UNITED STATES DISTRICT COURT

for the

Southern District of California

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

Vizocom ICT LLC, a single family dwelling located at 1506 Constancia Way, El Cajon, California 92019

Case No. '19MJ5592

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, incorporated herein by reference.

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

See Attachment B, incorporated herein by reference.

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*
Title 18 United States Code, Sections 287, 1001, 1343, and 1349.	False Claims, False Statements, Wire Fraud, and Conspiracy to Commit Wire Fraud.

The application is based on these facts:

See attached Affidavit of Special Agent John Doyle, incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

John Doyle, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/16/19

Judge's signature

City and state: San Diego, California

Hon. Michael S. Berg, United States Magistrate Judge

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched is 1506 Constancia Way, El Cajon, CA 92019, and any and all outbuildings, appurtenances, storage areas, and locked containers, associated therewith (the "**TARGET PREMISES**"). The property is further described as a single family dwelling with a two car garage located on the front south west corner of the house. The garage door is white in color with four narrow starburst style windows that line the top length of the door. The exterior appears to be a white or light tan stucco with red brick corners. The brick exterior covers the corners of the garage from the ground up, and covers a support column to the main entrance covered walkway.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. All records or other information located on the premises or contained in computer related equipment and electronic or digital storage devices which there is probable cause to believe contain, or constitute evidence, fruits, or instrumentalities of, violations of 18 U.S.C. § 287, False Claims, 18 U.S.C. § 1001, False Statements, 18 U.S.C. § 1343, Wire Fraud, and 18 U.S.C. § 1349, Conspiracy to Commit Wire Fraud, between April 1, 2018, and the present, including but not limited to any and all documents, logs, notes, records, or other files (including prior versions and drafts of files, deleted files, and fragments of files) containing or purporting to contain, or purporting to be:

a. Documents and/or correspondence between any representative of Vizocom ICT LLC ("Vizocom") and any representative of the U.S. Government;

b. Documents and/or correspondence between any representative of Vizocom and any representative of Mastodon Design and/or CACI International Inc.;

c. Documents and/or correspondence with Alpha Antenna or any other third-parties related to the supply, purchase, or shipping of antennas to the U.S. Government;

d. Documents and/or correspondence regarding the purchase, sale, manufacture, or testing of antennas that were intended to be sold to the U.S. Government or, alternatively, used to fulfill RFQ N0042119Q0303 and/or contract number N0042119P0467;

e. Documents and/or correspondence regarding the purchase, sale, manufacture, or testing of antennas matching Mastodon Design Part Number MD1008-1710-01, and any payments related to the purchase, manufacture, or inspection of antennas;

f. Documents and/or correspondence regarding the receipt of payment from the U.S. Government related to RFQ N0042119Q0303, contract number N0042119P0467, and/or the sale of Mastodon Design Part Number MD1008-1710-01, and any payments related to the purchase or manufacture of antennas;

g. Vizocom internal documents and/or correspondence regarding any and all of the above topics and/or subjects;

h. Any and all documents relating to financial transactions executed by Vizocom fulfilling RFQ N0042119Q0303 and/or contract number N0042119P0467;

i. Any and all business records showing the operation, financing, administration, accounting, bookkeeping or management of Vizocom; and

j. All appointment books, schedules, calendars, list of contacts, telephone message slips, phone records, diaries, memos, and all other similar items that appear to have been used by any representative of Vizocom.

2. All images, messages, and communications regarding methods to avoid detection by the U.S. Government and/or law enforcement;

3. Any and all documents, records, or correspondence pertaining to occupancy, ownership, or other connection to the **TARGET PREMISES**;

4. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to, the specified criminal offenses. The following definitions apply to the terms as set out in the affidavit and attachment:

a. Computer hardware: Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the term "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

5. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

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

6. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software, or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possibly recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file, or storage area, shall cease.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, John Doyle, being duly sworn, hereby state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following premises, as further described in Attachment A:

> Vizocom ICT LLC ("Vizocom"), located at 1506 Constancia Way, El Cajon, California 92019 ("**TARGET PREMISES**")

and to seize evidence of the Target Offenses (defined in paragraph 2, *infra*), including any computers, electronic media, or files seized from the **TARGET PREMISES**, as further described in Attachment B. Attachments A and B are incorporated herein by reference.

2. There is probable cause to believe that evidence, instrumentalities, and/or fruits of the following offenses (collectively, the "Target Offenses") will be found within the **TARGET PREMISES**:

a. False Claims, in violation of 18 U.S.C. § 287;

b. False Statements, in violation of 18 U.S.C. § 1001;

c. Wire Fraud, in violation of 18 U.S.C. § 1343; and

d. Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349.

3. The facts and information contained in the affidavit are based upon my personal knowledge, the investigation and observations of other agents involved in the investigation, information obtained from interviews of witnesses, a review of documents and other records obtained during the course of the investigation, my training and experience, and the training and experience of other agents with whom I have consulted. This affidavit does not include each and every fact known to the government, but only those facts necessary to support a finding of probable cause to support the requested warrant.

/ /

/ /

BACKGROUND AND TRAINING

4. I am a Special Agent with the U.S. Department of Defense, Defense Criminal Investigative Service ("DCIS"), assigned to the Southern Maryland Resident Agency. As a Special Agent with DCIS, I am authorized to investigate crimes involving computer intrusions and other financial crimes governed by federal law, including Title 18 of the United States Code. I was so employed from 2007-2014, and then returned to DCIS in 2015. As a special agent of the DCIS, I am authorized to make arrests for felony offenses. I have over 20 years of federal law enforcement experience. In addition to DCIS, I have also been employed by the Department of the Interior – Office of the Inspector General, Food and Drug Administration – Office of Criminal Investigations, and U.S. Immigration and Customs Enforcement. I have a B.A. in Criminal Justice and have received extensive training from the Federal Law Enforcement Training Center (FLETC) in the area of white collar crime, to include attendance of the Money Laundering and Asset Forfeiture Training Program and Procurement Fraud Investigations Training Program. I specialize in investigations of fraud against the Department of Defense, contract fraud, bribery of public officials, and false claims to the government. During my tenure, I have worked extensively on contract fraud and public corruption cases, particularly complex cases, and thus I am familiar with the techniques, strategies, and behavior of individuals who have defrauded the government or have made false claims to the government, and who seek to conceal such illicit activities from detection by law enforcement.

PROBABLE CAUSE

Vizocom's Sale of Counterfeit Antennas to the U.S. Navy

5. In October 2019, the DCIS Mid-Atlantic Field Office was contacted regarding the alleged sale of counterfeit antennas by Vizocom to the U.S. Navy.

6. On April 25, 2019,[1] the Naval Air Warfare Center Aircraft Division ("NAWCAD"), Patuxent River, Maryland, issued a Request for Quote ("RFQ"), N0042119Q0303, which sought quotes for the purchase of 450 Mastodon Design

[1] All dates and times are approximate and omit "on or about" for the sake of brevity.

("Mastodon") antennas to be utilized by members of the U.S. Naval Special Warfare Command ("NSWC"). In order to maximize procurement opportunities for small businesses, the Rapid Acquisition Team ("RAC"), NAWCAD, which was responsible for this procurement effort, offered priority to qualified small businesses. The RFQ indicated that the U.S. Government intended to purchase the antennas on a firm-fixed price basis—*i.e.*, that the price was not subject to adjustment based on the contractor's cost in performing the contract.

7. A requirement of the RFQ was that the antennas supplied be Mastodon Design brand antennas. Accordingly, "Section B – Supplies or Services and Prices" of the RFQ explicitly required that the antennas supplied carry the Mastodon Part Number (P/N): MD1008-1710-01. This is a part number specific to the "Scourge" VHF/UHF[2] body-worn antenna manufactured by Mastodon of Rochester, New York. CACI International Inc. is the parent company of Mastodon. The RFQ also stated that the offeror "MUST BE AN AUTHORIZED Mastodon Design DISTRIBUTOR/RESELLER." The deadline for bids in the RFQ was May 2, 2019.

8. On May 1, 2019, Dennis Marco from Vizocom's Procurement Department sent an e-mail—using a vizocom.com email address—to Mastodon requesting a quote for 450 Mastodon antennas, P/N MD1008-1710-01. In response, Mastodon informed Marco that the price (including delivery to destination) would be $165,109.50. Vizocom submitted a timely electronic bid for the RFQ through the government portal for Federal Business Opportunities. Marco also emailed Vizocom's bid from a vizocom.com email address. In his email signature, Marco provided a San Diego, California, address for Vizocom. Based on additional investigation, I have reason to believe that Vizocom does not conduct business out of that San Diego address, but instead operates out of the **TARGET PREMISES**. *See infra* ¶ 19. Vizocom's bid was $165,109.50—the exact amount quoted by Mastodon. The header of the Vizocom price proposal stated that the company's address is the **TARGET PREMISES**:

[2] Very High Frequency and Ultra High Frequency—two sets of radio wave signals.

Vizocom - www.vizocom.us - info@vizocom.com - +1 619 350 5980
1506 Constancia Way, E Cajon, CA 92019
ISO Certified Small Business
DUNS 079495111 CAGE # 7ER72 EIN 98-0662559

Date	2 May, 2019
Quote #	VZO-19-DE05022
Client	Navy
RFQ #	N0042119Q0303
Valid until	90 days

05/01

9. On May 7, 2019, a Purchasing Agent at NAWCAD emailed Marco—at a vizocom.com email address—to inform him that Mastodon did not require reseller agreements and to confirm that the antennas Vizocom intended to supply would be covered under Mastodon's warranty. Marco responded that he had spoken with Mastodon and that the items were covered under its warranty and that Vizocom also provided a one year limited warranty.

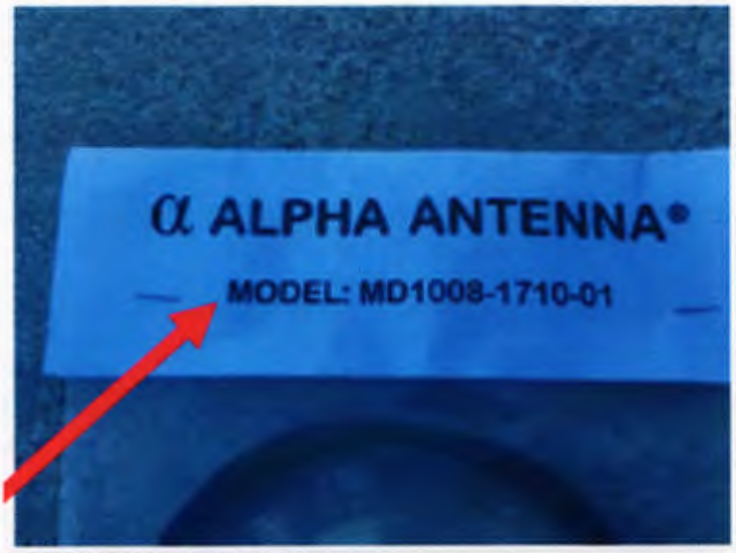
10. On May 14, 2019, the U.S. Navy awarded the contract to Vizocom for $165,109.50. The contract number was N0042119P0467. On May 15, 2019, NAWCAD issued an "Order for Supplies or Services" (DD Form 1155) to Vizocom for contract number N0042119P0467. Page one of the order listed the contractor—Vizocom—and the address for Vizocom—the **TARGET PREMISES**. Consistent with the RFQ, NAWCAD's order was for 450 Mastodon antennas at a cost of $366.91 each, for a total of $165,109.50.

11. On or before August 1, 2019, the completion date of the contract, Vizocom delivered 450 antennas to the U.S. Navy. The shipping labels for these antennas stated that they were shipped from Alpha Antenna in Pleasant Hill, Missouri to the U.S. Navy in St. Inigoes, Maryland. Consistent with the specifications on the RFQ and the DD 1155, the delivered antennas each had the requisite Mastodon part number etched on them. A purchase order issued to Alpha Antenna by Vizocom, dated July 17, 2019, requested testing, packaging, and sealing for 450 antennas for $12,208.50. This purchase order listed

the billing address for Vizocom as the **TARGET PREMISES**, and requested that the antennas be shipped to the U.S. Navy.

12. On July 30, 2019, George Attar ("**Attar**"), with the email address finance@vizocom.com, initiated an invoice and payment in the Wide Area Work Flow ("WAWF") system, which is used by the government and vendors to submit invoices and initiate payments. The payee was Vizocom at the **TARGET PREMISES**. On August 7, 2019, Vizocom was paid $165,109.50 by the U.S. Navy, pursuant to the contract. The payment was made via electronic funds transfer to Vizocom's Bank of America Account Number ending in 6928.

13. The antennas provided by Vizocom to the U.S. Navy stated Alpha Antenna on the packaging and listed the Mastodon antenna P/N MD1008-1710-01:



These antennas also had the Mastodon part number printed on the metal connector:

14. After the U.S. Navy received and began distribution of the antennas to the end users, the Tactical Communications Command within NSWC notified Special Communications Mission Solutions, the U.S. Navy Technical Point of Contact for the contract, that the Vizocom antennas differed physically from the Mastodon antennas and were of poorer quality. NSWC had previously received and utilized legitimate Mastodon antennas matching this part number. NSWC subsequently contacted Mastodon to find out the reason for the discrepancy in the antennas. Mastodon told NSWC that the antennas that Vizocom had provided were not supplied by Mastodon and that the serial numbers printed on the antennas were in fact counterfeit.

15. After Mastodon was contacted by NSWC, I have been informed that CACI's General Counsel spoke with Alok Kumar, Director of Sales & Operations at Vizocom. According to CACI, CACI informed Vizocom that CACI had learned from the U.S. Navy that Vizocom had supplied counterfeit Mastodon antennas to the U.S. Government. CACI demanded that Vizocom cease such activity immediately. CACI informed your affiant about this discussion with Vizocom and also told your affiant that Alpha Antenna never contacted Mastodon about antennas, nor is Alpha Antenna an authorized distributor or reseller of Mastodon antennas. Moreover, Vizocom never placed an order with Mastodon for these (or any other) antennas.

Vizocom's Operation at the TARGET PREMISES

16. According to California business filings, the **TARGET PREMISES** is the registered address for Vizocom and **Attar** is the Chief Executive Officer ("CEO") at

Vizocom. In the System for Award Management ("SAM")—a portal that current and potential government vendors use in order to be awarded contracts by the U.S. Government—**Attar** is listed as the point of contact with an address at the **TARGET PREMISES**. Moreover, Vizocom's profile with the U.S. Small Business Administration ("SBA") lists **Attar** as the point of contact and Vizocom's address as the **TARGET PREMISES**.

17. On September 17, 2018, the Department of the Army, Office of the Judge Advocate General, Procurement Fraud Division, contacted Vizocom to inform the company that it had been proposed for debarment from future contracting with the U.S. Government. The letter was addressed to Emad Al Attar at "Vizocom ICT LLC d/b/a Ruyat Al Mantaga for General Trading LLC." As is relevant to this affidavit, the **TARGET PREMISES** was listed as the business address for Vizocom.

18. According to 2019-2020 Tax Records for San Diego County, California, the **TARGET PREMISES** is owned by Fadi Attar. The deed filed in the San Diego County Recorder's Office reflected a deed transfer to Fadi Al Attar dated July 31, 2014. Additionally according to the San Diego County Recorder's Office, a Declaration of Trust, "The Fadi Attar Living Trust," was recorded on February 17, 2016, at the request of **Attar** with a mailing address listed as the **TARGET PREMISES**. The Grantor and the Trustee of the Trust is Fadi Attar and the Trust Property is the **TARGET PREMISES**. **Attar** is named as the successor Trustee and **Attar** along with Anam Gogi Attar are named as the beneficiaries of the Trust. The Declaration of Trust was signed by Fadi Attar and witnessed and notarized.

19. On its website, Vizocom lists its business address as 101 West Broadway, Suite 342, San Diego, California 92101. This building is a 20-story business district skyscraper bearing the "Morgan Stanley" name. On November 7, 2019, law enforcement visited the building to determine if Vizocom occupies these premises. In the main lobby on the ground floor, law enforcement observed a digital directory. "Vizocom ICT LLC" was listed under Suite 300, along with several other company names (also listed as residing

in that suite). Law enforcement entered the third floor from the elevator and encountered a receptionist at a front desk and observed what appeared to be safety deposit boxes or mail boxes numbered A1 through A30, B1 through B30, C1 through C30, and D1 through D30. None of the locked boxes had names or any other identifying markers. The entire floor appeared to be one large suite with multiple cubicle style or small partitioned offices with glass windows, many of which were frosted glass with company names and logos etched on the glass. Names of some companies included "GURU," "Borders," and "FYC." No company name or logo for Vizocom or Vizocom ICT LLC was identified on any of the cubicle style or partitioned glass office entrances. An internet search for the property address and suite number indicated Davinci Virtual, along with at least one other virtual office space provider company, provides virtual office space to other companies at that address. Specifically, Davinci Virtual rents virtual office space to companies that do not need dedicated or permanent office space, providing services such as: (i) a professional business address; (ii) mail receipt and forwarding; (iii) access to meeting spaces and workspaces; and (iv) lobby directory listing (among other services). Corporate representatives of Irvine Company Office Properties, the corporate property owner, described the location to agents as a "workshare environment."

20. Law enforcement has also conducted surveillance of the **TARGET PREMISES**. Law enforcement identified a black or dark color, four-door, Honda Civic with California license plate "7JVB320" parked in the driveway of the **TARGET PREMISES** on November 21, 2019. This vehicle is registered to Fadi Attar. Additionally, a silver Nissan compact sedan with California license plate "7MUN641" was parked on the street in front of the **TARGET PREMISES**. This vehicle is registered to **Attar** at the **TARGET PREMISES**. Both vehicles were observed at the **TARGET PREMISES** during subsequent surveillance conducted on November 26 and 27, 2019. Additionally, on November 26, 2019, an individual matching **Attar's** description, obtained from his California driver's license, was seen leaving the **TARGET PREMISES** with a black brief case and driving away in the silver Nissan.

Probable Cause to Find Records in the TARGET PREMISES

21. In the pages above, I have identified a number of facts which lead me to believe that evidence, instrumentalities, and/or fruits of the Target Offenses will be located in a search of the **TARGET PREMISES**. Some of these facts are restated below:

a. Vizocom states in its California business filings that its registered address is the **TARGET PREMISES**;

b. When registering with SAM and the SBA, Vizocom provided the **TARGET PREMISES** as its business address;

c. **Attar** is listed as the CEO of Vizocom and California property records indicate that **Attar** has a legal interest in the **TARGET PREMISES**;

d. Vizocom does not appear to operate out of the business address that it publicizes on its website;

e. Vizocom's bid for RFQ N0042119Q0303 stated that its business address is the **TARGET PREMISES**; and

f. Once the alleged Mastodon antennas were delivered, **Attar** initiated a payment through WAWF, which listed the payee as Vizocom at the **TARGET PREMISES**.

22. In addition to the facts above, from knowledge, training, and experience involving investigations of fraudulent activities and the training and experience of other agents with whom I am working in this investigation, I know:

a. Those involved in schemes such as the one described above often maintain records, receipts, notes, ledgers, bank deposit receipts, money transfer receipts, credit card receipts, money order receipts, and other papers relating to wire fraud and money laundering; and that the aforementioned records, receipts, note ledgers, etc., are maintained where they are readily accessible, including in places controlled by the criminals (such as their residences). In addition, I know that some of the information related to fraud is often stored in computer equipment, smart phones, and other

electronic storage media. Based on the evidence gathered in the investigation to date, the employees of Vizocom use email to communicate with third parties (including when contracting with the U.S. Government), and email is commonly stored on electronic devices, and sent and received using electronic devices as instrumentalities;

b. That it is common for businesses, including businesses operating out of residences or purporting to do so, to maintain business financial records, such as payment, tax, and expenses information; information related to bank accounts, wire payments, and receipts for any payments or expenses; and associated correspondence and records, in both electronic and written form, at addresses associated with the business and its principals, so that the records are readily accessible;

c. That it is common for businesses that engage in government contracting services to maintain information regarding their current and previous contracts with the U.S. Government; their current and previous contracts with suppliers, shipping companies, and other third parties that are and have assisted the business in applying for or fulfilling the government contracts; and associated correspondence and records, including but not limited to shipping records, in both electronic and written form, at addresses associated with the business and its principals, so that the records are readily accessible;

d. That it is common for businesses that engage in government contracting bidding to maintain information regarding market research, including determining specifications and information regarding the items being solicited by the U.S. Government, as well as competitor prices, in order to ensure the lowest bid, and that such information and records are maintained in both electronic and written form, at addresses associated

with the business and its principals, so that the information is readily accessible;

e. That it is common for businesses that engage in government contracting services to maintain information from parts and services suppliers, including conducting their own bidding process in order to ensure the lowest bid to the U.S. Government, and that such information and records are maintained in both electronic and written form, at addresses associated with the business and its principals, so that the information is readily accessible for future contracting efforts;

f. That it is common for businesses that engage in government contracting to have records on their computer systems regarding access to U.S. Government websites associated with the soliciting, bidding, and contracting process, including but not limited to SAM, SBA, WAWF, and the Federal Business Opportunities portal;

g. That it is common for employees and representatives of a company involved in fraudulent activities to maintain addresses, telephone numbers, and communications in books, on papers, and in computers/electronic media which reflect names, addresses, telephone numbers of, and communications with, their fellow employees, representatives, and associates in the fraudulent activities; and

h. That it is common for persons involved in fraudulent activities to hide the proceeds of bank transactions and records of fraudulent transactions in secure locations within their residences, automobiles, and business and storage facilities for their ready access and to conceal them from law enforcement.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. As described above and in Attachment B, this application seeks permission to search for records that might be found in the **TARGET 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 electronic 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).

24. *Probable cause*. I submit that if a computer or storage medium is found in the **TARGET 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. 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 "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."

25. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the **TARGET PREMISES** 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, e-mail 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 computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address

books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer 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 computer 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. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

26. *Necessity of seizing or copying 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. 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 in the **TARGET PREMISES**. However, taking the storage media off-site and reviewing them in a controlled environment will allow their 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.

d. *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 or imaging 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, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. *See infra* ¶¶ 27(b)-(j).

Business Computer Search Protocol

27. With the approval of the court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers found on the premises that may contain information subject to seizure pursuant to this warrant:

Incremental Search

a. Vizocom is a functioning company with an indeterminate number of employees. A seizure of the company's computer network may have the unintended and undesired effect of limiting the company's ability to provide lawful services to its legitimate customers. Consequently, the agents who execute the search will use an incremental approach to minimize the inconvenience to the company's customers, minimize the intrusion into the privacy of uninvolved third parties, and minimize the need to seize equipment and data. This incremental approach, which will be explained to all of the agents on the search team before the search is executed, will proceed as follows:

i. Upon arriving at the business to execute the search, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) willing to assist law enforcement with the identification of relevant systems and with the copying of computer files from network servers and other systems reasonably believed to contain information within the scope of the warrant. If the agents succeed at locating such an employee and are able to obtain copies of the relevant data in this fashion, the agents will not create a forensic image of the entire network. Imaging network servers is complex, time-consuming, usually interferes with any legitimate business activities and/or computer access, and can result in the acquisition of vast amounts of irrelevant data. Workstations and laptops believed to contain relevant data, however, may be imaged onsite or taken for imaging offsite, as provided above and below.

ii. If the business's employees choose not to assist the agents, the search team will attempt to locate network servers and will attempt to identify relevant data stores including user directories, file shares, electronic mail accounts and logs, and make electronic copies of the data stores reasonably believed to contain information subject to the warrant.

iii. If identifying and copying data stores onsite is technically or logistically not feasible, the entire server network may be imaged. As discussed below, whether the image is obtained onsite or offsite will be determined by technical issues, time-constraints, and safety concerns. After the images are obtained, the data will be analyzed as provided below.

iv. To the extent that there is probable cause to believe that information within the scope of this warrant may be found not only on servers, but

also on personal computers, workstations, laptops, and other electronic storage devices located at the business, such computers and devices will be forensically imaged onsite or offsite as provided below.[3]

Forensic Imaging

b. After securing the premises, or if sufficient information is available pre-search to make the decision, the executing agents will determine the feasibility of obtaining forensic images of electronic storage devices while onsite. A forensic image is an exact physical copy of the hard drive or other media. A forensic image captures all the data on the hard drive or other media without the data being viewed and without changing the data. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. The feasibility decision will be based upon the number of devices, the nature of the devices, the volume of data to be imaged, the need for and availability of computer forensics specialists, the availability of the imaging tools required to suit the number and nature of devices found, and the security of the search team. The preference is to image onsite if it can be done in a reasonable amount of time and without jeopardizing the integrity of the data and the agents' safety. The number and type of computers and other devices and the number, type, and size of hard drives are of critical importance. It can take several hours to image a single hard drive - the bigger the drive, the longer it takes. As additional devices and hard drives are added, the length of time that the agents must remain onsite can become dangerous and impractical.

[3] Forensic imaging of personal computers, workstations, laptops, and other electronic storage devices located at the **TARGET PREMISES** will be required should no network servers be located at the business.

c. If it is not feasible to image the data on-site, computers and other electronic storage devices, including any necessary peripheral devices, will be transported offsite for imaging. After verified images have been obtained, the owner of the devices will be notified and the original devices returned within sixty (60) days of seizure absent further application to this court.

d. Computers and other electronic storage devices and media that are retained as instrumentalities will not be returned to its owner. The owner will be provided the name and address of a responsible official to whom the owner may apply in writing for return of specific data not otherwise subject to seizure for which the owner has a specific need. The identified official or other representative of the seizing agency will reply in writing. In the event that the owner's request is granted, arrangements will be made for a copy of the requested data to be obtained by the owner. If the request is denied, the owner will be directed to Rule 41(g) of the Federal Rules of Criminal Procedure.

Identification and Extraction of Relevant Data

e. After obtaining a forensic image, the data will be analyzed to identify and extract data subject to seizure pursuant to this warrant. Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment, and software. There are thousands of different hardware items and software programs, and different versions of the same programs, that can be commercially purchased, installed, and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office or home environment can be different with respect to configuration, including permissions and access rights, passwords, data storage, and security. It is not unusual for a computer forensic examiner

to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

f. Analyzing the contents of a computer or other electronic storage device, even without significant technical challenges, can be very challenging. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process for several reasons. The computer may have stored metadata and other information about a relevant electronic record – e.g., who created it, when and how it was created or downloaded or copied, when it was last accessed, when it was last modified, when it was last printed, and when it was deleted. Keyword searches may also fail to discover relevant electronic records, depending on how the records were created, stored, or used. For example, keywords search text, but many common electronic mail, database, and spreadsheet applications do not store data as searchable text. Instead, the data is saved in a proprietary non-text format. Documents printed by the computer, even if the document was never saved to the hard drive, are recoverable by forensic programs because the printed document is stored as a graphic image. Graphic images, unlike text, are not subject to keyword searches. Similarly, faxes sent to the computer are stored as graphic images and not as text. In addition, a particular relevant piece of data does not exist in a vacuum. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed the data requires a search of other events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which user had logged in, whether users share passwords, whether the computer was connected to other computers or networks, and whether the user

accessed or used other programs or services in the time period surrounding events with the relevant data can help determine who was sitting at the keyboard.

g. It is often difficult or impossible to determine the identity of the person using the computer when incriminating data has been created, modified, accessed, deleted, printed, copied, uploaded, or downloaded solely by reviewing the incriminating data. Computers generate substantial information about data and about users that generally is not visible to users. Computer-generated data, including registry information, computer logs, user profiles and passwords, web-browsing history, cookies and application and operating system metadata, often provides evidence of who was using the computer at a relevant time. In addition, evidence such as electronic mail, chat sessions, photographs and videos, calendars and address books stored on the computer may identify the user at a particular, relevant time. The manner in which the user has structured and named files, run or accessed particular applications, and created or accessed other, non-incriminating files or documents, may serve to identify a particular user. For example, if an incriminating document is found on the computer but attribution is an issue, other documents or files created around that same time may provide circumstantial evidence of the identity of the user that created the incriminating document.

h. Analyzing data has become increasingly time-consuming as the volume of data stored on a typical computer system and available storage devices has become mind-boggling. For example, a single megabyte of storage space is roughly equivalent to 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is roughly equivalent to 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to 2 terabytes (2,000

gigabytes) of data. And, this data may be stored in a variety of formats or encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer). The sheer volume of data also has extended the time that it takes to analyze data. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. And, once reviewed, relevant data leads to new keywords and new avenues for identifying data subject to seizure pursuant to the warrant.

i. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including hashing tools to identify data subject to seizure pursuant to this warrant, and to exclude certain data from analysis, such as known operating system and application files. The identification and extraction process, accordingly, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred twenty (120) days from the date of seizure pursuant to this warrant, absent further application to this court.

j. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

Genuine Risks of Destruction of Data

k. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically-stored data can be permanently deleted or modified by users possessing basic computer skills. In this case, only if the subject receives advance warning of the execution of this warrant, will there be a genuine risk of destruction of evidence.

//

Prior Attempts to Obtain Data

l. The United States has not attempted to obtain this data by other means.

Procedures to Protect Third Party Privacy

m. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant. In the event that the personnel lawfully conducting the analysis identify information pertaining to crimes outside the scope of the warrant, such information will not be used except to obtain a new warrant authorizing a search for such information. In the event a new warrant is obtained, the government may make use the data seized in any lawful manner. Absent a new warrant, the personnel conducting the analysis may continue to search for and seize data only within the scope of this warrant.

28. In light of the issues enumerated above, your affiant requests the Court's permission to seize the computer hardware (and associated peripherals) and storage media that are believed to contain some or all of the evidence described in the warrant, and conduct an off-site search of the items for relevant evidence if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer items on-site for this evidence.

CONCLUSION

29. Based on the facts set forth herein, I respectfully submit that there is probable cause to believe that the **TARGET PREMISES**, as further described in Attachment A, contains evidence, fruits, and instrumentalities of the Target Offenses.

30. Therefore, I request the issuance of a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure authorizing law enforcement to search the **TARGET PREMISES** described in Attachment A and seize the items listed in Attachment B.

/ /

31. I affirm under penalty of perjury that the facts and circumstances outlined in this affidavit are true and accurate to the best of my knowledge and belief.

I swear the foregoing is true and correct to the best of my knowledge and belief.

John Doyle
Defense Criminal Investigative Service

Subscribed and sworn to before me this 16th day of December, 2019.

Hon. Michael S. Berg
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched is 1506 Constancia Way, El Cajon, CA 92019, and any and all outbuildings, appurtenances, storage areas, and locked containers, associated therewith (the "**TARGET PREMISES**"). The property is further described as a single family dwelling with a two car garage located on the front south west corner of the house. The garage door is white in color with four narrow starburst style windows that line the top length of the door. The exterior appears to be a white or light tan stucco with red brick corners. The brick exterior covers the corners of the garage from the ground up, and covers a support column to the main entrance covered walkway.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. All records or other information located on the premises or contained in computer related equipment and electronic or digital storage devices which there is probable cause to believe contain, or constitute evidence, fruits, or instrumentalities of, violations of 18 U.S.C. § 287, False Claims, 18 U.S.C. § 1001, False Statements, 18 U.S.C. § 1343, Wire Fraud, and 18 U.S.C. § 1349, Conspiracy to Commit Wire Fraud, between April 1, 2018, and the present, including but not limited to any and all documents, logs, notes, records, or other files (including prior versions and drafts of files, deleted files, and fragments of files) containing or purporting to contain, or purporting to be:

a. Documents and/or correspondence between any representative of Vizocom ICT LLC ("Vizocom") and any representative of the U.S. Government;

b. Documents and/or correspondence between any representative of Vizocom and any representative of Mastodon Design and/or CACI International Inc.;

c. Documents and/or correspondence with Alpha Antenna or any other third-parties related to the supply, purchase, or shipping of antennas to the U.S. Government;

d. Documents and/or correspondence regarding the purchase, sale, manufacture, or testing of antennas that were intended to be sold to the U.S. Government or, alternatively, used to fulfill RFQ N0042119Q0303 and/or contract number N0042119P0467;

e. Documents and/or correspondence regarding the purchase, sale, manufacture, or testing of antennas matching Mastodon Design Part Number MD1008-1710-01, and any payments related to the purchase, manufacture, or inspection of antennas;

f. Documents and/or correspondence regarding the receipt of payment from the U.S. Government related to RFQ N0042119Q0303, contract number N0042119P0467, and/or the sale of Mastodon Design Part Number MD1008-1710-01, and any payments related to the purchase or manufacture of antennas;

g. Vizocom internal documents and/or correspondence regarding any and all of the above topics and/or subjects;

h. Any and all documents relating to financial transactions executed by Vizocom fulfilling RFQ N0042119Q0303 and/or contract number N0042119P0467;

i. Any and all business records showing the operation, financing, administration, accounting, bookkeeping or management of Vizocom; and

j. All appointment books, schedules, calendars, list of contacts, telephone message slips, phone records, diaries, memos, and all other similar items that appear to have been used by any representative of Vizocom.

2. All images, messages, and communications regarding methods to avoid detection by the U.S. Government and/or law enforcement;

3. Any and all documents, records, or correspondence pertaining to occupancy, ownership, or other connection to the **TARGET PREMISES**;

4. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to, the specified criminal offenses. The following definitions apply to the terms as set out in the affidavit and attachment:

a. Computer hardware: Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the term "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

5. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

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

6. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software, or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possibly recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of

language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file, or storage area, shall cease.