

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: **<http://www.theblackvault.com>**



U.S. Department of Justice

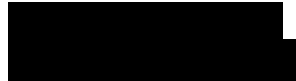
*Executive Office for United States Attorneys
Freedom of Information Act & Privacy Act Staff*

*Bicentennial Building
600 E Street, NW, Suite 7300
Washington, DC 20530*

*(202) 252-6020
(202) 252-6047 Fax*

May 12, 2017

John Greenwald, Jr.
The Black Vault



john@greenwald.com

Re: Request Number: EOUSA-2017-001076

Date of Receipt: April 5, 2017

Subject of Request: Petraeus Investigation – Records Pertaining to Civil Action No. 16-cv-00514

Dear John Greenwald, Jr.,

Your Freedom of Information Act/Privacy Act request for records released in the above-referenced action has been processed. This letter constitutes a reply from the Executive Office for United States Attorneys, the official record-keeper for all records located in this office and the various United States Attorneys' Office.

To provide you with the greatest degree of access authorized by the Freedom of Information Act and the Privacy Act, we have considered your request in light of the provisions of both statutes.

The records you seek are located in a Privacy Act system of records that, in accordance with regulations promulgated by the Attorney General, is exempt from the access provisions of the Privacy Act. 28 CFR § 16.81. We are making available to you documents that have been released in a previous FOIA request.

The exemption(s) cited for withholding records or portions of records are marked below. An enclosure to this letter explains the exemptions in more detail.

List of Exemptions:

b5
b6
b7C

For your convenience, we are also providing you with a direct link to the location of the recently unsealed search warrants located on the U.S. Attorney for the Western District of North

Carolina's website. The link to the website is: <http://www.ncwd.uscourts.gov/news/documents-released-general-petraeus>.

This is the final action on this above-numbered request. If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, DC 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following website: <https://foiaonline.regulations.gov/foia/action/public/home>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

You may contact our FOIA Public Liaison at the telephone number listed above for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Enclosure(s)

Sincerely,



Kevin Krebs
Assistant Director

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

FILED
CHARLOTTE, NC

DEC 20 2016

US District Court
Western District of NC

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT OF EMAIL ACCOUNT AS
DESCRIBED IN AFFIDAVIT AND
ATTACHMENTS, INCORPORATED
HEREIN.

) DOCKET NO.: 3:13-mj-100

) MOTION TO UNSEAL THE
) SEARCH WARRANT, AFFIDAVIT
) AND APPLICATION

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on April 4, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

//s//JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY
NC Bar Number # 17656

Attorney for USA
Carillon Bldg, Suite 1700
227 West Trade Street
Charlotte, NC 28202
Phone: 704-344-6222
Fax: 704-344-6629
Email: jill.rose@usdoj.gov

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT OF EMAIL ACCOUNT, AS
DESCRIBED IN AFFIDAVIT AND
ATTACHMENTS, INCORPORATED
HEREIN.

) DOCKET NO.: 3:13-mj-100

)

) **ORDER TO UNSEAL THE**

) **SEARCH WARRANT, AFFIDAVIT**

) **AND APPLICATION**

)

)

)

)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on April 4, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.


UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Content of email account, as described in Affidavit and
Attachments, incorporated herein.

Case No. 3:13mj100

Certified to be a true and
correct copy of the original
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By: B. Trucking
Deputy Clerk
Date: 4/4/13

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):
See Attachment B, which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before April 17, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been
established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____

Date and time issued: 4.3.13, 5:30 p.m.

Robert J. Conrad, Jr.
Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

Return

Case No.: 3:13mj100	Date and time warrant executed:	Copy of warrant and inventory left with:
---------------------	---------------------------------	--

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

FILED
CHARLOTTE, NC

APR 4 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 of email account, as described in Affidavit and
Attachments, incorporated herein.

Case No. 3:13-mj-100

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 USC 1924; 18 USC 793(e);	Unauthorized removal and retention of classified documents or material;
18 USC 371	Unauthorized possession, communication, and willful retention of national defense information; Conspiracy

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.

Certified to be a true and
correct copy of the original.
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By: B. Fickling
Deputy Clerk
Date: 4/4/13

Gerd J. Ballner
Applicant's signature

Gerd J. Ballner, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/03/2013

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.
Judge's signature

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

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Gerd J. Ballner, Jr., 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 Yahoo! Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, California 94089. 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 approximately thirteen years. I have investigated matters involving National Security to include Counterintelligence and Espionage. 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 hostile foreign intelligence services and their recruited human sources to illegally obtain, through clandestine action, classified and proprietary information, which if compromised poses risk to the national security of the United States. I have also received specialized 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 [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. David 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 July 4, 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. According to a Department of Defense (DOD) official, 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. According to a DOD official, 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 from the email addresses [REDACTED] and

[REDACTED] 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 David 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.

15. Investigation conducted by FBI Tampa identified [REDACTED] as the person suspected of using the email accounts [REDACTED] and [REDACTED]. Investigation also determined [REDACTED] uses the email account [REDACTED]. On September 24, 2012, FBI Tampa interviewed [REDACTED] at her residence. During this interview [REDACTED] admitted sending the emails to Witness 1, as well as other emails regarding Witness 1 to senior United States military officers as well as a foreign diplomat. [REDACTED] also stated that she

engaged in an extramarital affair with Petraeus. [REDACTED] provided consent to search two of her laptop computers and two external hard drives.

16. On September 25, 2012, FBI Tampa returned [REDACTED] laptop computers and conducted a follow-up interview. During this follow-up interview, [REDACTED] admitted she told Petraeus that he should get Witness 1 to "drop the charges."

[REDACTED] advised she does not know if Petraeus made the request of Witness 1.

During the course of this interview, [REDACTED] provided interviewing agents consent to search her Apple iPhone, which she had in her possession. FBI Charlotte Computer Analysis Response Team (CART) Forensic Examiners copied the contents of her Apple iPhone at the interview location, and the iPhone was returned to [REDACTED] at the conclusion of the interview. A review of [REDACTED] laptops and external hard drives located over 100 items which were identified by Charlotte CART Forensic Examiners as containing potentially classified information, including information up to the Secret level.

17. 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.

18. 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.

19. During interviews conducted of [REDACTED] and Petraeus under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with one another. 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.

A. [REDACTED] Consensual Search, November 12, 2012

20. As a result of finding potentially classified information on the laptops provided by [REDACTED], FBI Tampa and FBI Charlotte conducted a consensual search of [REDACTED] Charlotte residence on November 12, 2012 to recover any evidence related to cyber stalking, in violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents or material, in violation of 18 U.S.C. § 1924. On this same date, a consensual search was also conducted at the residence of [REDACTED] administrative assistant, [REDACTED], in Concord, North Carolina. [REDACTED] voluntarily provided the FBI with various items she maintained in her home in relation to her employment with [REDACTED]. During the searches, additional paper documents were found, some of which, upon belief and information of your affiant, are classified. As a result of the two searches, the following digital media were seized: eight computers, twelve external hard drives, two printers/scanners, two cellular telephones, two Apple iPods, seven thumbdrives/memory cards, and approximately fifty floppy discs, CDs, and optical discs.

21. Based on a preliminary review of [REDACTED] digital media, it is believed she came into possession of potentially classified information both before and during the writing of her book, "All In: The Education of General David Petraeus." Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. Given her extensive use of digital media, your affiant believes [REDACTED] received/exchanged classified information via email and/or made contact with individuals via email and/or telephone to schedule in-person meetings for the purpose of recording and collecting classified information, as detailed below.

[REDACTED] is also believed to have digitally stored numerous documents, photographs, and audio interviews which contain classified information.

B. Relevant Communications Regarding the Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED] sent an email to Petraeus at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, the email related to a document or series of documents provided by Petraeus to [REDACTED] which contained classified information.¹

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

¹ On June 27, 2012, FBI Tampa served a grand jury subpoena on Yahoo! for the [REDACTED] account. On June 29, 2012, FBI Tampa executed a search warrant on the account. On September 7, 2012, FBI Tampa obtained an additional search warrant on the account. Search warrant results received on October 16, 2012 included emails between the dates of July 1, 2012 and September 7, 2012. Because it is relevant to the current investigation what actions, if any, [REDACTED] took regarding the emails in the [REDACTED] account since the execution of the email search warrants by FBI Tampa, this affidavit seeks a search warrant requiring Yahoo! to disclose the entire contents of the account and not just the email content from September 7, 2012 to the present.

working on the storyboards and asked her for "a good SIPR number."² 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. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED], and Petraeus, using email address [REDACTED], discussed several topics, to include files maintained by Petraeus. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which Petraeus addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing Petraeus's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, Petraeus wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

² 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.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED] [REDACTED] the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."³ In response Petraeus wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, Petraeus, using email address [REDACTED] and [REDACTED], using email address [REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", Petraeus discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]. Petraeus wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about Petraeus's willingness to share the files writing: "[I]'ll protect them. And I'll protect you." Petraeus later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."⁴ Petraeus continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly

³ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

⁴ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

27. Your affiant believes that Petraeus's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

C. Continuing Communications Between [REDACTED] and Petraeus

28. [REDACTED] and Petraeus are believed to have had multiple telephonic contacts after each was made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:

- a. Petraeus's CIA security detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, Petraeus acknowledged that: (1) he was briefed by the security detail concerning the FBI investigation, and (2) he called [REDACTED] on June 23, 2012 regarding the emails received by Witness 1.
- b. Over the weekend of August 11, 2012 and August 12, 2012, Petraeus spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on August 11, 2012.
- c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on three occasions on September 25, 2012.
- d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3,

2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and Petraeus. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.

- e. During the October 26, 2012 interview of Petraeus by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to Petraeus called a telephone number attributed to [REDACTED] on October 16, 2012.
- f. Following FBI Tampa's interview of Petraeus on October 26, 2012, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.
- g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa. [REDACTED] stated that she and Petraeus had talked candidly since each of their interviews with the FBI.
- h. On November 9, 2012, [REDACTED] contacted FBI Tampa telephonically from telephone number [REDACTED]. She advised she received a telephone call from Petraeus earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number [REDACTED] called a telephone number attributed to Petraeus on November 9, 2012.

29. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to Petraeus. As detailed above,

Petraeus and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED] and Petraeus have admitted that they established covert communications systems using pre-paid cellular telephones and non-attributable email accounts. To date, the pre-paid telephone numbers used by Petraeus and [REDACTED] have not been identified.

30. These telephonic contacts and attempted telephonic contacts between telephone numbers attributed to [REDACTED] and Petraeus indicate [REDACTED] relationship with Petraeus continued after their interviews with FBI Tampa in September and October 2012. Based on these facts, and given [REDACTED] history of email communication with Petraeus, there is probable cause to believe that [REDACTED] Yahoo! account contains substantive communications regarding the content of [REDACTED] and Petraeus's FBI interviews, including additional information regarding [REDACTED] access to and retention of classified information.

BACKGROUND CONCERNING EMAIL

31. In my training and experience, I have learned that Yahoo! provides a variety of online services, including electronic mail ("email") access, to the general public. Subscribers obtain an account by registering with Yahoo!. During the registration process, Yahoo! requests subscribers to provide basic personal information. Therefore, the computers of Yahoo! are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo! subscribers) and information concerning subscribers and their use of Yahoo! services, such as account access information, email transaction information, and account application information. Such information can include the

subscriber's full name, physical address, telephone numbers and other identifiers, alternative email 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 account's user or users.

32. In general, an email that is sent to a Yahoo! subscriber is stored in the subscriber's "mail box" on Yahoo! servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Yahoo! servers indefinitely.
33. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Yahoo!'s servers, and then transmitted to its end destination. Yahoo! often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Yahoo! server, the email can remain on the system indefinitely.
34. A Yahoo! subscriber can also store files, including emails and other files, on servers maintained and/or owned by Yahoo!.
35. Subscribers to Yahoo! might not store on their home computers copies of the emails stored in their Yahoo! account. This is particularly true when they access their Yahoo! account through the web, or if they do not wish to maintain particular emails or files in their residence.
36. 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.

37. 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. 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.

LOCATION TO BE SEARCHED

38. 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 warrant to require Yahoo! 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.

39. 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 Yahoo! Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, California 94089, 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

40. 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 Yahoo! 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.

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

Because the warrant will be served on Yahoo!, 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.

42. 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

43. 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.

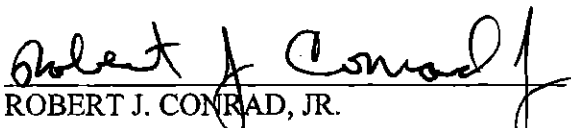
Respectfully submitted,



Gerd J. Ballner, Jr.
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me

on this, the 3 day of April, 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 Yahoo!, a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by Yahoo! ("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, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 16, 2012 and February 14, 2013, 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, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. 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

e. 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 [REDACTED] and Petraeus;
- b. All records or information related to any communications, from December 2008 to the present, between [REDACTED] 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 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 [REDACTED] 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 [REDACTED] or Petraeus;
 - i. Any information recording [REDACTED] or Petraeus's schedule or travel from December 2008 to the present;
 - j. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
 - k. 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.

DEC 20 2016

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

US District Court
Western District of NC

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT OF EMAIL ACCOUNTS;
FORENSIC IMAGES OF IPHONE, 2
LAPTOPS, AND 2 EXTERNAL HARD
DRIVES AS DESCRIBED IN AFFIDAVIT
AND ATTACHMENT, INCORPORATED
HEREIN.

) DOCKET NO.: 3:13-mj-101

) MOTION TO UNSEAL THE
) SEARCH WARRANT, AFFIDAVIT
) AND APPLICATION

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on April 4, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

//s//JILL WESTMORELAND ROSE

ASSISTANT UNITED STATES ATTORNEY

NC Bar Number # 17656

Attorney for USA

Carillon Bldg, Suite 1700

227 West Trade Street

Charlotte, NC 28202

Phone: 704-344-6222

Fax: 704-344-6629

Email: jill.rose@usdoj.gov

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT OF EMAIL ACCOUNTS;
FORENSIC IMAGES OF IPHONE, 2
LAPTOPS, AND 2 EXTERNAL HARD
DRIVES AS DESCRIBED IN AFFIDAVIT
AND ATTACHMENT, INCORPORATED
HEREIN.

) DOCKET NO.: 3:13-mj-101

)

) **ORDER TO UNSEAL THE**
) **SEARCH WARRANT, AFFIDAVIT**
) **AND APPLICATION**
)
)
)
)
)
)
)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on April 4, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.


UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Content of email accounts; forensic images of iPhone, 2
laptops, and 2 external hard drives, as described in
Affidavit and Attachment, incorporated herein.

Case No. 3:13mj/101

Certified to be a true and
correct copy of the original
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.

By: B. Fickling
Deputy Clerk

Date: 4/4/13

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):
See Attachment B, which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before

April 17, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.☒ at any time in the day or night as I find reasonable cause has been
established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____

Date and time issued:

4.3.13, 5:35 p.m.

Robert J. Conrad
Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaFILED
CHARLOTTE, NC

APR 4 2013

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Content of email accounts; forensic images of iPhone, 2
laptops, and 2 external hard drives, as described in
Affidavit and Attachments, incorporated herein.US District Court
Western District of NC
Case No. 3:13-mj-10

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 USC 1924; 18 USC 793(e);	Unauthorized removal and retention of classified documents or material;
18 USC 371	Unauthorized possession, communication, and willful retention of national defense information; Conspiracy

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.

Certified to be a true and
correct copy of the original
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By: B. Fickling
Deputy Clerk
Date: 4/4/13

111. DMJ
Applicant's signature

Gerd J. Ballner, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/03/2013

City and state: Charlotte, North Carolina

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

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Gerd J. Ballner, Jr., 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 email accounts [REDACTED], [REDACTED], [REDACTED] and [REDACTED], as well as forensic images of an Apple iPhone (serial number C28J60GKDTDD), two laptop computers (Apple MacBook Air, serial number C02HF37GDJWV, and IBM/Lenova, serial number L3-AY867), and two external hard drives (Toshiba 500GB, serial number 523GFNJASN69, and LaCie, no visible serial number), which were previously searched and seized pursuant to search warrants or by consent during a computer intrusion investigation conducted by Federal Bureau of Investigation (FBI) Tampa Division.¹ All items are currently stored at the FBI Charlotte Field Office at 7915 Microsoft Way, Charlotte, North Carolina 28273. The items identified above are stored in a GSA-approved safe in a Sensitive Compartmented Information Facility, which is accessible only by FBI Charlotte Acting ASAC Scott Cheney, who is the designated filter agent on this investigation.² The specifics of the

¹ The following items were obtained by FBI Tampa by way of search warrants: email accounts [REDACTED], [REDACTED], [REDACTED] and [REDACTED]

The following items were obtained by FBI Tampa by way of consent: forensic images of an Apple iPhone (serial number C28J60GKDTDD), two laptop computers (Apple MacBook Air, serial number C02HF37GDJWV, and IBM/Lenova, serial number L3-AY867), and two external hard drives (Toshiba 500GB, serial number 523GFNJASN69, and LaCie, no visible serial number).

² The items which this affidavit seeks authority to search were originally seized, both pursuant to warrants and by way of consent, in a computer intrusion investigation by FBI Tampa. Those warrants did not permit the FBI to search for or seize items relating to the unlawful removal, communication, or storage of classified information, and the consent to search the laptop

information to be searched and items to be seized are more fully described in

Attachments A and B, which are incorporated fully by reference herein.

2. I am a Special Agent with the FBI and have been employed as such for approximately thirteen years. I have investigated matters involving National Security to include Counterintelligence and Espionage. 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 hostile foreign intelligence services and their recruited human sources to illegally obtain, through clandestine action, classified and proprietary information, which if compromised poses grave danger to the national security of the United States. I have also received specialized 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 is conducting an investigation of [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,

computers, external hard drives, and iPhone was obtained during the course of a voluntary interview focused on cyber stalking activities. The items have been stored by FBI Charlotte in the care of a filter agent. This filter agent has retained sole custody of the items to ensure no access to the information has been provided to agents investigating the matter under the statutes set forth in this affidavit.

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); (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 accounts

[REDACTED], [REDACTED], [REDACTED], and

[REDACTED] as well as forensic images of an Apple iPhone (serial number C28J60GKDTDD), two laptop computers (Apple MacBook Air, serial number C02HF37GDJWV, and IBM/Lenova, serial number L3-AY867), and two external hard drives (Toshiba 500GB, serial number 523GFNJASN69, and LaCie, no visible serial number) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful communication and/or retention of classified information. The items to be searched described in this paragraph consist entirely of items previously seized by the FBI pursuant to court authorized search warrants and by consent. All of the items remain in the FBI's possession. The prior search warrants allowed the FBI to search the items and seize materials relating to what was at the time an investigation into a potential cyber stalking matter, as more fully explained below. The instant request for a search warrant of those items is made to permit the FBI to search those items which are in the FBI's possession and seize materials relating to the violations set forth in paragraph 4 above. With regard to the email accounts identified above, the materials in the FBI's possession consist of data provided by internet service providers pursuant to service of the prior search warrants in the cyber stalking

investigation. The instant request is made to allow the FBI to search that data and seize those materials relating to violations set forth in paragraph 4 above.

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. David 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 July 4, 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. According to a Department of Defense (DOD) official, 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. According to a DOD official, 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 from the email addresses [REDACTED] and [REDACTED]. 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.

15. Investigation conducted by FBI Tampa identified [REDACTED] as the person suspected of using the email accounts [REDACTED] and [REDACTED] referred to above. Investigation also determined [REDACTED] used the email account [REDACTED] On September 24, 2012, FBI Tampa interviewed [REDACTED] at her residence. During this voluntary interview, [REDACTED] admitted sending the emails to Witness 1, as well as other emails regarding Witness 1 to senior United States military officers as well as a foreign diplomat. [REDACTED] also stated that she had engaged in an extramarital affair with Petraeus. [REDACTED] provided consent to search two of her laptop computers and two external hard drives. The computers were imaged by FBI Computer Analysis Response Team (CART) Forensic Examiners.

16. On September 25, 2012, FBI Tampa returned [REDACTED] laptop computers and conducted a follow-up interview. During this follow-up interview, [REDACTED] admitted she told Petraeus that he should get Witness 1 to "drop the charges." [REDACTED] advised agents that she did not know if Petraeus made the request of Witness 1. During the course of this interview, [REDACTED] provided interviewing agents consent to search her Apple iPhone, which she had in her possession. FBI CART

³ On June 29, 2012, FBI Tampa executed a search warrant on the [REDACTED] account. On September 7, 2012, FBI Tampa obtained an additional search warrant on the account. Search warrant results received on October 16, 2012 included emails between the dates of July 1, 2012 and September 7, 2012. On June 29, 2012, FBI Tampa executed a search warrant on the [REDACTED] account. On July 20, 2012, FBI Tampa executed a search warrant on the [REDACTED] account.

Forensic Examiners imaged the contents of her Apple iPhone at the interview location, and the iPhone was returned to [REDACTED], at the conclusion of the interview. A later review of [REDACTED]'s laptops and external hard drives located over 100 items which were identified by CART Forensic Examiners as containing potentially classified information, including information classified up to the Secret level.⁴

17. 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.

18. 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

⁴ On September 26, 2012, FBI Tampa again met with [REDACTED] and returned the two external hard drives, which had also been imaged by CART Forensic Examiners.

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.

19. During interviews conducted of [REDACTED] and Petraeus under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with one another. 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.

A. [REDACTED] Consensual Search, November 12, 2012

20. As a result of finding potentially classified information on the laptops provided by [REDACTED], FBI Tampa and FBI Charlotte conducted a consensual search of [REDACTED] Charlotte residence on November 12, 2012 to recover any evidence related to cyber stalking, in violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents or material, in violation of 18 U.S.C. § 1924. On this same date, a consensual search was also conducted at the residence of [REDACTED] administrative assistant, [REDACTED], in Concord, North Carolina. [REDACTED] voluntarily provided the FBI with various items she maintained in her home in relation to her employment with [REDACTED]. During the searches,

additional paper documents were found, some of which, upon belief and information of your affiant, are classified. As a result of the two searches, the following digital media were seized: eight computers, twelve external hard drives, two printers/scanners, two cellular telephones, two Apple iPods, seven thumbdrives/memory cards, and approximately fifty floppy discs, CDs, and optical discs.⁵

21. Based on a preliminary review of [REDACTED] digital media, it is believed she came into possession of potentially classified information both before and during the writing of her book, "All In: The Education of General David Petraeus." Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. Given her extensive use of digital media, your affiant believes [REDACTED] received/exchanged classified information via email and/or made contact with individuals via email and/or telephone to schedule in-person meetings for the purpose of recording and collecting classified information, as detailed below.
- [REDACTED] is also known to have digitally stored numerous documents, photographs, and audio interviews which contain classified information.

B. Communications Regarding the Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED] sent an email to Petraeus at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parentheses, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, the email related to a

⁵ These items include the two laptops and two external hard drives previously provided by [REDACTED] to FBI on September 24, 2012.

document or series of documents provided by Petraeus to [REDACTED] which contained 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."⁶ 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. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED] and Petraeus, using email address [REDACTED], discussed several topics, to include files

⁶ 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.

maintained by Petraeus. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which Petraeus addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing Petraeus's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, Petraeus wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED] [REDACTED], the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."⁷ In response Petraeus wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, Petraeus, using email address [REDACTED] and [REDACTED] using email address [REDACTED], exchanged over ten emails. In the first email, with the subject line "Found the", Petraeus discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]. Petraeus wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about Petraeus's willingness to share the files writing: "[I]'ll protect them. And I'll protect you." Petraeus later responded to

⁷ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

██████████, writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."⁸ Petraeus continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if ██████████ kept copies. **Class'd, but I guess I might share!**" (emphasis added).

27. Your affiant believes that Petraeus's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to ██████████, --- are classified.

C. Continuing Communications Between ██████████ and Petraeus

28. ██████████ and Petraeus are believed to have had multiple telephonic contacts after each was made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:

- a. Petraeus's CIA security detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, Petraeus acknowledged that: (1) he was briefed by the security detail concerning the FBI investigation, and (2) he called ██████████ on June 23, 2012 regarding the emails received by Witness 1.

⁸ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

- b. Over the weekend of August 11, 2012 and August 12, 2012, Petraeus spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on August 11, 2012.
- c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on three occasions on September 25, 2012.
- d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3, 2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and Petraeus. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.
- e. During the October 26, 2012 interview of Petraeus by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to Petraeus called a telephone number attributed to [REDACTED] on October 16, 2012.
- f. Following FBI Tampa's interview of Petraeus on October 26, 2012, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.

g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa.

[REDACTED] stated that she and Petraeus had talked candidly since each of their interviews with the FBI.

h. On November 9, 2012, [REDACTED] contacted FBI Tampa telephonically from telephone number [REDACTED]. She advised she received a telephone call from Petraeus earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number [REDACTED] called a telephone number attributed to Petraeus on November 9, 2012.

29. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to Petraeus. As detailed above, Petraeus and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED] and Petraeus have admitted that they established covert communications systems using pre-paid cellular telephones and non-attributable email accounts. One of the non-attributable email accounts used by [REDACTED] was [REDACTED].⁹ To date, the pre-paid telephone numbers used by Petraeus and [REDACTED] have not been identified.

30. These telephonic contacts and attempted telephonic contacts between telephone numbers attributed to [REDACTED] and Petraeus indicate [REDACTED] relationship with Petraeus continued after their interviews with FBI Tampa in September and October 2012. Based on these facts, and given [REDACTED] history of email communication with Petraeus, there is probable cause to believe that the [REDACTED]

⁹ On September 5, 2012, FBI Tampa executed a search warrant on the [REDACTED] account.

account as well as the [REDACTED] account contain substantive communications regarding the content of [REDACTED] and Petraeus's FBI interviews, including additional information regarding [REDACTED] access to and retention of classified information.

LOCATION TO BE SEARCHED

31. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant to search the evidence previously seized by FBI Tampa, to include email accounts [REDACTED], [REDACTED], [REDACTED], and [REDACTED] as well as forensic images of an iPhone (serial number C28J60GKDTDD), two laptop computers (Apple MacBook Air, serial number C02HF37GDJWV, and IBM/Lenova, serial number L3-AY867), and two external hard drives (Toshiba 500GB, serial number 523GFNJASN69, and LaCie, no visible serial number), all of which are stored at the FBI Charlotte Field Office at 7915 Microsoft Way, Charlotte, North Carolina 28273. The items are stored in a GSA-approved safe in a Sensitive Compartmented Information Facility, which is accessible only by Acting ASAC Scott Cheney, the designated filter agent in the investigation.

CONCLUSION

32. 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 within the aforementioned items 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.

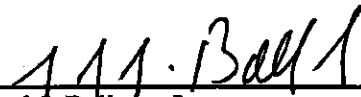
33. Based on the foregoing, I request that the Court issue the proposed search warrant.

Because the warrant will be served on the Federal Bureau of Investigation, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

34. 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,



Gerd J. Ballner, Jr.
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me

on this, the 3d day of April, 2013.



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

ATTACHMENT A

Particular Items To Be Searched

This warrant applies to records and other information contained within evidence seized by FBI Tampa pursuant to warrants or by consent in a computer intrusion investigation of

██████████ to include:

1. Content of email account ██████████ received by FBI Tampa pursuant to search warrants executed on June 29, 2012 and September 7, 2012;
2. Content of email account ██████████ received by FBI Tampa pursuant to a search warrant executed September 5, 2012;
3. Content of email account ██████████ received by FBI Tampa pursuant to a search warrant executed June 29, 2012;
4. Content of email account ██████████ received by FBI Tampa pursuant to a search warrant executed July 20, 2012;
5. Forensic image of an Apple iPhone, serial number C28J60GKDTDD, obtained by consent on September 25, 2012;
6. Forensic image of an Apple MacBook Air laptop computer, serial number C02HF37GDJWV, obtained by consent on September 24, 2012;
7. Forensic image of an IBM/Lenova laptop computer, serial number L3-AY867, obtained by consent on September 24, 2012;
8. Forensic image of a Toshiba 500GB external hard drive, serial number 523GFNJASN69, obtained by consent on September 24, 2012; and
9. Forensic image of a LaCie external hard drive, no visible serial number, obtained by consent on September 24, 2012;

all of which are stored in a GSA-approved safe in a Sensitive Compartmented Information Facility located at the FBI Charlotte Field Office at 7915 Microsoft Way, Charlotte, North Carolina 28273.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Seized by the Government

1. All records or information that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including:
 - a. All records or information related to any communications between [REDACTED] and Petraeus;
 - b. All records or information related to any communications, from December 2008 to the present, between [REDACTED] 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 to [REDACTED] and any involvement of Petraeus in such;
 - 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 [REDACTED] 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 [REDACTED] or Petraeus;
- i. Any information recording [REDACTED] or Petraeus's 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. 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.

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT AND FORENSIC IMAGES OF
EMAIL ACCOUNT AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENT,
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-244

)

) **ORDER TO UNSEAL THE**
) **SEARCH WARRANT, AFFIDAVIT**
) **AND APPLICATION**

)

)

)

)

)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on August 8, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the ____ day of December, 2016.

UNITED STATES MAGISTRATE JUDGE

DEC 20 2016

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

US District Court
Western District of NC

UNITED STATES OF AMERICA

) DOCKET NO.: 3:13-mj-244

v.

)

)

MOTION TO UNSEAL THE

)

SEARCH WARRANT, AFFIDAVIT

)

AND APPLICATION

)

)

)

)

IN THE MATTER OF THE SEARCH OF
CONTENT AND FORENSIC IMAGES OF
EMAIL ACCOUNT AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENT,
INCORPORATED HEREIN

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on August 8, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

//s//JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY
NC Bar Number # 17656

Attorney for USA
Carillon Bldg, Suite 1700
227 West Trade Street
Charlotte, NC 28202
Phone: 704-344-6222
Fax: 704-344-6629
Email: jill.rose@usdoj.gov

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT AND FORENSIC IMAGES OF
EMAIL ACCOUNT AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENT,
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-244

)

) **ORDER TO UNSEAL THE**

) **SEARCH WARRANT, AFFIDAVIT**

)

) **AND APPLICATION**

)

)

)

)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on August 8, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.


UNITED STATES MAGISTRATE JUDGE

FILED
CHARLOTTE, NC

AUG - 8 2013

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

US District Court
Western District of NCIn 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
 18 U.S.C. 1924
 18 U.S.C. 793(e)

Offense Description
 Unauthorized removal and retention of classified documents and materials.
 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.

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

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.

Judge's signature

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] [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

██████████ was the individual who had sent the emails to Witness 1.

15. On September 24, 2012 as part of the FBI Tampa investigation, ██████████ 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 ██████████. He denied providing any classified documents to ██████████ 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 May 12, 2011, [REDACTED], using email account [REDACTED] sent an email to PETRAEUS at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, the email related to a document or series of documents provided by PETRAEUS to [REDACTED] which contained 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."¹ 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. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED] and PETRAEUS, using email address [REDACTED], discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

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.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! Susan Lemke, the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."² In response, PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address [REDACTED], and [REDACTED], using email address [REDACTED]

[REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED].

PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you."

PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."³ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to

² NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!"** (Emphasis added).

27. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

28. 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

29. 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.

30. 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.

31. 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.

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

33. 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.

34. 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.

35. 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

36. 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.
37. 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

38. 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.
39. 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.
40. 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


41. 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

 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.

DEC 20 2016

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NC

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT AND FORENSIC IMAGES OF
EMAIL ACCOUNT AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENT,
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-246

) **MOTION TO UNSEAL THE**
) **SEARCH WARRANT, AFFIDAVIT**
) **AND APPLICATION**

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on August 8, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

//s//JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY
NC Bar Number # 17656

Attorney for USA
Carillon Bldg, Suite 1700
227 West Trade Street
Charlotte, NC 28202
Phone: 704-344-6222
Fax: 704-344-6629
Email: jill.rose@usdoj.gov

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

RECEIVED
CLERK OF COURT
DEC 20 2016

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT AND FORENSIC IMAGES OF
EMAIL ACCOUNT AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENT,
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-246

)

)

)

)

)

)

)

)

ORDER TO UNSEAL THE
SEARCH WARRANT, AFFIDAVIT
AND APPLICATION

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on August 8, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.


UNITED STATES MAGISTRATE JUDGE

FILED
CHARLOTTE, NC

AUG - 8 2013

US District Court
Western District of NC

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

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.

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

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.

Judge's signature

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 email 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] [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. 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

██████████ was the individual who had sent the emails to Witness 1.

15. On September 24, 2012 as part of the FBI Tampa investigation, ██████████ 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 ██████████. He denied providing any classified documents to ██████████ 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 email accounts using non-attributable names and pre-paid cellular telephones. 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 Charlotte, 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.

A. Communications Regarding Potential Mishandling of Classified Information

22. On December 29, 2009, PETRAUES, using email account [REDACTED], sent an email to [REDACTED] at email account [REDACTED]. During a series of emails with the subject line, "Lincoln's T-Mails?" PETRAUES wrote to [REDACTED], "You're pretty accurate! Off in the morning to Iraq, Sinai, and possibly the new focus of our attention..." Based on my training, experience, and information reviewed to date in this investigation, PETRAUES routinely provided [REDACTED] with his schedule and potentially classified operational plans.
23. On January 14, 2010, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account [REDACTED]. The subject line of the email read: "Revolutions in Doctrine" and the body of the email read: "Thank you for this rich feedback. Again, I appreciate your candor! (Except when the off-the-record stuff is so important but I can't use it for PC reasons...damn☺)"
24. On January 16, 2010, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account [REDACTED]. The body of the email read, "GEN Petraeus, The research hat is back on! These attached are some good emails too. Mostly, all of these provide a wonderful timeline of key domestic and Iraq events and your associated sentiment at the time. Thank goodness and lucky me! Good see rapprochement between you and then candidate Obama. (I'm curious about

your promise to tell [REDACTED] about the "one-on-one" discussion you had. Dare I ask?) And I know enough to keep your discussions about politicians with [REDACTED] OTR ...

PETRAEUS replied to [REDACTED], "I'll tell you my pull-aside with now POTUS someday. I owed it to him and was a bit astonished at the self-confidence of his reply- but also quite reassured."

25. On January 23, 2010, [REDACTED], using email account [REDACTED] sent an email to PETRAEUS at email account [REDACTED]. The body of the email read, "GEN Petraeus, Please tell me about your conversation with PM TB! ☺ Best [REDACTED]" Based on the investigation to date, "PM TB" is believed to be then-British Prime Minister Tony Blair. PETRAEUS replied to [REDACTED], "☺" to which [REDACTED] wrote, "pretty please? ☺" PETRAEUS responded, "Add it to the 'over a beer' list, pls. [REDACTED]."

26. Based on my training, experience, and information reviewed to date in this investigation, the emails referenced in paragraphs 23, 24, and 25 demonstrate PETRAEUS' willingness to provide sensitive information to [REDACTED], on an "off the record" basis.

27. On January 16, 2010, PETRAEUS, using email account [REDACTED] forwarded an email to [REDACTED] at email account [REDACTED]. The forwarded email stated, "[REDACTED] the exchanges you've had with [REDACTED] reminded me of the courage you showed in writing your 'strategic Op-Ed' piece in July 07...I think you need to do another one today... The situation in Iraq has turned very serious in the past 48-72 hours with the Accountability and Justice Commission (run by Faisal al-Lami, an Iranian controlled individual, who's being guided by Ahmed Chalabi) recommending over 400 candidates for the Parliamentary Elections be disqualified..." PETRAEUS was

worried about the results of this process and its implications for Iraq. PETRAEUS continued, writing, "We need to galvanize national/world attention/pressure" and ended by saying "Pls protect your source as always. Best – Dave" In her response to PETRAEUS' forwarded email, [REDACTED] wrote, "He is flying to Florida today with his parents...I know I am nobody but let me know if I can help!"

28. PETRAEUS followed up shortly with an email from his [REDACTED] email account to a British political advisor at another CENTCOM-based email account. In the email to the British political advisor PETRAEUS wrote, "ok, please don't betray my hand (act surprised with [REDACTED]), but think this is a way of getting attention to this crisis. I shot up a big red star cluster on SIPR last night too. Got attention. Alerted WH and SEN McCain, as well. Again, please don't share with other than the big one (but tell him). We need to save our beloved land of the two rivers..."
29. [REDACTED] had a copy of the email exchange referenced in paragraphs 27 and 28 in her [REDACTED] email account. Based on information reviewed to date in this investigation, it is believed that PETRAEUS blind carbon copied (bcc) [REDACTED] on many of his email exchanges, and the email above appears to have been found in [REDACTED] Yahoo! Account because she was bcc'd by PETRAEUS.
30. Based on my training, experience, and information reviewed to date in this investigation, the emails referenced in paragraphs 27 and 28 demonstrate PETRAEUS' willingness to share and provide access to sensitive and possibly classified material with [REDACTED].
31. Based on these facts, and given PETRAEUS's history of email communication with [REDACTED], there is probably cause to believe that PETRAEUS's email account,

[REDACTED], contains substantive communications regarding
[REDACTED] access to and retention of classified information.

BACKGROUND CONCERNING EMAIL

32. 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.
33. 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.
34. 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.

35. A CENTCOM subscriber can also store files, including emails, files and other data, on servers maintained and/or owned by CENTCOM.
36. 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.
37. 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.
38. 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

39. 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.
40. 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

41. 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 US CENTCOM 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.

42. Based on the foregoing, I request that the Court issue the requested search warrant.

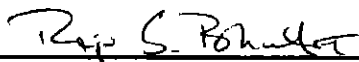
Because the warrant will be served on US CENTCOM, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

43. 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


44. 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 28th 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, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. 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
- e. 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;
 - j. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
 - k. 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.

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT AND FORENSIC IMAGES OF
EMAIL ACCOUNT AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENT,
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-247

)

) **ORDER TO UNSEAL THE**

) **SEARCH WARRANT, AFFIDAVIT**

) **AND APPLICATION**

)

)

)

)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on August 8, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the ____ day of December, 2016.

UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

FILED
CHARLOTTE, NC
DEC 20 2016

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT AND FORENSIC IMAGES OF
EMAIL ACCOUNT AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENT,
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-247

US District Court
Western District of NC

)

)

)

)

)

)

)

)

MOTION TO UNSEAL THE
SEARCH WARRANT, AFFIDAVIT
AND APPLICATION

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on August 8, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

//s//JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY
NC Bar Number # 17656

Attorney for USA
Carillon Bldg, Suite 1700
227 West Trade Street
Charlotte, NC 28202
Phone: 704-344-6222
Fax: 704-344-6629
Email: jill.rose@usdoj.gov

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
CONTENT AND FORENSIC IMAGES OF
EMAIL ACCOUNT AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENT,
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-247

)

) **ORDER TO UNSEAL THE**

) **SEARCH WARRANT, AFFIDAVIT**

)

) **AND APPLICATION**

)

)

)


)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on August 8, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.



UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

FILED
CHARLOTTE, NC

for the

Western District of North Carolina

AUG - 8 2013

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.

US District Court
Western District of NC

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
18 U.S.C. 1924
18 U.S.C. 793(e)

Offense Description
Unauthorized removal and retention of classified documents and materials.
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

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.
Judge's signature
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] [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

██████████ was the individual who had sent the emails to Witness 1.

15. On September 24, 2012 as part of the FBI Tampa investigation, ██████████ 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 ██████████. He denied providing any classified documents to ██████████ 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 SIPR¹) 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.

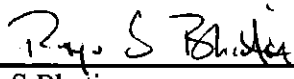
Because the warrant will be served on US CENTCOM, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

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

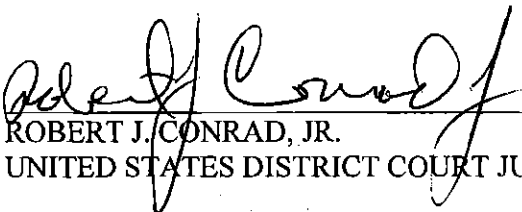
37. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit 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

 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.

DEC 20 2016

US District Court
Western District of NCUNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
MYBOOK ESSENTIAL HARD DRIVE
SERIAL: WCAV5L400801T, AND
CONTENTS, AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENTS
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-277

) MOTION TO UNSEAL THE
) SEARCH WARRANT, AFFIDAVIT
) AND APPLICATION

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on September 23, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY//s//JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY

NC Bar Number # 17656
Attorney for USA
Carillon Bldg, Suite 1700
227 West Trade Street
Charlotte, NC 28202
Phone: 704-344-6222
Fax: 704-344-6629
Email: jill.rose@usdoj.gov

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

FILED
DEC 20 2016

RECEIVED
CLERK OF COURT

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
MYBOOK ESSENTIAL HARD DRIVE
SERIAL: WCAV5L400801T, AND
CONTENTS, AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENTS
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-277

)

) **ORDER TO UNSEAL THE**

) **SEARCH WARRANT, AFFIDAVIT**

) **AND APPLICATION**

)

)

)

)

)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on September 23, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.


UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

MyBook Essential hard drive serial: WCAV5L400801T,
and contents, as described in Affidavit and Attachments
incorporated herein.

Case No.

3:13mj 277

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(Identify the person or describe the property to be searched and give its location):
See Attachment A which is incorporated fully herein

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the
property to be seized):
See Attachment B which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before October 4, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.☒ at any time in the day or night as I find reasonable cause has been
established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for days (not to exceed 30).

☐ until, the facts justifying, the later specific date of Date and time issued:

Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)MyBook Essential hard drive, serial WCAV5L400801T as
described in Affidavit and Attachments, incorporated fully
herein.

Case No. 3:13mj 277

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
 18 U.S.C. 1924
 18 U.S.C. 793(e)

Offense Description
 Unauthorized removal and retention of classified documents and materials.
 Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

See attached Affidavit which is incorporated fully herein

☒ Continued on the attached sheet.

Certified to be a true and correct copy of the original. 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.

U.S. District Court

Frank G. Johns, Clerk

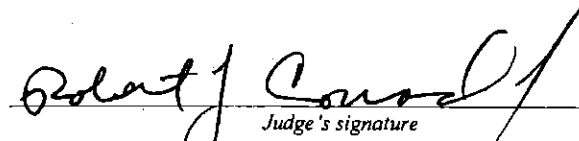
Western District of N.C.

By: 
Deputy ClerkDate: 09/20/2013 Sworn to before me and signed in my presence.Date: 09/20/2013City and state: Charlotte, North Carolina

Applicant's signature

Diane Wehner, Special Agent, FBI

Printed name and title



Judge's signature

Robert J. Conrad, Jr., United States District Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Diane M. Wehner, 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 electronic information associated with certain hard drives supplied by the National Defense University (NDU)¹. 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 7 years. I have investigated matters involving complex financial fraud, public corruption and counterterrorism. 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 specialized 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.

¹ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [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 electronic records held on the following hard drives: a My Book Essential hard drive, serial: WCAV5L25257IT, a My Book Essential hard drive, serial: WCAZA5221633 and a My Book Essential hard drive, serial: WCAV5L400801T (all described in detail in Attachment A) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful 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 July 4, 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. According to a Department of Defense (DOD) official, 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. According to a DOD official, 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 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have 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 email accounts using non-attributable names and pre-paid cellular telephones. 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.

A. Communications Regarding Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED] sent an email to PETRAEUS at email account [REDACTED]

[REDACTED] The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED] which contained 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."² 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 likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED], and PETRAEUS, using email address [REDACTED], discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

² 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.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED]"

[REDACTED] the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there." In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address

[REDACTED], and [REDACTED], using email address

[REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED].

PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you."

PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."³ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

27. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

28. Your affiant believes PETRAEUS and [REDACTED] communicated about the sharing of classified information via PETRAEUS's NIPR⁴ email account. Additionally, based on paragraph 23 above, your affiant believes PETRAEUS allowed classified documents for [REDACTED] to be sent to his SIPR email account.

BACKGROUND CONCERNING NDU COLLECTION

29. Through my training and experience, I have learned that in accordance with the provisions of Title 44, United States Code, Section 3301, 1, PETRAEUS transferred and delivered to NDU, for inclusion in the collections of NDU's library, a collection of personal papers and other non-record personal property.

30. In general, the collection is made up of PETRAEUS's personal files. The collection includes both classified and unclassified documents. The classified collection contains items such as reports, briefings, background material and glossaries. The unclassified collection includes items such as speeches, talking points to the press, newspaper articles and photographs.

31. PETRAEUS's physical documents were provided to NDU in September 2011.

PETRAEUS's electronic documents were provided to NDU in May or June 2012 via hard drives.

32. PETRAEUS's historian provided NDU with three hard drives related to PETRAEUS; two classified and one unclassified. The historian provided two classified hard drives as

⁴ NIPR is an acronym for Non-Classified Internet Protocol Router network, a U.S. government communication system allowing for the exchange of sensitive but unclassified information.

one hard drive contained NATO classified information and the other hard drive contained United States classified information. Later, PETRAEUS's historian wanted to add additional information to the single unclassified hard drive, therefore, PETRAEUS's historian asked NDU to return it. PETRAEUS's historian then combined all the unclassified information onto a single hard drive that was provided to NDU. Both the unclassified hard drive and classified hard drives contain information related to PETRAEUS's career, including his time as Commander of the International Security Assistance Force.

33. The unclassified hard drive contained photographs, speeches made by PETRAEUS, newspaper articles, talking points to the press, administrative paperwork, including tracking calendars and orders, as well as PETRAEUS's NIPR email.
34. The classified hard drives primarily contain PETRAEUS's SIPR email, as well as briefings, classified talking points, reference material, background briefs, maps and daily updates.
35. On or about August 6, 2013, NDU consented to a search of two hard drives from PETRAEUS's collection. A My Book Essential hard drive, serial: WCAV5L25257IT and a My Book Essential hard drive, serial: WCAZA5221633 were transferred from a NDU representative to FBI Agents from the Washington Field Office. The hard drives were then shipped to FBI Charlotte and are currently in the possession of FBI Charlotte. The hard drives are maintained by FBI employees not assigned to the instant matter.
36. On or about August 22, 2013, NDU consented to a search of a My Book Essential hard drive, serial: WCAV5L400801T. This hard drive had been inadvertently overlooked when NDU provided consent on the other two hard drives on or about August 6, 2013.

37. Because it is probable that these drives contain email communications through Petraeus's retirement from the military, there is probable cause to believe they contain communications between Petraeus and [REDACTED], including an email sent to Petraeus's SIPR account attaching a classified document intended for delivery to [REDACTED].

LOCATION TO BE SEARCHED

38. 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 FBI Charlotte to disclose to the government the contents of the hard drives described herein (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.

39. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information found on certain hard drives, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by FBI Charlotte, 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

40. Based upon the foregoing, your affiant submits that there is sufficient probable cause to believe that stored on the hard drives, 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.

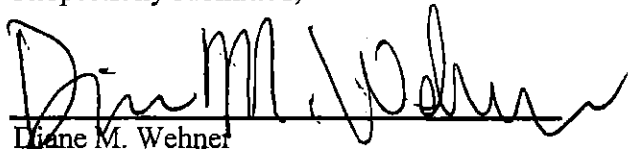
41. Based on the foregoing, I request that the Court issue the requested search warrant.

Because the warrant will be served on FBI Charlotte, 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.

REQUEST FOR SEALING

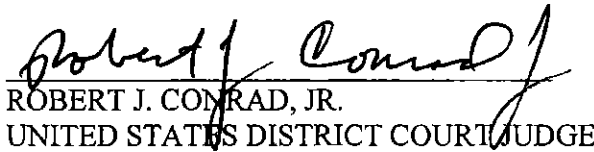
42. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit 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,



Diane M. Wehner
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 20th day of September, 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) contained on the My Book Essential hard drive, serial: WCAV5L25257IT, the My Book Essential hard drive, serial: WCAZA5221633 and the MyBook Essential hard drive, serial WCAV5L400801T that are stored at premises controlled by the FBI, which accepts service of legal process at FBI Charlotte, Charlotte, North Carolina.

ATTACHMENT B

Particular Things To Be Seized

1. All records, information, documents and items on the hard drives that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant:
 - 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 concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
 - h. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
- 2. 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.

DEC 20 2016

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

US District Court
Western District of NC

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
MYBOOK ESSENTIAL HARD DRIVE
SERIAL: WCAV5L25257IT, AND
CONTENTS, AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENTS
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-278

)

) **MOTION TO UNSEAL THE**
) **SEARCH WARRANT, AFFIDAVIT**
) **AND APPLICATION**

)

)

)

)

)

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on September 23, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

//s//JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY

NC Bar Number # 17656
Attorney for USA
Carillon Bldg, Suite 1700
227 West Trade Street
Charlotte, NC 28202
Phone: 704-344-6222
Fax: 704-344-6629
Email: jill.rose@usdoj.gov

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

DEC 30 2016

U.S. DISTRICT COURT
CLERK'S OFFICE
100 S. 1ST ST., 10TH FLOOR
CHARLOTTE, NC 28201

UNITED STATES OF AMERICA

) DOCKET NO.: 3:13-mj-278

v.

)

) **ORDER TO UNSEAL THE**

) **SEARCH WARRANT, AFFIDAVIT**

) **AND APPLICATION**

IN THE MATTER OF THE SEARCH OF
MYBOOK ESSENTIAL HARD DRIVE
SERIAL: WCAV5L25257IT, AND
CONTENTS, AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENTS
INCORPORATED HEREIN.

)

)

)

)

)

)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on September 23, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.


UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

MyBook Essential hard drive serial: WCAV5L252571T,
and contents, as described in Affidavit and Attachments
incorporated herein.

Case No.

3:13mj-278

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of North Carolina
(identify the person or describe the property to be searched and give its location):
See Attachment A which is incorporated fully herein

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):
See Attachment B which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before October 4, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.

☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____

Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature_____
Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

MyBook Essential hard drive, serial WCAV5L252571T as
described in Affidavit and Attachments, incorporated fully
herein.

Case No. 3:13mj278

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:

See attached Affidavit which is incorporated fully herein

☒ Continued on the attached sheet.

Certified to be a true and correct copy of the original. 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.

U.S. District Court

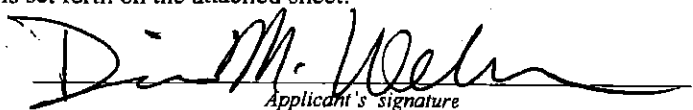
Frank G. Johns, Clerk
Western District of N.C.

By: Cynthia Hilly
Deputy Clerk

Date: 09/23/2013 Sworn to before me and signed in my presence.

Date: 09/20/2013

City and state: Charlotte, North Carolina


Applicant's signature

Diane Wehner, Special Agent, FBI
Printed name and title


Judge's signature

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

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Diane M. Wehner, 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 electronic information associated with certain hard drives supplied by the National Defense University (NDU)¹. 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 7 years. I have investigated matters involving complex financial fraud, public corruption and counterterrorism. 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 specialized 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.

¹ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [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 electronic records held on the following hard drives: a My Book Essential hard drive, serial: WCAV5L25257IT, a My Book Essential hard drive, serial: WCAZA5221633 and a My Book Essential hard drive, serial: WCAV5L400801T (all described in detail in Attachment A) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful 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 July 4, 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. According to a Department of Defense (DOD) official, 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. According to a DOD official, 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 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have 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 email accounts using non-attributable names and pre-paid cellular telephones. 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]'s 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 [REDACTED] and Tampa Divisions of the FBI participated in a consensual search of [REDACTED]'s residence in Charlotte, 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]'s 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]'s 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.

A. Communications Regarding Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED], which contained 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."² 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 likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED] using email address [REDACTED] and PETRAEUS, using email address [REDACTED] discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

² 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.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED]
[REDACTED], the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there." In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address [REDACTED] and [REDACTED], using email address [REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]. PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you." PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."³ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

27. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

28. Your affiant believes PETRAEUS and [REDACTED] communicated about the sharing of classified information via PETRAEUS's NIPR⁴ email account. Additionally, based on paragraph 23 above, your affiant believes PETRAEUS allowed classified documents for [REDACTED] to be sent to his SIPR email account.

BACKGROUND CONCERNING NDU COLLECTION

29. Through my training and experience, I have learned that in accordance with the provisions of Title 44, United States Code, Section 3301, 1, PETRAEUS transferred and delivered to NDU, for inclusion in the collections of NDU's library, a collection of personal papers and other non-record personal property.

30. In general, the collection is made up of PETRAEUS's personal files. The collection includes both classified and unclassified documents. The classified collection contains items such as reports, briefings, background material and glossaries. The unclassified collection includes items such as speeches, talking points to the press, newspaper articles and photographs.

31. PETRAEUS's physical documents were provided to NDU in September 2011.

PETRAEUS's electronic documents were provided to NDU in May or June 2012 via hard drives.

32. PETRAEUS's historian provided NDU with three hard drives related to PETRAEUS; two classified and one unclassified. The historian provided two classified hard drives as

⁴NIPR is an acronym for Non-Classified Internet Protocol Router network, a U.S. government communication system allowing for the exchange of sensitive but unclassified information.

one hard drive contained NATO classified information and the other hard drive contained United States classified information. Later, PETRAEUS's historian wanted to add additional information to the single unclassified hard drive, therefore, PETRAEUS's historian asked NDU to return it. PETRAEUS's historian then combined all the unclassified information onto a single hard drive that was provided to NDU. Both the unclassified hard drive and classified hard drives contain information related to PETRAEUS's career, including his time as Commander of the International Security Assistance Force.

33. The unclassified hard drive contained photographs, speeches made by PETRAEUS, newspaper articles, talking points to the press, administrative paperwork, including tracking calendars and orders, as well as PETRAEUS's NIPR email.
34. The classified hard drives primarily contain PETRAEUS's SIPR email, as well as briefings, classified talking points, reference material, background briefs, maps and daily updates.
35. On or about August 6, 2013, NDU consented to a search of two hard drives from PETRAEUS's collection. A My Book Essential hard drive, serial: WCAV5L25257IT and a My Book Essential hard drive, serial: WCAZA5221633 were transferred from a NDU representative to FBI Agents from the Washington Field Office. The hard drives were then shipped to FBI Charlotte and are currently in the possession of FBI Charlotte. The hard drives are maintained by FBI employees not assigned to the instant matter.
36. On or about August 22, 2013, NDU consented to a search of a My Book Essential hard drive, serial: WCAV5L400801T. This hard drive had been inadvertently overlooked when NDU provided consent on the other two hard drives on or about August 6, 2013.

37. Because it is probable that these drives contain email communications through Petraeus's retirement from the military, there is probable cause to believe they contain communications between Petraeus and [REDACTED], including an email sent to Petraeus's SIPR account attaching a classified document intended for delivery to [REDACTED]

LOCATION TO BE SEARCHED

38. 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 FBI Charlotte to disclose to the government the contents of the hard drives described herein (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.

39. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information found on certain hard drives, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by FBI Charlotte, 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

40. Based upon the foregoing, your affiant submits that there is sufficient probable cause to believe that stored on the hard drives, 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.

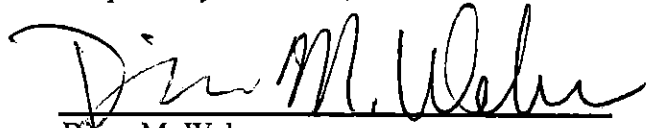
41. Based on the foregoing, I request that the Court issue the requested search warrant.

Because the warrant will be served on FBI Charlotte, 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.

REQUEST FOR SEALING


42. 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,



Diane M. Wehner
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 20th day of September, 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) contained on the My Book Essential hard drive, serial: WCAV5L25257IT, the My Book Essential hard drive, serial: WCAZA5221633 and the MyBook Essential hard drive, serial WCAV5L400801T that are stored at premises controlled by the FBI, which accepts service of legal process at FBI Charlotte, Charlotte, North Carolina.

ATTACHMENT B

Particular Things To Be Seized

1. All records, information, documents and items on the hard drives that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant:
 - 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 concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
 - h. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
- 2. 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.

DEC 20 2016

US District Court
Western District of NCUNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
MYBOOK ESSENTIAL HARD DRIVE
SERIAL: WCAZA5221633, AND
CONTENTS, AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENTS
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-279

) MOTION TO UNSEAL THE
) SEARCH WARRANT, AFFIDAVIT
) AND APPLICATION

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on September 23, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY//s//JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY

NC Bar Number # 17656
Attorney for USA
Carillon Bldg, Suite 1700
227 West Trade Street
Charlotte, NC 28202
Phone: 704-344-6222
Fax: 704-344-6629
Email: jill.rose@usdoj.gov

DEC 30 2016

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

FILED
U.S. DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
MYBOOK ESSENTIAL HARD DRIVE
SERIAL: WCAZA5221633, AND
CONTENTS, AS DESCRIBED IN
AFFIDAVIT AND ATTACHMENTS
INCORPORATED HEREIN.

) DOCKET NO.: 3:13-mj-279

)

) **ORDER TO UNSEAL THE**

) **SEARCH WARRANT, AFFIDAVIT**

) **AND APPLICATION**

)

)

)

)

)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on September 23, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.


UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

MyBook Essential hard drive serial: WCAZA5221633,
and contents, as described in Affidavit and Attachments
incorporated herein.

)
)
) Case No. 3:13mj 279
)
)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(Identify the person or describe the property to be searched and give its location):
See Attachment A which is incorporated fully herein

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the
property to be seized):
See Attachment B which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before October 4, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been
established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____

Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)MyBook Essential hard drive, serial WCAZA5221633 as
described in Affidavit and Attachments, incorporated fully
herein.

Case No.

3:13mj 279

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

18 U.S.C. 1924.

18 U.S.C. 793(e)

Offense Description

Unauthorized removal and retention of classified documents and materials.

Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

See attached Affidavit which is incorporated fully herein

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested

Certified to be a true and correct copy of the original. U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

U.S. District Court

Frank G. Johns, Clerk

Western District of N.C.

By: [Signature]

Deputy Clerk

Sworn to before me and signed in my presence.

Date 9/23/2013Date: 09/20/2013City and state: Charlotte, North Carolina[Signature]

Applicant's signature

Diane Wehner, Special Agent, FBI

Printed name and title

[Signature]

Judge's signature

Robert J. Conrad, Jr., United States District Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Diane M. Wehner, 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 electronic information associated with certain hard drives supplied by the National Defense University (NDU)¹. 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 7 years. I have investigated matters involving complex financial fraud, public corruption and counterterrorism. 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 specialized 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.

¹NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [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 electronic records held on the following hard drives: a My Book Essential hard drive, serial: WCAV5L25257IT, a My Book Essential hard drive, serial: WCAZA5221633 and a My Book Essential hard drive, serial: WCAV5L400801T (all described in detail in Attachment A) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful 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 July 4, 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. According to a Department of Defense (DOD) official, 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. According to a DOD official, 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 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have 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 email accounts using non-attributable names and pre-paid cellular telephones. 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]'s 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 [REDACTED] and Tampa Divisions of the FBI participated in a consensual search of [REDACTED] residence in Charlotte, 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.

A. Communications Regarding Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account

[REDACTED] The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED], which contained 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."² 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 likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED] and PETRAEUS, using email address [REDACTED] discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED]'s email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

² 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.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED] the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there." In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address [REDACTED], and [REDACTED], using email address [REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]. PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you." PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."³ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

27. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED], --- are classified.

28. Your affiant believes PETRAEUS and [REDACTED], communicated about the sharing of classified information via PETRAEUS's NIPR⁴ email account. Additionally, based on paragraph 23 above, your affiant believes PETRAEUS allowed classified documents for [REDACTED] to be sent to his SIPR email account.

BACKGROUND CONCERNING NDU COLLECTION

29. Through my training and experience, I have learned that in accordance with the provisions of Title 44, United States Code, Section 3301, 1, PETRAEUS transferred and delivered to NDU, for inclusion in the collections of NDU's library, a collection of personal papers and other non-record personal property.

30. In general, the collection is made up of PETRAEUS's personal files. The collection includes both classified and unclassified documents. The classified collection contains items such as reports, briefings, background material and glossaries. The unclassified collection includes items such as speeches, talking points to the press, newspaper articles and photographs.

31. PETRAEUS's physical documents were provided to NDU in September 2011. PETRAEUS's electronic documents were provided to NDU in May or June 2012 via hard drives.

32. PETRAEUS's historian provided NDU with three hard drives related to PETRAEUS; two classified and one unclassified. The historian provided two classified hard drives as

⁴NIPR is an acronym for Non-Classified Internet Protocol Router network, a U.S. government communication system allowing for the exchange of sensitive but unclassified information.

one hard drive contained NATO classified information and the other hard drive contained United States classified information. Later, PETRAEUS's historian wanted to add additional information to the single unclassified hard drive, therefore, PETRAEUS's historian asked NDU to return it. PETRAEUS's historian then combined all the unclassified information onto a single hard drive that was provided to NDU. Both the unclassified hard drive and classified hard drives contain information related to PETRAEUS's career, including his time as Commander of the International Security Assistance Force.

33. The unclassified hard drive contained photographs, speeches made by PETRAEUS, newspaper articles, talking points to the press, administrative paperwork, including tracking calendars and orders, as well as PETRAEUS's NIPR email.
34. The classified hard drives primarily contain PETRAEUS's SIPR email, as well as briefings, classified talking points, reference material, background briefs, maps and daily updates.
35. On or about August 6, 2013, NDU consented to a search of two hard drives from PETRAEUS's collection. A My Book Essential hard drive, serial: WCAV5L25257IT and a My Book Essential hard drive, serial: WCAZA5221633 were transferred from a NDU representative to FBI Agents from the Washington Field Office. The hard drives were then shipped to FBI Charlotte and are currently in the possession of FBI Charlotte. The hard drives are maintained by FBI employees not assigned to the instant matter.
36. On or about August 22, 2013, NDU consented to a search of a My Book Essential hard drive, serial: WCAV5L400801T. This hard drive had been inadvertently overlooked when NDU provided consent on the other two hard drives on or about August 6, 2013.

37. Because it is probable that these drives contain email communications through Petraeus's retirement from the military, there is probable cause to believe they contain communications between Petraeus and [REDACTED] including an email sent to Petraeus's SIPR account attaching a classified document intended for delivery to [REDACTED].

LOCATION TO BE SEARCHED

38. 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 FBI Charlotte to disclose to the government the contents of the hard drives described herein (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.

39. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information found on certain hard drives, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by FBI Charlotte, 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

40. Based upon the foregoing, your affiant submits that there is sufficient probable cause to believe that stored on the hard drives, 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.

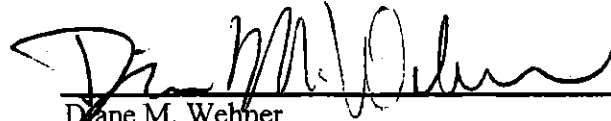
41. Based on the foregoing, I request that the Court issue the requested search warrant.

Because the warrant will be served on FBI Charlotte, 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.

REQUEST FOR SEALING

42. 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,



Diane M. Wehner
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 20th day of September, 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) contained on the My Book Essential hard drive, serial: WCAV5L25257IT, the My Book Essential hard drive, serial: WCAZA5221633 and the MyBook Essential hard drive, serial WCAV5L400801T that are stored at premises controlled by the FBI, which accepts service of legal process at FBI Charlotte, Charlotte, North Carolina.

ATTACHMENT B

Particular Things To Be Seized

1. All records, information, documents and items on the hard drives that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant:
 - 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 concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
 - h. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
2. 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.

DEC 20 2016

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

US District Court
Western District of NC

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT [REDACTED]

AS DESCRIBED IN AFFIDAVIT AND
ATTACHMENT INCORPORATED
HEREIN.

) DOCKET NO.: 3:13-mj-99

)

) MOTION TO UNSEAL THE
) SEARCH WARRANT, AFFIDAVIT
) AND APPLICATION
)
)
)
)
)

NOW COMES the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, who respectfully shows unto the Court that on April 4, 2013, the court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant and the affidavit in support of the application for the warrant; after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States District Court for the District of Columbia, the United States now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto).

THEREFORE, the United States respectfully moves the Court for the search warrant, the application for the warrant, and the affidavit in support of the application for the warrant listed above be unsealed.

Respectfully submitted, on this day of December 19, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

//s//JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY

NC Bar Number # 17656
Attorney for USA
Carillon Bldg, Suite 1700
227 West Trade Street
Charlotte, NC 28202
Phone: 704-344-6222
Fax: 704-344-6629
Email: jill.rose@usdoj.gov

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA

v.

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT [REDACTED]

AS DESCRIBED IN AFFIDAVIT AND
ATTACHMENT INCORPORATED
HEREIN.

) DOCKET NO.: 3:13-mj-99

)


) **ORDER TO UNSEAL THE**
) **SEARCH WARRANT, AFFIDAVIT**
) **AND APPLICATION**
)
)
)
)

UPON MOTION of the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, it appearing that on April 4, 2013, the Court issued a search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government, after reviewing the materials in connection with pending Freedom of Information Act litigation in the United States Court for the District of Columbia, now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government are attached hereto), it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant, as redacted by the government, are hereby UNSEALED.

The Clerk is directed to certify copies of this Order to the United States Attorney's Office.

This the 20 day of December, 2016.


UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

FILED
CHARLOTTE, NC

APR 4 2013

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 3:13-mj-99

US District Court
Western District of NC

The Premises Located at [REDACTED]
[REDACTED] as described in Affidavit
and Attachments, incorporated herein.

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 USC 1924; 18 USC 793(e);	Unauthorized removal and retention of classified documents or material;
18 USC 371	Unauthorized possession, communication, and willful retention of national defense information; Conspiracy

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.

Certified to be a true and
correct copy of the original.
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By: B. Tehting
Deputy Clerk
Date: 4/4/13

111. Ballner
Applicant's signature

Gerd J. Ballner, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/03/2013

City and state: Charlotte, North Carolina

Robert J. Conrad
Judge's signature

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

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Gerd J. Ballner, Jr., 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 warrant to search the residence of [REDACTED], residing at [REDACTED]. The premises to be searched and items to be seized are more fully described in Attachments A and B.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for approximately thirteen years. I have investigated matters involving National Security to include Counterintelligence and Espionage. 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 hostile foreign intelligence services and their recruited human sources to illegally obtain, through clandestine action, classified and proprietary information, which if compromised poses risk to the national security of the United States. I have also received specialized 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.

LOCATION TO BE SEARCHED

4. As set forth below, your affiant submits that probable cause exists for the issuance of a search warrant for [REDACTED] residence, as more fully described in Attachment A to this affidavit, 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.
5. On March 29, 2013, your affiant conducted a search of the CLEAR public source database for [REDACTED] and determined that her current address of record is [REDACTED]. According to 2011 tax records filed in Mecklenburg County, North Carolina, this home is owned by [REDACTED] and [REDACTED], and it is further described as a [REDACTED]. The house number [REDACTED] is visible as brass numerals on the molding above the front entry door.

STATUTORY AUTHORITY

6. The FBI has been conducting an investigation of [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.

7. 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).

8. 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).

9. 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.

10. 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."

11. 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

12. David 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 July 4, 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. According to a Department of Defense (DOD) official, 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.

13. [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. According to a DOD official, 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.
14. In June 2012, the FBI's Tampa Division (FBI Tampa) opened a computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1, which alleged the receipt of threatening and harassing emails from the email addresses [REDACTED] and [REDACTED]. Witness 1 claimed friendships with several high-ranking public and military officials.
15. 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.

16. Investigation conducted by FBI Tampa identified [REDACTED], as the person suspected of using the email accounts [REDACTED] and [REDACTED]. Investigation also determined [REDACTED] uses the email account [REDACTED]. On September 24, 2012, FBI Tampa interviewed [REDACTED] at her residence. During this interview [REDACTED] admitted sending the emails to Witness 1, as well as other emails regarding Witness 1 to senior United States military officers as well as a foreign diplomat. [REDACTED] also stated that she had engaged in an extramarital affair with Petraeus. [REDACTED] provided consent to search two of her laptop computers and two external hard drives.

17. On September 25, 2012, FBI Tampa returned [REDACTED] laptop computers and conducted a follow-up interview. During this follow-up interview, [REDACTED] admitted she told Petraeus that he should get Witness 1 to "drop the charges." [REDACTED] advised she does not know if Petraeus made the request of Witness 1. During the course of this interview, [REDACTED] provided interviewing agents consent to search her Apple iPhone, which she had in her possession. FBI Charlotte Computer Analysis Response Team (CART) Forensic Examiners copied the contents of her Apple iPhone at the interview location. This iPhone, serial number C28J60GKDTDD, is believed to be the same iPhone currently in [REDACTED] possession. It was returned

to [REDACTED] at the conclusion of the interview.¹ A review of [REDACTED] laptops and external hard drives located over 100 items which were identified by Charlotte CART Forensic Examiners as containing potentially classified information, including information up to the Secret level.

18. 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.

19. 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

¹ Because the consensual search of the iPhone was conducted as part of FBI Tampa's computer intrusion investigation, FBI Charlotte has not reviewed the forensic images of the iPhone.

obtain a paper copy of the briefings to preserve the information as research for her book.

██████████ advised that she never received classified information from Petraeus.

20. During interviews conducted of ██████████ and Petraeus under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with one another. 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 ██████████ and Petraeus stated they could not recall all the account names which they created and used to communicate. During ██████████ 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.

A. ██████████ Consensual Search, November 12, 2012

21. As a result of finding potentially classified information on the laptops provided by ██████████, FBI Tampa and FBI Charlotte conducted a consensual search of ██████████ Charlotte residence on November 12, 2012 to recover any evidence related to cyber stalking, in violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents or material, in violation of 18 U.S.C. § 1924. On this same date, a consensual search was also conducted at the residence of ██████████ administrative assistant, ██████████, in Concord, North Carolina. ██████████ voluntarily provided the FBI with various items she maintained in her home in relation to her employment with ██████████. During the searches, additional paper documents were found, some of which, upon belief and information of

your affiant, are classified. As a result of the two searches, the following digital media were seized: eight computers, twelve external hard drives, two printers/scanners, two cellular telephones, two Apple iPods, seven thumbdrives/memory cards, and approximately fifty floppy discs, CDs, and optical discs.

22. Based on a preliminary review of [REDACTED] digital media, it is believed she came into possession of potentially classified information both before and during the writing of her book, "All In: The Education of General David Petraeus." Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. Given her extensive use of digital media, your affiant believes [REDACTED] received/exchanged classified information via email and/or made contact with individuals via email and/or telephone to schedule in-person meetings for the purpose of recording and collecting classified information, as detailed below. [REDACTED] is also believed to have digitally stored numerous documents, photographs, and audio interviews which contain classified information.

B. Additional Evidence of Potential Mishandling of Classified Information

23. A review of [REDACTED] digital media has identified photographs of at least two black books, which appear to be the daily event and calendar books used by Petraeus to memorialize significant events during his military assignments.² Investigators have reviewed the metadata from some of the digital media obtained consensually from [REDACTED] and have determined that from on or about August 29, 2011 to on or about August 31, 2011, there were approximately one hundred and seventeen separate

² Based on a review of these photographs and their embedded metadata, your affiant believes that all of the photographs referenced in paragraphs 23 through 28 of this affidavit were taken using [REDACTED] iPhone.

photographs taken of the contents of the black books. These photographs have been reviewed by your affiant in close coordination with other government agencies designated to assist with this investigation. Based upon a preliminary review by another government agency designated to assist in this investigation, your affiant has reason to believe that at least five of these photographs contain classified information, including information up to the Top Secret level.

24. Additional review of embedded metadata, including date and time stamps, allowed investigators to identify specific photographs from [REDACTED] digital media. On August 29, 2011, at 9:47 a.m., two photographs were taken of the front cover of a black book which had Petraeus's personal business card taped to the front cover. The business card identified Petraeus as "General David H. Petraeus, Commander, International Security Assistance Force."
25. Open source information includes a photograph depicting Petraeus with a black book. See www.thedailybeast.com/newsweek/2011/07/17/general-david-petraeus-on-leaving-afghanistan-and-going-to-cia.html. Based on my review, I believe that the black book depicted in the photographs described in paragraph 24 above is the same black book depicted in the photograph of Petraeus in the news article on the above-mentioned website. The photograph shows Petraeus, while in Afghanistan, standing with then-Secretary of Defense Leon Panetta and General John Allen. This photograph, dated July 9, 2011, reportedly captured Petraeus while he was ending his command in Afghanistan. On the table next to Petraeus in the same photograph, is a similarly sized black book with a business card taped to the front. The format of the business card, its position on the book, the manner in which it is taped to the book, and its general characteristics are very

similar to the photographs of the front cover of a black book located on [REDACTED] digital media.

26. Photographs of what appear to be this same black book were taken on August 30, 2011 at 11:21 a.m., 11:22 a.m., 11:28 a.m., 12:09 p.m., and on August 31, 2011 at 6:15 a.m.

Based upon a preliminary review by another government agency designated to assist with this investigation, your affiant has reason to believe these photographs depict pages from the black books containing classified information, including classified information at up to the Top Secret level.

27. An 8.5 x 11 inch sized printed photograph was located during the consensual search of [REDACTED] residence on November 12, 2012. This photograph showed the content of a black book, specifically a page containing a daily calendar for December 3, 2010 on the left side of the notebook and handwritten notes on the right side of the notebook. The written entry on the top line read, "[REDACTED]: C-N Community of Interest." The calendar in the photograph reflected a "CN Briefing" between 1:45 p.m. and 2:30 p.m. on December 3, 2010. Your affiant opines that the written note for [REDACTED] was added by Petraeus so as to provide [REDACTED] context in reading that day's calendar entry. An initial review of the calendar and notes on this specific image revealed a reference to military units and potential needs for these units.

28. Additional review of [REDACTED] digital media also revealed multiple photographs taken between August 16, 2011 and August 17, 2011. On review of the photographs and the embedded metadata, investigators have determined the following:

- a. On August 16, 2011 at 11:04 p.m., a photograph was taken of at least three medium-sized cardboard boxes sitting on a bed. In the photograph, the boxes are

open, and although the contents are unknown, there appear to be some file folders visible inside the boxes. Sitting on the bed next to the boxes is a black laptop computer which is open and powered on, though the screen image is difficult to discern.

- b. On August 16, 2011 at 11:04 p.m., a second photograph from a different angle was taken of the same boxes referenced above. The boxes are open, and one box has the letters "Petrae" written in black and clearly visible on the side. Your affiant believes this writing spelled out "Petraeus," as the "us" in "Petraeus" was partially obscured.
- c. On August 17, 2011 at 9:23 a.m., [REDACTED] is observed in a photograph which she took of herself in a mirror. In the photograph, [REDACTED] is posing next to the same bed mentioned in paragraphs 33a and 33b above. In this photograph, what appear to be two of the same boxes are visible on the bed. The boxes are open, though the contents of the boxes cannot be clearly discerned.

C. Continuing Communications Between [REDACTED] and Petraeus

29. [REDACTED] and Petraeus are believed to have had multiple telephonic contacts after each was made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:

- a. Petraeus's CIA security detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, Petraeus acknowledged that: (1) he was briefed by the security detail concerning the FBI investigation, and (2) he called [REDACTED] on June 23, 2012 regarding the emails received by Witness 1.

- b. Over the weekend of August 11, 2012 and August 12, 2012, Petraeus spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on August 11, 2012.³
- c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on three occasions on September 25, 2012.
- d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3, 2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and Petraeus. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.
- e. During the October 26, 2012 interview of Petraeus by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to Petraeus called a telephone number attributed to [REDACTED] on October 16, 2012.
- f. Following FBI Tampa's interview of Petraeus on October 26, 2012, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.

³ Unless otherwise noted, the "telephone number associated with [REDACTED]" in these subparagraphs was [REDACTED], the mobile telephone number used on her current iPhone.

g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa.

[REDACTED] stated that she and Petraeus had talked candidly since each of their interviews with the FBI.

h. On November 9, 2012, [REDACTED], contacted FBI Tampa telephonically from telephone number [REDACTED]. She advised she received a telephone call from Petraeus earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number [REDACTED] called a telephone number attributed to Petraeus on November 9, 2012.

30. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to Petraeus. As detailed above, Petraeus and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED], and Petraeus have admitted that they established covert communications systems using pre-paid cellular telephones and non-attributable email accounts. To date, the pre-paid telephone numbers used by Petraeus and [REDACTED] have not been identified.

31. These telephonic contacts and attempted telephonic contacts between telephone numbers attributed to [REDACTED] and Petraeus indicate [REDACTED] relationship with Petraeus continued after their interviews with FBI Tampa in September and October 2012.

32. Considering these facts, and given [REDACTED] history of email and telephone communication with Petraeus, as well as the numerous photographs of what, based on a preliminary review, appear to be classified materials, there is probable cause to believe

that [REDACTED] iPhone contains classified information as well as substantive communications regarding the content of [REDACTED] and Petraeus's FBI interviews, including additional information regarding [REDACTED] access to and retention of classified information.

33. During the consensual search of [REDACTED] Charlotte residence on November 12, 2012, investigators recovered a damaged Apple iPhone, serial number 61116264A4S. Many of the photographs of the black books and cardboard boxes referenced above were located on this damaged iPhone. A review of voicemail and call logs indicates that the damaged iPhone was last used by [REDACTED] in April 2012.
34. Based on your affiant's experience, Apple iPhones allow for the transfer of a user's contents from one telephone to another. It is plausible that [REDACTED], when she ceased using the damaged iPhone, would have transferred data from her damaged iPhone to her current iPhone. Since the damaged iPhone contained photographs of what, based on a preliminary review, appear to be classified materials, and with the potential for transfer of data to her current iPhone, there is probable cause to believe that these photographs were transferred to the iPhone currently in [REDACTED] possession.

TECHNICAL TERMS RELATED TO THE SEARCH

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or

traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other

digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs

usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

36. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises, in whatever form they are found. One form in which the records might be found is data stored on an electronic device. In particular, this application seeks permission to seize an Apple iPhone (hereinafter "the Device"), which could transmit and store such data. Thus, the warrant applied for would authorize the seizure of the Apple iPhone under Rule 41(e)(2)(B).
37. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time, including text messages. Texts messages sent or received on a cellular phone can be stored on a cellular phone at little or no cost. Even when text messages have been deleted by the user of a cellular phone, those text messages, or remnants of those deleted text files, can be recovered months after they have been deleted from a cellular phone. This is so because when a user of a cellular phone "deletes" a text message, the data contained in that message does not actually disappear; rather, that data remains on the cellular phone until it is overwritten with new data. Deleted text messages, or remnants of deleted text messages, may reside on the cellular phone for long periods of time before they are overwritten. Such data can sometimes be recovered with forensic tools.
38. Forensic evidence: As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when.

There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to unlawfully communicate and/or retain classified information, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

39. Necessity of seizing or copying entire computers or storage media: In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with

the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

40. Nature of examination: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. Searches and seizures of evidence from computers commonly requires agents to download or copy information from the computer and components, and to seize the computer to be processed later by a qualified computer expert in a laboratory or other controlled environment. Searching computer systems for evidence is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover hidden, erased, deleted, compressed, password-protected, or encrypted files. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

41. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, emails, texts, email addresses used, IP address information, and internet browsing history.

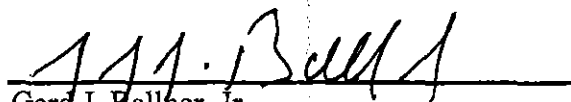
CONCLUSION

42. Based upon the foregoing, your affiant submits that sufficient probable cause exists for the issuance of a warrant to search [REDACTED] [REDACTED], as further described in Attachments A and B; and that the described premises contains 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.

REQUEST FOR SEALING


43. 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,


Gerald J. Ballher, Jr.
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me

on this, the 3d day of April, 2013.


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

ATTACHMENT A

Property To Be Searched

This warrant applies to a single family home and adjoining two-car garage owned by

[REDACTED]

, located at

[REDACTED]

[REDACTED]

. This property is further described as

[REDACTED]

[REDACTED]

which sits on the corner of

[REDACTED]

[REDACTED]

The house number

[REDACTED]

is visible as brass numerals on the molding above

the front entry door. A photograph of the residence is provided below:



ATTACHMENT B

Particular Thing To Be Seized

Apple iPhone, serial number C28J60GKDTDD, hereinafter "the Device."

Information To Be Seized by the Government

1. All records or information on the Device that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including:
 - a. All records or information related to any communications between [REDACTED] and Petraeus;
 - b. All records or information related to any communications, from December 2008 to the present, between [REDACTED] 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 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 [REDACTED] 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 [REDACTED] or Petraeus;
 - i. Any information recording [REDACTED] or Petraeus's schedule or travel from December 2008 to the present;
 - j. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
 - k. Records evidencing the use of the Internet, including records of Internet Protocol addresses used;
2. 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.

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

) Case No. 3:13-mj-99

The Premises Located at [REDACTED]
[REDACTED], as described in Affidavit
and Attachment, incorporated herein.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):
See Attachment B, which is incorporated fully herein.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.YOU ARE COMMANDED to execute this warrant on or before April 17, 2013

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____

Date and time issued:

4.3.13, 5:34pmRobert J. Conrad, Jr.
Judge's signatureCity and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

Certified to be a true and
correct copy of the original.
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By B. F. Felling
Deputy Clerk
Date 4/4/13

Return

Case No.:

3:13mj 99

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature_____
Printed name and title