

COPY

UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)THE PREMISES LOCATED AT
[REDACTED]

Case No. 1:13sw

273

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 Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

See Attachment A

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

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 18, 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
Ivan D. Davis

(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 Apr 13 @ 1535 hrs.[Signature]
Ivan D. Davis Judge's signature

United States Magistrate Judge

The Honorable Ivan D. Davis

Printed name and title

City and state: Alexandria, Virginia

ATTACHMENT A

Property To Be Searched

This warrant applies to a single family home owned by [REDACTED], located at [REDACTED]
[REDACTED]. This property is further described as a two-story colonial house with [REDACTED]. The house has two floors and a basement. The residence is a single family detached home located on a [REDACTED] property. The home is approximately [REDACTED]
[REDACTED]. The number "[REDACTED]" appears above the main entrance door. The driveway is located to the left side of the main entrance as viewed from [REDACTED]. The premises is located on [REDACTED]
[REDACTED]

ATTACHMENT B

Particular Things To Be Seized

All records, information, documents, and items on the premises that relate to violations of: (a) Title 18, United States Code, Section 1924; (b) Title 18, United States Code, Section 793(e); and (c) Title 18, United States Code, Section 371, including:

1. All handwritten notes, documents, photographs or other instruments related to U.S. government operations;
 2. All records or information related to any communications between PETRAEUS and [REDACTED];
 3. All records or information related to any communications between PETRAEUS and any other person or entity concerning classified and/or national defense information from December 2008 to the present;
 4. All records or information related to any classified and/or national defense information from December 2008 to the present;
 5. All records or information related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED] from December 2008 to the present;
 6. All records or information related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information from December 2008 to the present;
 7. 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;
-

8. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;
9. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS; and
10. Any information recording PETRAEUS's schedule or travel from December 2008 to the present.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
6. Evidence of the times the COMPUTER was used;
7. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
8. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
9. Records of or information about Internet Protocol addresses used by the COMPUTER;
10. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
11. Contextual information necessary to understand the evidence described in this attachment.

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.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

APR - 4 2013

UNDER SEAL DISTRICT COURT
ALEXANDRIA, VIRGINIAIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)THE PREMISES LOCATED AT
[REDACTED]

Case No. 1:13sw

273

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

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

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); Unlawful removal and retention of classified documents; unlawful possession and
18 USC 371 communication 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.

Diane M. Wehner
Applicant's signature

Diane M. Wehner, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

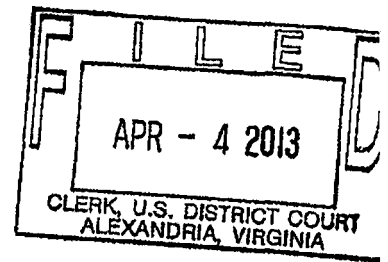
Date: 04/04/2013City and state: Alexandria, Virginia

Ivan D. Davis /s/

Ivan D. Davis
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



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

UNDER SEAL

Case No. 1:13sw 273

**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 warrant to search the residence of DAVID PETRAEUS, 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 seven 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.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the PETRAEUS residence at [REDACTED] (and described in detail in Attachment A) contains 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 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. E.O. 13526 also provides that certain senior U.S. officials are authorized to establish "special access programs" upon a finding that "the vulnerability of, or threat to, specific information is exceptional" and "the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure." Within the U.S. Intelligence Community, the Director of National Intelligence is authorized to establish special access programs for intelligence sources, methods, and activities. Such intelligence programs are called "Sensitive Compartmented Information Programs" or SCI Programs.
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. 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 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.
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 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.

16. 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.
17. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.
18. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her

time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

19. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED] September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.
20. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [REDACTED] residence in Charlotte, North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital

media as well as four boxes and one folder of documents. On this same date,

██████████ 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 ██████████. 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.

21. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. ██████████ 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.
22. ██████████ paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting ██████████ access to classified information for the purpose of writing his biography. For example, in an email dated January 16, 2011, which Petraeus marked as CONFIDENTIAL and sent to multiple members of the military, he instructed a member of his staff to "PLS PRINT FOR ██████████ ON AN OFF THE RECORD BASIS." Travel documents show that ██████████ was in Afghanistan at this time.

A. Communications Regarding Potential Mishandling of Classified Information

23. On May 12, 2011, ██████████, using email account ██████████, sent an email to PETRAEUS at email account ██████████. 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.

24. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED], emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was working on the storyboards and asked her for "a good SIPR number."¹ Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED]. [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

25. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED], and PETRAEUS, using email address [REDACTED]

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

[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." Based on information provided by DOD, your affiant has learned that for a part of 2011 PETRAEUS was provided base housing at Fort Myer in Arlington County, Virginia. According to DOD records, PETRAEUS was assigned to residential quarters on Lee Avenue on Fort Myer between March 1, 2011 and August 10, 2011. PETRAEUS's reference to "unpack[ing] at the house in late July/Aug," probably refers to his private residence at [REDACTED], as he was about to retire from the U.S. Army when he wrote that email and it is unlikely that he would unpack items at base housing he was to vacate in a very short time.² When PETRAEUS vacated the residential quarters on Fort Myer, the Physical Security Manager personally cleared the quarters and found no items left behind. The clearing of the quarters included a search of the attic and basement. According to the Physical Security Manager, if PETRAEUS was traveling, there were specified storage rooms

² The basement of PETRAEUS's residence at [REDACTED] contained a Sensitive Compartmented Information Facility (SCIF) installed by the Central Intelligence Agency. This SCIF was approved for the storage of Top Secret/SCI materials and was given final certification on August 10, 2011. It was closed and de-accredited on January 3, 2013 and physically removed by February 13, 2013.

available at the Military Police station on base where PETRAEUS could leave classified material. After PETRAEUS vacated the residential quarters, the only items related to PETRAEUS remaining at the storage facility at the Military Police station were pieces of CENTCOM equipment, which were subsequently retrieved by CENTCOM personnel.

26. In response to PETRAEUS's email about the items being in boxes that he will unpack in July or August, [REDACTED] wrote: "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."³ In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER." Your affiant believes that, based on the timing of this email, PETRAEUS's statement that the files are "at home" refers to the quarters on Fort Myer.⁴

27. 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

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

⁴ According to records provided by the Department of Defense, PETRAEUS and other senior Army officials were permitted to store and access up to Secret-level data in on-post residential quarters at Fort Myer. This special approval was set forth in a March 15, 2010 memorandum and authorized such storage and access during the entire period in which PETRAEUS was assigned to residential quarters on Fort Myer in 2011.

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..."⁵ 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).

28. 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. Your affiant also believes that, based on the timing of this email, PETRAEUS's statement that the files are "at home" refers to the residential quarters on Fort Myer.

B. Audio Recordings Indicating Potential Mishandling of Classified Information

29. PETRAEUS, in his capacity as ISAF Commander, maintained a digital recorder and may have used the recorder to capture select conversations. Your affiant has identified at least five images on the internet which show PETRAEUS with a recorder. One image shows PETRAEUS in military uniform, apparently in Afghanistan, another is a photograph from [REDACTED] Facebook account showing PETRAEUS and [REDACTED] sitting

⁵ 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.

together in an office, believed to be PETRAEUS's office in Afghanistan. Your affiant has reviewed audio files recovered from [REDACTED] digital media and identified recorded conversations in which [REDACTED] is not heard on the recording and is not believed to have been present. Based upon the content of these recordings, your affiant believes the recorded conversations were originated by PETRAEUS. Your affiant has reviewed publicly available video and audio voice files of PETRAEUS and believes that the above-referenced recordings do include the voice of PETRAEUS. Investigators have not yet recovered any digital recorders from [REDACTED] or PETRAEUS.

30. In an audio file located on a computer received from [REDACTED] administrative assistant, there is a recording of an interview conducted by [REDACTED] during the course of her research on PETRAEUS. This recording is approximately twenty-four minutes, and based on the content of the audio, seems to have been recorded in the August 2011 timeframe. During the recorded conversation, [REDACTED] informed an unknown individual she was interviewing that she would be traveling to Washington, D.C. a lot that month to meet with PETRAEUS and would go through boxes in "his attic." As noted above, although [REDACTED] is not specific as to which PETRAEUS home she is referring, your affiant believes that based on the timeframe of the recording, it is likely that [REDACTED] was referring to the attic in PETRAEUS's residence at Fort Myer.

31. In an audio file located on a hard drive seized from [REDACTED] residence on November 12, 2012, there is a recorded conversation between PETRAEUS and, inter alia, Washington Post reporters, which, based on the information and belief of your affiant, occurred in or about March 2011. In the conversation, PETRAEUS stated, "[I

would really love to be on background as a senior military officer.” Later in the recording, PETRAEUS discusses sensitive military campaigns and operations, some of which, on the basis of a preliminary review by another government agency designated to assist in this investigation, is believed to contain classified information, including information at the Top Secret level.

32. In an audio file located on electronic evidence seized from [REDACTED] residence on November 12, 2012, there is a recorded conversation between PETRAEUS, a reporter, and at least one other individual. During the conversation, PETRAEUS requested that information he provided be attributed to a “defense official familiar with PETRAEUS’s activities.” PETRAEUS was concerned about the sensitivity of the information he was providing, and wanted to ensure the information was not attributed to him because it would come out after he was confirmed as Director of the CIA. PETRAEUS then discussed with the reporter information that, on the basis of a preliminary review by another government agency designated to assist in this investigation, is believed to be classified, including information at the Top Secret level.

C. Additional Evidence of Potential Mishandling of Classified Information

33. 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. 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 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 photographs contain classified information, including information up to the Top Secret level.

34. 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."

35. 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 believes 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.

36. 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 34 above is the same black book depicted in a 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.

37. In an email dated June 26, 2011, an Army historian previously assigned to ISAF replied to an email from PETRAEUS in which PETRAEUS discussed [REDACTED] research efforts. In the body of the Army historian's response, the historian wrote, "I [am] happy to receive [REDACTED] research effort and will add it to the collection. It is still my understanding that your 'black books' and other sensitive items are off limits. She can look at the other documents such as update briefs, info papers, photos, and other reference materials, but not the sensitive ones. Am I correct on that rule?"
38. In an audio file located on a laptop computer seized from [REDACTED], there is a recorded conversation between [REDACTED] and PETRAEUS, which is approximately twenty-five minutes long, and, based on the content of the entire recording, seems to have been recorded in late July/early August of 2011. In the recording, [REDACTED] asked PETRAEUS about the location of the "black books." PETRAEUS responded that the black books are "in a rucksack up there somewhere." PETRAEUS further stated the

black books, "are highly classified, some of them, they don't have it on it, but I mean there's code word stuff in there..." Your affiant believes that when PETRAEUS stated that "there's code word stuff in there," it is possible that he was indicating that there was special access program information contained in the black books. Moreover, your affiant believes PETRAEUS's reference to "they don't have it on it" indicates that the black books do not have the proper classification markings on them. Just as in paragraphs 28 and 30 above, the statement regarding the location of the materials likely referred to PETRAEUS's former residence at Fort Myer. Photographs of the contents of these black books were found during the review of digital and physical evidence recovered during the consensual search of [REDACTED] house.

39. 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 39a and 39b 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.
40. The boxes and black books photographed by [REDACTED], and believed to belong to PETRAEUS, were not recovered during the consensual search conducted at [REDACTED] residence on November 12, 2012, nor were they recovered when the Sensitive Compartmented Information Facility in PETRAEUS's residence was cleared by CIA personnel after PETRAEUS's resignation as Director in November 2012.
41. Based upon PETRAEUS's description of the various items your affiant believes PETRAEUS had stored in the residential quarters at Fort Myer, including both the black books described in paragraph 38 above as well as the files and boxes discussed in paragraphs 25-27 above, it appears that that he had kept some of these materials for nearly a decade, and thus through various geographical moves in the military. Your affiant believes that these are items PETRAEUS values, and it is therefore likely he would have taken them with him when he was required to vacate the residential quarters at Fort Myer and moved to his private residence at [REDACTED]
[REDACTED]

D. Continuing Communications Between PETRAEUS and [REDACTED]

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

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

- e. During the October 26, 2012 interview of PETRAEUS by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to PETRAEUS called a telephone number attributed to [REDACTED] on October 16, 2012.
 - f. Following FBI Tampa's interview of PETRAEUS on October 26, 2012, a telephone number attributed to [REDACTED] called a telephone number attributed to PETRAEUS on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.
 - g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa. [REDACTED] stated that she and PETRAEUS had talked candidly since each of their interviews with the FBI.
 - h. On November 9, 2012, [REDACTED] contacted FBI Tampa telephonically from telephone number [REDACTED]. She advised she received a telephone call from PETRAEUS earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number [REDACTED] called a telephone number attributed to PETRAEUS on November 9, 2012.
43. 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.

LOCATION TO BE SEARCHED

44. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for PETRAEUS's 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.
45. On April 2, 2013, a search of the CLEAR public source database for the address [REDACTED], revealed the residence was owned by [REDACTED] and that it was purchased on [REDACTED]. Consistent with his obligations as a government employee, PETRAEUS filed a 2011 financial disclosure form with the United States government, listing his home address as [REDACTED]. The form stated that PETRAEUS purchased the residence in [REDACTED] for a purchase price of [REDACTED] and also stated that PETRAEUS and his wife are trustees of [REDACTED] the company that owns the residence at [REDACTED]. Given the information noted in the financial disclosure, as well as information provided by the CIA, your affiant believes that PETRAEUS's current residence is [REDACTED].

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

46. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
47. The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
48. 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 a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
49. I submit that if a computer or storage medium is found on the premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:
- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

50. 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 devices were used, the purpose of their use, who used them, and

when. There is probable cause to believe that this forensic electronic evidence might be on the devices 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.

51. 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.

52. 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 devices 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.

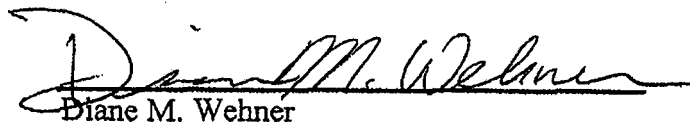
53. Because more than one person uses the premises as a residence, it is possible that the premises will contain storage media that are predominantly used, and perhaps owned, by a person who is not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

54. Based upon the foregoing, your affiant submits that sufficient probable cause exists for the issuance of a warrant to search [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

55. 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.

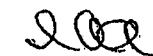


Diane M. Wehner

Special Agent

FBI Charlotte Division

Sworn to and subscribed before me
this 4th day of April, 2013.

 /s/ _____
Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

This warrant applies to a single family home owned by [REDACTED], located at [REDACTED]

[REDACTED] This property is further described as a two-story colonial house [REDACTED]. The house has two floors and a basement. The residence is a single family detached home located on a [REDACTED] The home is approximately [REDACTED] [REDACTED] [REDACTED]. The number [REDACTED] appears above the main entrance door. The driveway is located to the left side of the main entrance as viewed from [REDACTED]. The premises is located on [REDACTED].

ATTACHMENT B

Particular Things To Be Seized

All records, information, documents, and items on the premises that relate to violations of: (a) Title 18, United States Code, Section 1924; (b) Title 18, United States Code, Section 793(e); and (c) Title 18, United States Code, Section 371, including:

1. All handwritten notes, documents, photographs or other instruments related to U.S. government operations;
2. All records or information related to any communications between PETRAEUS and [REDACTED];
3. All records or information related to any communications between PETRAEUS and any other person or entity concerning classified and/or national defense information from December 2008 to the present;
4. All records or information related to any classified and/or national defense information from December 2008 to the present;
5. All records or information related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED] from December 2008 to the present;
6. All records or information related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information from December 2008 to the present;
7. 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;

8. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;
9. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS; and
10. Any information recording PETRAEUS's schedule or travel from December 2008 to the present.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
6. Evidence of the times the COMPUTER was used;
7. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
8. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
9. Records of or information about Internet Protocol addresses used by the COMPUTER;
10. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
11. Contextual information necessary to understand the evidence described in this attachment.

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.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.