

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]
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):

- [x] evidence of a crime;
[x] 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:

Table with 2 columns: Code Section, Offense Description. Rows include 18 USC 1924; 18 USC 793(e); 18 USC 371 and descriptions of unauthorized removal and possession of classified documents.

The application is based on these facts:

- [x] 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: [Signature] Deputy Clerk
Date 4/4/13

[Signature]
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

[Signature]
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 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]
[REDACTED]. According to 2011 tax records filed in Mecklenburg County, North Carolina, this home is owned by [REDACTED] and [REDACTED]
[REDACTED], and it is further described as a [REDACTED]
[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

²Based 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.

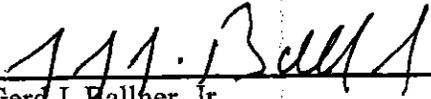
CONCLUSION

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

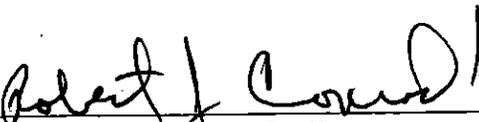
43. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit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



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 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 Carolina

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

The Premises Located at [REDACTED])
[REDACTED], as described in Affidavit)
and Attachment, incorporated 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. F. Felling
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, 5:34pm 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.: 3:13mj99	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