UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

FILED
CHARLOTTE, NC

AUG - 8 2013

US District Court
Western District of NC

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Content and forensic images of email account as described in Affidavit and Attachment, incorporated herein.	))))))	Case No.

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, which is incorporated fully herein.

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

See attachment B which is incorporated fully herein.

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	*Offense Description*
18 U.S.C. 1924	Unauthorized removal and retention of classified documents and materials.
18 U.S.C. 793(e)	Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

☑ 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.

(SA) Raju S Bhatia
Applicant's signature

Raju S. Bhatia Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 8.8.13

Robert J. Conrad
Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr., United States District Court Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Raju S Bhatia, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account stored at premises owned, maintained, controlled, or operated by United States Central Command (US CENTCOM) headquartered at MacDill Air Force Base, Tampa, Florida. The information to be searched is described in the following paragraphs and in Attachment A, all incorporated fully by reference herein.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for over 14 years. I have investigated matters involving complex financial fraud, public corruption, organized crime, counterterrorism, and counterespionage. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received training in the proper collection, retention, and dissemination of classified information.

3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [redacted], for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.

5. For the reasons set forth below, there is probable cause to believe that the email account [redacted] (described in detail in Attachment A) contains evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the improper communication and/or retention of classified information.

6. Title 18, United States Code, Section 1924(a) states:

> Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

> Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates,

> delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.

9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about June 23, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. To obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

12. [redacted] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [redacted] held a United States government security clearance allowing her access to classified United States government information. To obtain that clearance, [redacted] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

13. In June 2012, the FBI's Tampa Division (FBI Tampa) opened a computer intrusion investigation related to alleged cyber stalking activity. This investigation was predicated

on a complaint received from Witness 1, which alleged the receipt of threatening and harassing emails. Witness 1 claimed friendships with several high-ranking public and military officials.

14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that [redacted] was the individual who had sent the emails to Witness 1.

15. On September 24, 2012 as part of the FBI Tampa investigation, [redacted] consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which were identified by Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.

16. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with [redacted]. He denied providing any classified documents to [redacted], or having any arrangement to provide her

with classified information. PETRAEUS stated that [redacted] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [redacted], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

17. On November 2, 2012, FBI Tampa interviewed [redacted], in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [redacted] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [redacted] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [redacted] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [redacted] advised that she never received classified information from PETRAEUS.

18. During interviews conducted of [redacted] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not

known if all the accounts were identified because both [redacted] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [redacted] September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

19. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [redacted] residence in [redacted], North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital media as well as four boxes and one folder of documents. On this same date, [redacted] administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with [redacted]. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.

20. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. [redacted] traveled into and out of Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.

21. [redacted] paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting [redacted] access to classified information for the

purpose of writing his biography. For example, in an email dated January 16, 2011, which PETRAEUS marked as CONFIDENTIAL and sent to multiple members of the military, he instructed a member of his staff to "PLS PRINT FOR [redacted], ON AN OFF THE RECORD BASIS." Travel documents show that [redacted] was in Afghanistan at this time.

A. Communications Regarding Potential Mishandling of Classified Information

22. On July 13, 2011, [redacted] and a U.S. Army Captain exchanged several emails. [redacted], using email account [redacted] emailed the Captain at his military email account, seeking information about military operations. In an email to the Captain, in which PETRAEUS was carbon copied (cc'd) at email account [redacted], [redacted], wrote, "If it's ok with you, may I trouble you to send the storyboards (via SIPR[1]) directly to GEN Petraeus (copied here) and he will print them out for me? (He is gracious and willing to help out given my compressed timeline!)" PETRAEUS followed up to this email by writing to the Captain and [redacted], "Happy to help, [redacted], if my SIPR account would be convenient. It's on the main address list. We decided [redacted] was serious and have sought to help…" The Captain replied to PETRAEUS's email, "Sir, I will be happy to send these on SIPR to your account for [redacted]…" Based on my training, experience, and information reviewed to date in this investigation, the email chain related to a document or series of documents provided by PETRAEUS to [redacted] which contained classified information. This

[1] SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

email correspondence between [redacted], and the Captain reflects some agreement by PETRAEUS to provide [redacted] access to classified information.

23. Between July 13, 2011 and July 15, 2011, [redacted], and a U.S. Army Lieutenant Colonel exchanged numerous emails. [redacted], using email account [redacted], emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [redacted] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [redacted], on July 15, 2011, he advised he was working on the storyboards and asked her for "a good SIPR number." Later on July 15, 2011, [redacted] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [redacted]. [redacted] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [redacted], and the Lieutenant Colonel reflects some agreement by PETRAEUS to provide [redacted] access to classified information.

24. Based on these facts, there is probable cause to believe that PETRAEUS's email account, [redacted], contains substantive communications regarding PETRAEUS's sharing of classified information as well as [redacted] access to and retention of classified information.

BACKGROUND CONCERNING EMAIL

25. In my training and experience, I have learned that US CENTCOM provides electronic mail ("email") access to uniformed and civilian employees. These users are provided an email account for use in their official duties. Consequently, US CENTCOM computers are likely to contain stored electronic communications (including retrieved and unretrieved email for US CENTCOM users) and information concerning users and their use of US CENTCOM services. This information would include details regarding users of US CENTCOM service, such as the user's full name, physical locations, telephone numbers and other identifiers, account access information, email transaction information, and alternative email addresses. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. In general, an email that is sent to a CENTCOM subscriber is stored in the subscriber's "mail box" on CENTCOM servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on CENTCOM servers indefinitely.

27. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to CENTCOM servers, and then transmitted to its end destination. CENTCOM often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the CENTCOM server, the email can remain on the system indefinitely.

28. A CENTCOM subscriber can also store files, including emails, files and other data, on servers maintained and/or owned by CENTCOM.

29. Subscribers to CENTCOM might not store, on their home computers, copies of the emails stored in their CENTCOM account. This is particularly true when the subscriber accesses their CENTCOM account through the web, or if they do not maintain particular emails or files in their residence or on their home computer.

30. In my training and experience, email 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 log-in (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, email providers often have records of the Internet Protocol address ("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 email account.

31. In my training and experience, in some cases email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email 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. Such information may

constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

LOCATION TO BE SEARCHED

32. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the requested warrant to require US CENTCOM to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, the information described in Attachment B will be subject to seizure by law enforcement.

33. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information associated with a certain account, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by US CENTCOM, headquartered at MacDill Air Force Base, Tampa, Florida, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

CONCLUSION

34. Based on my training and experience, and the facts as set forth in this affidavit, your affiant asserts there is probable cause to believe that stored in the email account, [redacted], there exists evidence of a crime relating to: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

35. Based on the foregoing, I request that the Court issue the requested search warrant. Because the warrant will be served on US CENTCOM, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

36. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711; and Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offenses being investigated," Title 18, United States Code, Sections 1924, 793(e), and 371. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

37. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,

Raju S Bhatia
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 8th day of August, 2013.

ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Account To Be Searched

This warrant applies to records and other information (including the contents of communications) for the account associated with the email address [redacted]_____ that is stored at premises controlled by US Central Command, which accepts service of legal process at MacDill Air Force Base, Tampa, Florida.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by CENTCOM ("the Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the account listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, and log files;

c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

d. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized by the Government

1. All records or information described above in Section I that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including, for the account identified on Attachment A:

    a. All records or information related to any communications between PETRAEUS and [redacted];

    b. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;

    c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;

    d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided by PETRAEUS to [redacted];

    e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;

    f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

    g. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;

h. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS or [redacted];

i. Any information recording PETRAEUS's or [redacted] schedule or travel from December 2008 to the present;

and

j. Records evidencing the use of the Internet, including records of Internet Protocol addresses used;

2. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.