compromised files would be relevant to investigating whether any of the files had been improperly accessed and by whom; and

e. Although he had been advised not to discuss the C-17 investigation, he responded in a chat to [redacted] when asked to talk specifically about the C-17 investigation "I know nothing. :)," indicating that he in fact does know something about it;

f. Gartenlaub said that until approximately 2011, only one form of authentication was necessary to remotely access Boeing's network via VPN. I have learned from other employees that two factors of authentication were in fact required even before 2011. That is significant because Gartenlaub would know that to investigators researching an unauthorized access, a compromise of an employee's login or credentials could be used to gain access to the Boeing network, even if the person to whom those credentials belonged was not aware of that abuse. With two factor authentication, ongoing contact with the person whose credentials were used would be necessary in order to continue to have access for the period of time it would take in order to copy the entire C-17 project's files; and

g. The PSO never trusted Gartenlaub, Gartenlaub was always a concern for the security personnel, that Gartenlaub felt he was above the rules, and that she felt it was a loss to the C-17 project when he transferred to it.

L. Extent and Concealment of Illicit Collection Activities

58. As set forth in this affidavit, the FBI is continuing to investigate the identities of the individuals that are responsible for the illicit secreting of technical information from the United States, as well as the scope of their conduct. Furthermore, based on my training and experience, I know that persons engaged in such conduct often engage in various layers of subterfuge concerning their identities and e-mail accounts as well as the true nature and purpose of their activities. I also believe, based on my training and experience, discussions with agents trained in computer and internet issues, and the facts set forth above, that e-mail subscribers sometimes keep items in their e-mail accounts for extended periods of time, even years, in accounts which remain active. Because one of the primary purposes of the investigation at this point is to identify the individual(s) responsible for the illicit secreting of technical information, I therefore request that the PROVIDERS provide the entire content for the SUBJECT ACCOUNTS since inception until the time the requested warrant is served on them, and that the items to be seized set forth in detail below permit law enforcement to seize such items without limit as to time in order to assist in identifying the individuals participating in this scheme and their activities.

59. Based on my training and experience, I also know that networks and hierarchies involved in illicit secreting of national defense information are often extensive and have many layers. Often times certain individuals involved in acquiring the information or directing its acquisition may not be actively engaged in directing a particular step of the procurement, but are kept informed, often by receiving or sending carbon copying ("cc'ing") others on e-mail communications. In order to fully identify the extent and nature of the network, it is important to obtain e-mail communications that may not show participation by the user of a particular account, but that will help identify that person and their role in the network. I also know that a user's e-mail account can include photographs or other notes in the contact list or address book regarding who the user is in contact, information that is either automatically imported from other social media sites or data files or actively entered by the user of the e-mail account. Therefore I request authority to seize documents related to the identity of the user of any e-mail account included on communications relevant to the collection and acquisition of national defense information described herein.

III.

BACKGROUND REGARDING E-MAIL AND THE PROVIDER

60. In my training and experience, I have learned that the PROVIDER provides a variety of online services, including e-mail, to the public. The PROVIDER allows subscribers to obtain e-mail accounts at the domain names yahoo.com and ymail.com like the SUBJECT ACCOUNTS. Subscribers obtain an account by registering with the PROVIDER. During the registration process, the PROVIDER asks subscribers to provide basic personal information. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNTS.

61. A subscriber of the PROVIDER can also store with the PROVIDER files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and

experience, evidence of who was using an e-mail account may be found in such information.

62. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNTS.

63. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol

("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNTS.

64. In my training and experience, e-mail account users will sometimes communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNTS.

65. I know from my training and experience that the complete contents of an e-mail account may be important to establishing the actual user who has dominion and control of that account at a given time. E-mail accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which e-

mail accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an e-mail account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search for information showing the actual user of the account would, in some instances, prevent the government from identifying the user of the account and, in other instances, prevent a defendant from suggesting that someone else was responsible. Therefore, the complete contents of a given account, including the e-mail addresses and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of the SUBJECT ACCOUNTS, I am requesting a warrant requiring the PROVIDER to turn over all information associated with the SUBJECT ACCOUNTS without a date restriction for review by the search team.

66. Relatedly, the government must be allowed to determine whether other individuals had access to the SUBJECT ACCOUNTS.

If the government were constrained to review only a small subsection of an e-mail account, that small subsection might give the misleading impression that only a single user had access to the account.

67. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as lol to express "laugh out loud"), or codewords (which require entire strings or series of e-mail conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an e-mail or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an e-mail account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

68. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER under seal until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for the PROVIDER to authenticate information taken from the SUBJECT ACCOUNTS as its business record without the original production to examine. Even if the PROVIDER kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the PROVIDER to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the PROVIDER to examine a particular document found by the search team and confirm that it was a business record of the PROVIDER's taken from the SUBJECT ACCOUNTS.

b. I also know from my training and experience that many e-mail accounts are purged as part of the ordinary course of business by providers. For example, if an e-mail account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an e-mail account might be the production that a provider makes to the government, for

example, if a defendant is incarcerated and does not (perhaps cannot) access his or her e-mail account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

IV.

REQUEST FOR NON-DISCLOSURE

69. Pursuant to Title 18 United States Code, Section 2705(b), I request that the Court enter an order commanding the PROVIDERS not to notify any person, including the subscriber(s) of the SUBJECT ACCOUNTS, of the existence of the warrant because there is reason to believe that such notification will result in (1) destruction of or tampering with evidence; (2) intimidation of potential witnesses; (3) otherwise seriously jeopardizing the investigation; or (4) unduly delaying trial. Specifically, although Gartenlaub has been interviewed, he has not been made aware that he is the subject of the investigation. Revealing that he is the subject may cause him to . If the subjects learned that they were under investigation or that the contents of their e-mail accounts were going to be seized as evidence, they would likely delete the contents of their e-mail accounts, destroy other evidence, and begin using other e-mail accounts that would be difficult to discover. In addition, if the PROVIDER or other person notifies the targets of the

investigation that a warrant has been issued for the SUBJECT ACCOUNTS, the subject will further mask their activity and seriously jeopardize the investigation.

V.

CONCLUSION

70. Based on the foregoing, I request that the Court issue the proposed search warrant.

/s/
WESLEY K. HARRIS
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 18, 2013.

ANDREW J. WISTRICH
HONORABLE ANDREW J. WISTRICH
UNITED STATES MAGISTRATE JUDGE

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

CERTIFICATE OF SERVICE
SEALED DOCUMENTS
INTERIM CIRCUIT RULE 27-13

Case Number: 16-50339

Case Title: United States of America v. Keith Gartenlaub

Note: Documents to be filed under seal are to be submitted electronically. As the parties will not have online access to those documents once they are submitted, the CM/ECF electronic notice of filing will not act to cause service of those documents under FRAP 25(c)(2) and Ninth Circuit Rule 25-5(f). Interim Circuit Rule 27-13(c) therefore requires an alternative method of serving the motion or notice to seal and the materials to be sealed.

○ I certify that I have provided a paper copy of the document(s) listed below to all other parties via personal service, mail, or third-party commercial carrier on the date noted below. *See* FRAP 25(c)(1)(A) – (C).

◉ I certify that, having obtained prior consent, I have provided a copy of the document(s) listed below to all other parties via electronic mail. *See* FRAP 25(c)(1)(D); Interim Circuit Rule 27-13(c).

DESCRIPTION OF DOCUMENTS:

(1) Motion to Seal Exhibit C to Defendant's Motion for Bail Pending Appeal
(2) Exhibit C to Defendant's Motion for Bail Pending Appeal---Public Redacted Version
(3) Notice of Intent to File Publicly re: (2)

Signature: /s/ Vicki Chou

(use "s/" format with typed name)

Date: November 18, 2016