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 WCAV5L25257IT 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.

☐ 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 Deputy Clerk
Date 9/23/2013

Applicant's signature

Diane Wehner, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/20/2013

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, 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 Stated 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] 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], 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 NIPR[4] 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.