AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

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

261 Richland Road
Fredericksburg, Virginia, 22406

Case No. 3:18SW49

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, fully incorporated by reference herein;

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

See Attachment B, fully incorporated by reference 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. § 641	Theft of Government Property
18 U.S.C. § 793(e)	Willful Retention of National Defense Information
18 U.S.C. § 798(a)	Disclosure of Classified Communications Intelligence Information

The application is based on these facts:

See attached Affidavit, fully incorporated by reference 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.

Steven K. Hall
Applicant's signature

Steven K. Hall, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: Mar 7, 2018

/s/
David J. Novak
United States Magistrate Judge
Judge's signature

City and state: Richmond, Virginia

David J. Novak, United States Magistrate Judge
Printed name and title

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

IN THE MATTER OF THE SEARCH OF:

261 Richland Road
Fredericksburg, Virginia, 22406

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Steven K. Hall, 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 the residence of JOHN GLENN WEED ("WEED"), 261 Richland Road, Fredericksburg, Virginia, which is located within the Eastern District of Virginia and is further described in Attachment A. This application also seeks authorization to seize contraband, evidence, instrumentalities, and fruits of crime as described below.

2. I am a special agent with the Federal Bureau of Investigation (FBI), United States Justice Department, and am currently assigned to the Richmond Field Office, Fredericksburg Resident Agency. I have been an FBI special agent since July 1998. I am a 1988 graduate from Texas A&M University with a bachelor's degree in political science. Prior to becoming an FBI agent, I was employed for seven years in the United States Air Force, attaining the rank of captain.

3. During my tenure as an FBI special agent I have participated in, and lead numerous investigations, to include but not limited to, homicide, organized crime, narcotics trafficking, white collar crime, cyber, terrorism, and counter-intelligence violations. These violations are included in Titles 18 and 21 of the United States Code. I have authored search and

seizure and arrest warrants in connection with these investigations.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents 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.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C § 641 (Theft of Government Property), 18 U.S.C. § 793(e) (Willful Retention of National Defense Information), and 18 U.S.C. § 798(a) (Disclosure of Classified Communications Intelligence Information), have been committed and that there is also probable cause to search the property described in Attachment A for evidence of these crimes.

OVERVIEW OF CLASSIFIED INFORMATION AND APPLICABLE STATUTES

6. Information may be classified by the United States Government at one of three general levels. Information may be classified as "Top Secret" if the unauthorized disclosure of such information "reasonably could be expected to cause *exceptionally grave damage* to the national security[.]" *See* Executive Order 13526 § 1.2(a)(1) (emphasis added) (hereinafter "E.O. 213526"). Additionally, information may be classified as "Secret" if the unauthorized disclosure of such information "reasonably could be expected to cause *serious damage* to the national security[.]" *See* E.O. 13526 § 1.2(a)(2) (emphasis added). Finally, information may be classified as "Confidential" if the unauthorized disclosure of such information "reasonably could be expected to cause *damage* to the national security[.]" *See* E.O. 13526 § 1.2(a)(3) (emphasis added). Access to classified information at any level may be further restricted through compartmentalization in Sensitive Compartmentation Information (SCI) categories.

7. Generally, an individual may have access to classified information if and *only* if: (1) a favorable determination of that individual's eligibility for access has been made by an agency head or designee; (2) the individual has signed an approved nondisclosure agreement; (3) the individual has a need to know the information; and (4) the individual receives contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on any individual who fails to protect classified information from unauthorized disclosure. *See* E.O. 13526 § 4.1. Individuals who meet these criteria and are granted access to classified information are commonly referred to as having a "security clearance" for information classified at a certain level.

8. Even if an individual possesses a security clearance, access to classified information at a certain level is allowed only if the individual possesses the clearance corresponding to that level of classification and the individual has a legitimate need to know the information. For example, an individual holding a security clearance for information classified at the "Secret" level is ineligible to access information classified at the "Top Secret" level. Moreover, even if that person requests access to information classified at the "Secret" level, access will be denied *unless* there is a legitimate need for that person to access the information as part of his or her duties.

PROBABLE CAUSE

9. From 1993 through November 2012, JOHN GLENN WEED was a computer systems architect, Level 6, for The Analytic Sciences Corporation (TASC), Chantilly, Virginia, and was briefed into multiple classified programs. In his position as a computer systems architect, WEED developed both classified and unclassified communications systems for the United States Government. Much of WEED's work at TASC was in support of the National

Reconnaissance Office ("NRO").

10. As part of his periodic reinvestigation (PR) for his security clearance, an adjudications investigator with the Department of Defense learned that WEED had received a third Driving Under the Influence (DUI) arrest in May 2012. WEED had not promptly reported that arrest as he was required to do as a condition of maintaining his security clearance, and only reported the incident in September 2012 after he had pleaded guilty and been convicted of the offense in Fauquier County Circuit Court. On or about September 17, 2012, the same background investigator attempted to schedule an interview with WEED regarding the unreported DUI. An interview was scheduled for September 18, 2012. On that day, WEED contacted the investigator and stated that he would be unable to come in because he was working on "Iran issues." A review of public records has revealed that on September 18, 2012, WEED was charged with Violation of Probation in Fauquier County, Virginia.

11. The background investigator interviewed WEED on September 20, 2012. WEED appeared at the interview carrying a photograph of the officer who arrested him for his third DUI. The officer's photo had multiple bullet holes in it. WEED stated that he got the picture off the Internet and used the picture of the arresting officer as "target practice." WEED believed he was unjustly convicted and that he intended to "ruin the life" of the arresting officer for what he did. As a result of the PR investigation, on November 1, 2012, WEED's clearance was revoked for cause based on criminal and personal conduct.

12. WEED appealed his termination and revocation of his security clearance. During the appeals process, WEED responded to his revocation with a letter dated December 24, 2012, titled *"Double Standards, the Putrefaction of Public Trust and the Erratic Dispensing of Justice."* WEED asserted several concerns he claimed to have in an attempt to rebut his

revocation and included details of work performed for the U.S. Government. Due to security concerns with the letter (which was sent via regular mail and likely produced on an Unclassified computer), a preliminary classification review was completed by NRO personnel. WEED did not have access to a classified computer at this time. The review determined the letter contained classified information up to the level of Secret//SCI. In this letter, WEED described his involvement in deployments around the world in support of operations in the "Global War On Terror." In doing so, WEED revealed the names of specific organizations, the geographic location of their operations, and the nature of the activities in which they are engaged. This disclosure of the information in this letter could cause serious damage to national security.

13. Prior to his termination WEED had worked on multiple classified programs for the United States Government for many years. During that time he regularly received the customary security refresher training given to employees with such access, signed multiple nondisclosure agreements ("NDA") that further discussed the proper handling of SCI information, and even wrote a security manual for one such classified program. WEED clearly knew or should have known that certain statements he wrote in his *Double Standards* letter involved sensitive classified information. Even so, the strong and widely-held reputation that WEED's colleagues had of him—which I know from first-hand interviews I've conducted with WEED's civilian supervisors at TASC, his military supervisors at the NRO, and his military and civilian coworkers—was that WEED felt the rules did not apply to him.

14. In May 2013, NRO investigators discovered that four remote desktop protocol (RDP) sessions had been established on WEED's NRO computer to an external IP address during a four-day period just prior to WEED's termination on September 2012. NRO's network security procedures did not, and do not, permit such RDP sessions. Further investigation

determined that the contents of these RDP sessions were compressed and encrypted. Information obtained from Comcast, including both business records and explanatory information provided verbally to me by Comcast employees, revealed that the external IP address associated with these RDP sessions had been assigned on the dates in question to WEED's residential Comcast account with service to 261 Richland Road, Fredericksburg, Virginia. Based on all this and other information, on August 23, 2013, I obtained a search warrant for WEED's residence, Case No. 3:13-ms-235.

15. On August 27, 2013, FBI investigators executed the above-described warrant at WEED's residence and seized numerous items. Among items seized was a radio set worth over $200,000 that had been provided to the NRO by another government agency in 2005. Investigators also seized 11 "friendly force trackers," also known as "blue force trackers" (BFTs), which are carried by U.S. Government assets on operational missions and are designed to provide a secure method for operational commanders to track the movements of such assets, including both personnel and vehicles, when operating in or near hostile territory. Each of those BFTs had a value of approximately $6,000. The total value of the U.S. government radio equipment recovered from WEED's residence was approximately $340,000. WEED did not have permission to possess any of this equipment at his home following the termination of his employment with TASC.

16. Investigators also seized multiple computers and electronic media from WEED's residence. Forensic analysis of those devices revealed the presence of source code for two communications programs classified at the SECRET/SCI level that WEED had worked on or with during his employment with TASC in support of the NRO. Other classified electronic data was recovered from WEED's computers, including several operational reports that included the

word "SECRET" in the classification field of the messages themselves.

17. On or about April 17, 2017, officials at the NRO were notified about a Facebook page posted in the name of "WILLIAM AMOS (JAKE)." The Facebook page had a picture on the page, posted on January 14, 2017, that appeared to depict computer code for a government computer system that WEED had designed while employed with TASC. NRO officials conducted a review of the information depicted in the picture, and on May 1, 2017, determined that the information posted on the page was indeed classified at the SECRET level. Subject matter experts with the NRO informed me that the computer code depicted in the Facebook post is related, to the design, construction and use of a communications intelligence device and system used by United States government assets to communicate intelligence activities. Certain computer files related to this same communications program were found on one or more of the computers seized from WEED's residence on August 27, 2013.

18. I believe that "WILLIAM AMOS" is actually WEED. In the Facebook post with the above-described picture there is a file folder named "Connor" on the computer desktop depicted in that photo. WEED's son is named Connor. In another posting to the same "WILLIAM AMOS" account, dated January 14, 2017, there is a picture of an individual shooting a gun. This picture closely resembles an image file recovered from one of WEED's computers seized during the execution of the search warrant at his residence. There is probable cause to believe that AMOS is actually WEED. On May 26, 2017, I obtained a federal search warrant for the WILLIAM AMOS Facebook account, which I served on Facebook on May 30, 2017. On June 9, 2017, Facebook returned the results of the warrant to the Federal Bureau of Investigation. The results show the account was registered on January 2, 2017, and the individual registering the account as "WILLIAM AMOS." The registration IP address was

2601:5cc:0:2e23:201:c0ff:fe19:9a13, and the account was listed as active. As discussed further below, the results of the search warrant return indicate WILLIAM AMOS is actually JOHN WEED.

19. Specific examples showing AMOS is actually WEED were discovered during the analysis of the information. Those instances include but are not limited to the following:

a. In one conversation included in the returns, AMOS told an individual named KEN MILLS, "Ken, this is JW (dog hunter), sent you a friend request. I'm finally up with the times and using Facebook. Have to use this alias for reasons I won't go into here." Later on "AMOS" talked about the ongoing investigation concerning WEED and a search warrant that was executed at his residence in August 2013.

b. AMOS states in his Facebook account that he is involved in the buying and selling of antique coins. During one particular discussion with a potential customer, AMOS stated, "I'll be ending [*sic*] it form the US, I live here, contrary to what the site says; after nearly 30 years in the [*sic*] Intelligence Community and too many overseas assignments I nervous about putting too much stuff on Facebook, one of the reasons Ive never joined until recently." AMOS's comment "contrary to what the site says" appears to refer to AMOS's Facebook page indicating a current city of Incirlik Air Base in Turkey. I also know from my investigation of WEED that the above quote of "after nearly 30 years in teh [sic] Intelligence Community and [] many overseas assignments" is consistent with WEED's career working at government contractors supporting the NRO

and other intelligence agencies.

c. In another post, AMOS told an individual named SEAN WALKER "It's me, brother... facebook didn't like the Non Sequitur name and they woldn't let me crate a john wed account without sending photo id because they said weed was not a valid last name." On the same page he also states "Billy amos was a childhood friend of mine that I used to try and protect. He MS and was always getting picked on on the way home. So I'd jump in and take the beating while he hurried home."

d. Also in the Facebook search warrant returns from the WILLIAM AMOS account is a photograph of a man who I recognize as JOHN GLENN WEED based on multiple encounters I have had with him. Depicted in that photograph with WEED is a woman identified as ELLEN HOWLETT.

e. There is an exchange between WEED and CLAYTON PFEILER, where WEED stated, "OK, tis will be my first try at invoicing. I will be sending it from the guys account that has my power of attorney while I'm gone on travel, so I don't have to create a new account. It'll be John Weed. Just an FYI." Related to this conversation is a photograph of a Registered Mail Receipt showing the "To" address as JOHN WEED, 261 Richland Road, Fredericksburg, VA 22406.

f. The Facebook search warrant returns also include several conversations during which "AMOS" mentions an ongoing investigation of him being conducted by the FBI and/or the NRO, and AMOS specifically names

individuals with whom I've worked on the investigation, of JOHN WEED, including NRO investigators and an Assistant United States Attorney assigned to the case.

20. The search warrant returns for the WILLIAM AMOS Facebook account included the Facebook posting described above that is a photograph of what appears to be computer code. In a letter dated May 1, 2017, officials at the NRO determined that the information contained in that photograph is classified at the SECRET// REL to the USA, AUS, and GBR level, and the unauthorized disclosure of this information could reasonably be expected to cause serious damage to the national security of the United States of America. I believe this photograph shows WEED currently has classified national defense information at his residence, on a mobile device in his possession, or on his person. The computer code that was posted on Facebook is known to be a classified program WEED worked on at the NRO.

21. On June 26, 2017, a Federal Grand Jury subpoena was sent to Comcast, Legal Response Center, concerning the above-listed IP address (*i.e.,* 2601:5cc:0:2e23:201:c0ff:fe19:9a13,) that was used to access Facebook at the time the WILLIAM AMOS account was created. On July 5, 2017, Comcast faxed the results of the subpoena to the Federal Bureau of Investigation. Comcast, in the return, stated the subscriber information as below:

Subscriber name:	JOHN WEED
Service Address:	261 Richland Road, Fredericksburg, VA 22406
Telephone number:	540-737-5070
Type of service:	High Speed Internet Service
New Account number:	8299610380465236
Old Account number:	1501176052002

Start of Service: Unknown

Account Status: Active

IP Assignment: Dynamically Assigned

22. Investigators have not been able to identify what type of computer or laptop WEED has. Investigators were not able to locate the source of the classified information during the previous search of WEED's residence in August 2013. Based on the Comcast information outlined above, WEED currently maintains an active high-speed Internet service account at his home address. A search of real property records shows that this address is a single-family residence owned jointly by JOHN and ANN WEED. Together, I believe this information establishes probable cause that WEED has used, and continues to use, some type of computer equipment at 261 Richland Road, Fredericksburg, Virginia, 22406.

23. Based on my experience, it is easy and common to transfer electronic data from one electronic device to another. Such electronic devices include: computers, computer software, external hard drives, thumb drives, compact discs, tapes, flash drives, memory sticks, PDAs, Blackberry devices, and cellular telephones.

24. Based on my experience, it is also possible to print documents stored in electronic form. As a result, it is common to find printed copies of documents in and around areas near computer systems or mobile devices that store documents electronically.

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

a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross

state and international borders, even when the devices communicating with each other are in the same state.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

26. As described in Attachment B, this application seeks permission to search for records that might be at 261 Richland Road, Fredericksburg, Virginia, 22406, 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).

27. *Probable cause.* I submit that if a computer or storage medium is found at 261 Richland Road, Fredericksburg, Virginia, 22406, 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 or saved onto a storage medium. Electronic files downloaded to a storage medium can be stored for years at little to 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. Therefore, 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 "recovery" file.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28. *Necessity of seizing entire computers or storage media.* In most cases, a thorough search of 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. Further, in this case, there is probable cause to believe WEED is in possession of stolen United States government property, including classified information. Seizing all computer and storage media will be necessary to conduct a thorough investigation and make sure any stolen information is properly secured. Following seizure, a thorough examination will be conducted to identify the data recorded on the computer and storage media, and to prevent the loss of the data either from accidental or intentional destruction. In addition, offsite examination is appropriate for the following reasons:

a. *The time required for an examination.* 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. Taking that much time on the premises could be unreasonable. 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. This would be impractical and invasive to attempt on-site. However, the possibility exists that computers or computer equipment will be in use and encrypted. Since the data that was compromised as described above was not found during the previous search warrant in August 2013, it may be hidden among other files or data. Taking the computer and storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

b. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Further, storage media can be concealed in a variety of ways at different locations, such as a home, vehicle, or other location. Based on this reality, authority is requested to search computers, safes, lock-boxes, locked drawers, outbuildings, vehicles, or other areas, devices, or media located on the target property that may contain classified information.

29. *Nature of examination.* Based on the foregoing and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing any computers and storage

media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to, computer-assisted scans of the entire medium.

30. *Special Search and Seizure Requirements for Classified Information Stored on Electronic Media.* Where, as here, the purpose of the search is to identify and seize classified information from an unauthorized document, computer system, electronic media, or storage medium, there may be additional procedures that must be followed. For the reasons described above, simply deleting a classified document from a computer or electronic storage device is insufficient to ensure that all classified data is completely removed. Accordingly, to adequately ensure that files containing classified information are truly deleted, and no residual classified data remains, it will be necessary to seize the entire hard drive or other storage medium, isolate any unclassified information that is not subject to seizure, and return a completely new hard drive or storage medium to that owner that contains the files and information not subject to seizure.

SURVEILLANCE

31. Over the past several days preceding my application for this search warrant, myself and other investigators have conducted surveillance of the premises located at 261 Richland Road, Fredericksburg, VA 22406. That surveillance has confirmed that JOHN GLENN WEED still resides at that address.

PROPERTY TO BE SEARCHED AND THINGS TO BE SEIZED

32. I anticipate executing this warrant to search for and seize evidence, fruits, and instrumentalities of offenses involving violations of 18 U.S.C § 641 (Theft of Government Property), 18 U.S.C. § 793(e) (Willful Retention of National Defense Information), and 18

U.S.C. § 798(a) (Disclosure of Classified Communications Intelligence Information) particularly described in Attachment B. The property to be searched is described in Attachment A.

CONCLUSION

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

Respectfully submitted,

Steven K. Hall
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on March 7, 2018

/s/
David J. Novak
United States Magistrate Judge

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

The residence of JOHN GLENN WEED, which is located at 261 Richland Road, Fredericksburg, Virginia, 22406, together with any computers, safes, lock-boxes, locked drawers, outbuildings, vehicles, or other areas, devices or media located on the property that may contain classified information. The residence at 261 Richland Road, Fredericksburg, Virginia, 22406, is described as a contemporary-type house, with tan wood siding and a multi-car garage.

ATTACHMENT B

Property to be Seized

1. All records relating to violations of 18 U.S.C § 641 (Theft of Government Property), 18 U.S.C. § 793(e) (Willful Retention of National Defense Information), and 18 U.S.C. § 798(a) (Disclosure of Classified Communications Intelligence Information), including:

   a. records or other evidence related to the unauthorized gathering, transmitting, storing, and removal of U.S. government or classified documents or material;

   b. records or other evidence related to financial transactions, such as bank records, account statements, accounting software, billing and accounting records, payment receipts, and other financial records;

   c. records or other evidence indicating contact with any foreign government, business entity, or individuals with respect to the unauthorized gathering, transmitting, storing, and removal of classified documents or material;

   d. records or other evidence indicating any internet, electronic, or physical shipping or transmission methods used to transmit or receive classified documents or material;

   e. records or other evidence reflecting the operations associated with the production of fraudulent identification documents, including, but not limited to, ledgers, inventory lists, customer lists, financial statements, receipts, and other items.

2. Computers or storage media potentially used as a means to commit the violations described above.

3. 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"):

   a. 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;

b. 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;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. 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;

k. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

5. During the course of the search, law enforcement officials may photograph the searched SUBJECT PREMISES to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

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.