# UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

| | | |
|---|---|---|
| In the Matter of the Search of<br>*(Briefly describe the property to be searched or identify the person by name and address)*<br><br>Content of email accounts; forensic images of iPhone, 2 laptops, and 2 external hard drives, as described in Affidavit and Attachment, incorporated herein. | )<br>)<br>)<br>)<br>)<br>) | Case No. 3:13mj101 |

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 Frehling
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*

**Return**

| Case No.: 3:13mj101 | 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 accounts; forensic images of iPhone, 2 laptops, and 2 external hard drives, as described in Affidavit and Attachments, incorporated herein.

Case No. 3:13mj10

## 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.

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

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); 18 USC 371 | Unauthorized removal and retention of classified documents or material; 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.

*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

*Judge's signature*

City and state: Charlotte, North Carolina

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

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

I, 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] 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], 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.

[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…"[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 [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.

[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 [redacted] to include:

1. Content of email account [redacted] received by FBI Tampa pursuant to search warrants executed on June 29, 2012 and September 7, 2012;
2. Content of email account [redacted] received by FBI Tampa pursuant to a search warrant executed September 5, 2012;
3. Content of email account [redacted] received by FBI Tampa pursuant to a search warrant executed June 29, 2012;
4. Content of email account [redacted] 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.