

b. CESAR MORENO, as President of Baja Horizon, Inc., entered into a "Membership Interest to Purchase Agreement" with David D. Connor and Christine K. Connor for the purchase of a yacht for \$1,800,010, with a closing date of September 29, 2006.

c. Several photos were taken of CESAR MORENO standing on the yacht that was purchased.

35. On or about July 16, 2008, I obtained a photograph from the California Department of Motor Vehicle (DMV) for a California resident named CESAR MORENO. I compared the DMV photograph of CESAR MORENO with the photographs taken by the Yacht dealership and determined that they are the same person.

36. On or about _____, 2008, I reviewed CESAR MORENO's bank account records and discovered that he received \$9,000 from Sorvill's bank account, which later he used as a down payment on a home in the State of Washington.

37. On July 12, 2008, I reviewed GRUPO's Global account records from September 1 through November 30, 2006 (the time period when Goodman sold NESTOR MORENO the yacht) and discovered a check made payable to "South Shore Yacht Sales" in the amount of \$540,000. As in the documents provided by the Yacht dealership, the check was dated August 28, 2006.

38. On July 12, 2008, I reviewed LINDSEY's Preferred Bank records (Account #XXXX132) between September 29, 2006 and November 28, 2006 (the time period when Goodman sold NESTOR

MORENO the yacht). During this time period, LINDSEY wired a total of \$3,378,932.70 into GRUPO's Global account. Although the amount of money LINDSEY transferred into GRUPO's Global account exceeded the cost of the yacht and the \$540,000 withdrawn from GRUPO's Global account, I know, based on my training and experience, that persons receiving bribe payments will often pay for very expensive items like a home or a yacht using multiple accounts in an effort to conceal the true source of the funds, and that the additional money LINDSEY wired into GRUPO's Global account was likely used, at least in part, to cover the payments towards the yacht that came from accounts other than GRUPO's Global account (\$1,260,000). In addition, in my training and experience, intermediaries often take a substantial fee for making illegal payments to foreign officials. Finally, if NESTOR MORENO is, in fact, the brother-in-law of ANGELA OR ENRIQUE AGUILAR, as ANGELA AGUILAR claimed on the form authorizing NESTOR MORENO's American Express credit card payments, any remaining funds in the GRUPO account may benefit NESTOR MORENO to the extent that they benefit his family.

THE AMEX BILLS

39. On July 12, 2008, I reviewed a February 5, 2008 letter Jane E. Bates (Bates), Global's Chief Compliance Officer, wrote to the SEC and learned the following:

a. Although NESTOR MORENO did not have a brokerage account with Global, he did have a Corporate American

Express (AMEX) credit card affiliated with GRUPO.

b. The payments for NESTOR MORENO's AMEX bills were paid by GRUPO per written instructions from ANGELA AGUILAR, acting as a Director of GRUPO.

40. On July 12, 2008, I reviewed NESTOR MORENO's AMEX statements from September 5, 2006 through January 5, 2008, and learned the following:

a. NESTOR MORENO incurred AMEX charges totaling \$164,791.22.

b. All of the payments towards NESTOR MORENO's AMEX balance were paid from GRUPO's Global account.

c. For each payment, ANGELA AGUILAR signed a form authorizing the transfer of funds from GRUPO's Global account to pay NESTOR MORENO's AMEX bill.

d. Under the "must provide detailed explanation" section, ANGELA AGUILAR wrote "brother-in-law of company owner," as the apparent justification for paying NESTOR MORENO AMEX bills.

41. On July 12, 2008, I reviewed each of the wires LINDSEY paid into GRUPO's Global account from January 12, 2007 through October 12, 2007, excluding "the Ferrari" and "the yacht" payments referenced above, and discovered that each of these wires contained a reference to either "CFE" and/or "outside service and commission."

42. On July 12, 2008, I reviewed all of the wires

between LINDSEY and GRUPO's Global account, including those discussed in the Ferrari, the Yacht and the AMEX sections referenced above (\$5,330,022.38), and discovered that they were all authorized by STEVE LEE, who served as a bank account signatory for LINDSEY.

H. CONTRACTS BETWEEN LINDSEY AND CFE MEXICO

43. On July 19, 2008, I reviewed printouts from the Mexican government's public access website for government documents, Portal de Obligaciones de Transparencia, at www.portaltransparencia.gob.mx/pot/, which lists, among other things, the contracts between LINDSEY and CFE Mexico. The printout shows each contract and the amount of each contract, in Mexican pesos. According to this printout, LINDSEY was awarded the following contracts from CFE Mexico:

- a. Contract number 700113303, starting on March 10, 2004, for 2,081,641 Mexican pesos.
- b. Contract number 700131808, starting on October 20, 2004, for 5,490,347 Mexican pesos.
- c. Contract number 700191011, starting on May 22, 2006, for 4,538,600 Mexican pesos.
- d. Contract number 700190421, starting on May 24, 2006, for 1,804,919 Mexican pesos.
- e. Contract number 700191352, starting on May 24,

2006, for 3,870,984 Mexican pesos.

f. Contract number 800311925, starting on June 11, 2007, for \$358,546 Mexican pesos.

g. Contract number 700195528, starting on July 3, 2006, for 4,931,881 Mexican pesos.

h. Contract number 700195444, starting on July 5, 2006, for 4,294,010 Mexican pesos.

i. Contract number 700197454, starting on July 20, 2006, for 116,341,284 Mexican pesos.

j. Contract number 700193790, starting on July 24, 2006, for 5,026,266 Mexican pesos.

k. Contract number 700197867, starting on August 3, 2006, for 3,285,777 Mexican pesos.

l. Contract number 700236626, starting on August 17, 2007, for 1,540,111 Mexican pesos.

m. Contract number 700237280, starting on August 29, 2007, for 1,174,892 Mexican pesos.

n. Contract number 700238137, starting on September 13, 2007, for 1,313,259 Mexican pesos.

o. Contract number 700238282, starting on September 17, 2007, for 937,649 Mexican pesos.

p. Contract number 700238207, starting on September 18, 2007, for 1,006,465 Mexican pesos.

q. Contract number 700238918, starting on September 21, 2007, for 941,813 Mexican pesos.

r. Contract number 700239186, starting on September 28, 2007, for 153,176 Mexican pesos.

s. Contract number 700240396, starting on October 3, 2007, for 938,298 Mexican pesos.

44. On or about September 25, 2008, I reviewed an online currency converter, as well as the currency exchange rate between the U.S. dollar and the Mexican peso for the time period of the above contracts. Although there was some minor fluctuation over the time period, the exchange rate was roughly nine point three Mexican pesos per one U.S. dollar. I compared this information with LINDSEY'S Bank of America account records and determined that between September 2, 2003 and July 18, 2008, CFE Mexico wired contract payments to LINDSEY totaling \$19,146,715.77 U.S. dollars.

I. LINK BETWEEN THE CONTRACTS AND THE LINDSEY PAYMENTS

45. On or about November 3, 2008, I reviewed the memo sections for each of the wires sent from LINDSEY's Preferred bank account to GRUPO's Global account between January 19, 2005 and February 14, 2007. I discovered that on at least six of the wires, the numbers referenced in the memo section of the wire matched the contract numbers for contracts CFE Mexico awarded to LINDSEY around that same time period.

J. EVIDENCE LINKING LINDSEY TO THE SUBJECT PREMISES

46. On or about July 11, 2008, I performed an internet search of LINDSEY's website (LINDSEY-usa.com) and learned that

LINDSEY lists its business and mailing address as the SUBJECT PREMISES.

47. On or about July 11 through July 15th, 2008, I reviewed LINDSEY's bank account records at the following banks and learned that on each of these records LINDSEY listed the SUBJECT PREMISES as its address:

- a. Bank of the West (Account #XXXXXX480), dated January 2003 through June 2, 2004;
- b. Preferred Bank (Account #XXXX132), dated January 2005 through February 2007; and
- c. United California Bank (Account #XXXXXX004), dated December 26, 2006 through May 31, 2008.

48. On June 18, 2008, FBI SA Guernsey conducted surveillance at the SUBJECT PREMISES and observed that (1) the five buildings described in paragraph 5 above are all either painted blue or have a blue metal roof; (2) buildings 1, 2, and 3 all have the word "LINDSEY" written on them; and (3) buildings 1, 2, 3, and 4 all have signs written in black letters on a yellow background, all of which tends to confirm that LINDSEY is housed within the five buildings located on the SUBJECT PREMISES.

K. TRAINING AND EXPERIENCE

49. During the course of my training and experience as a Special Agent and my conversations with other law enforcement agents, I have become familiar with the practices and methods of persons committing acts of business fraud and corruption, and

have learned that participants in such conduct routinely maintain records reflecting or attempting to disguise the fraudulent or corrupt activity. Retaining business records relating to the crime is often necessary for the owner to operate a business, know if the business is profitable, and give the appearance of complying with other laws, such as federal statutes relating to taxation. Typically, these records expressly reflect fraudulent or corrupt activity or, more often, an attempt to disguise the fraudulent or corrupt activity as legitimate business conduct. Moreover, business records often provide evidence of, among other things, how the crime was committed, who was involved, what the motivation was for commission, where various criminal conduct took place, the relationship among those who knowingly or unwittingly assisted, what happened to the profits of the crime, and whether those involved acted with criminal intent.

50. Therefore, based on my training and experience, I believe the following records are likely to be maintained by LINDSEY at the SUBJECT PREMISES, either in digital format or in a hard copy:

a. Business records relating to STEVE LEE, GRUPO, Sorvill, Asset Management Plus, CFE Mexico, ENRIQUE AGUILAR, ANGELA AGUILAR, NESTOR MORENO and/or CESAR MORENO and/or any agent or employee of any of the above (hereinafter collectively referred to as "SUBJECT PERSONS AND/ENTITIES"), including financial records, address lists, personal diaries,

ledgers, general ledgers, logs, telephone records, board minutes, memoranda, informal notes of meetings, brochures, promotional literature, incorporation and business license papers, documentation of ownership, corporate filings, and other documents relating to or reflecting the operation of a business involved in contracting with foreign governmental entities or with intermediaries;

b. Bank records relating to the SUBJECT PERSONS AND/OR ENTITIES, including applications, bank statements, cancelled checks, deposit slips, withdrawal transactions, records of wire transfers, wire transfer instructions, cashier's checks, certificates of deposits, and other financial instruments and commercial paper;

c. Records of income relating to the SUBJECT PERSONS AND/OR ENTITIES, including sales invoices, receipts, cash register tapes, and sales journals;

d. Records of expenses relating to the SUBJECT PERSONS AND/OR ENTITIES, including receipts, invoices, expense reports, account books of entry, records of payments to employees and others, cancelled checks, journals and ledgers of expenditures, and other means of keeping track of money;

e. Financial statements relating to the SUBJECT PERSONS AND/OR ENTITIES, including income statements, profit and loss statements, statements of cash flow, balance sheets, and income and expense projections;

f. Contractual documents relating to the SUBJECT PERSONS AND/OR ENTITIES, including bidding documents, requests for proposals, contracts, agreements, amendments, variances, purchase orders, laws or rules applying to bidding, and other similar documents;

g. Budget documents relating to the SUBJECT PERSONS AND/OR ENTITIES, including budgets and budget preparation materials, financial projections, revenue estimates, cost estimates, and other similar documents;

h. Inventory records relating to the SUBJECT PERSONS AND/OR ENTITIES, including purchase receipts, shipping information, and inventory journals);

i. Tax records relating to the SUBJECT PERSONS AND/OR ENTITIES, including preparation materials, payroll tax information, tax forms, completed returns, and supporting documentation;

j. Travel records relating to the SUBJECT PERSONS AND/OR ENTITIES, including passports, visas, visa applications, travel itineraries, expense reports, airline receipts, hotel receipts and entertainment records;

k. Contact information relating to any LINDSEY or LINDSEY INTERNATIONAL business, including lists of client companies, credit references, business cards, Rolodexes, electronic organizers and address books;

l. Correspondence relating to the SUBJECT

PERSONS AND/OR ENTITIES, including emails, facsimiles, letters, and logs of correspondence;

m. Telephone records relating to the SUBJECT PERSONS AND/OR ENTITIES, including bills, logs, and records of telephone calls;

n. Media reports relating to the SUBJECT PERSONS AND/OR ENTITIES; and

o. Audio/visual materials relating to the SUBJECT PERSONS AND/OR ENTITIES, including photographs, videotapes, and audio records.

VI.

CONCLUSION

51. Based on the foregoing, there is probable cause to believe that between September 2003 and May 2008, LINDSEY made payments into GRUPO's Global account totaling \$5,330,022.38. ENRIQUE AGUILAR, ANGELA AGUILAR, and CESAR MORENO, who claim to be relatives of NESTOR MORENO, used \$2,262,301 of that money to help buy NESTOR MORENO, a Mexican public official, a Ferrari, a yacht, and to make over \$100,000 in payments towards his AMEX credit card bills. During that same time period, CFE Mexico, where NESTOR MORENO was acting as a foreign official, awarded LINDSEY nineteen (19) government contracts worth \$14,911,659. Accordingly, there is probable cause to believe that the SUBJECT PREMISES will contain evidence of these corrupt payments, which violate Title 18, United States Code, Section 371 (Conspiracy),

Title 15, United States Code, Section 78dd-1, et seq. (Corrupt Payments to Foreign Officials), and Title 18, United States Code, Sections 1956 and 1957 (Money Laundering).

Date: _____

Farrell A. Binder
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me
on this ___ day of November, 2008.

United States Magistrate Judge

ATTACHMENT A

THE PREMISES TO BE SEARCHED

The premises to be searched is more particularly described as follows:

a. The business address and offices of LINDSEY located at 760 N. Georgia Avenue, Azusa, California 91702 ("SUBJECT PREMISES"), which is made up of five separate buildings located along the east side of North Georgia Avenue, between Foothill Boulevard and Eighth Street.

BUILDING #1

b. BUILDING #1 is located on the SUBJECT PREMISES. BUILDING #1 is a tan one story office building facing North Georgia Avenue with the numbers "760" affixed above the front door in black numerals on a white background. The front door to BUILDING #1 is made of tinted glass and is centered between two tinted glass windows that are the same length as the front door. The numbers "760" are also painted in black on a white background on the front of a cement walkway that leads to the front door. The exterior of BUILDING #1 has a brick facade with a flat pale blue metal roof. On either side of the front door of BUILDING #1 are four windows, and a planter, which holds bushes that grow between each window. At the top of the blue metal roof overhang of BUILDING #1, centered above the door, is a sign written in black letters on a yellow background that reads "LINDSEY." At the south end of BUILDING #1, also on the blue

metal roof overhang, is another sign with black lettering on a yellow background that reads "L" and has a lightning bolt running through the "L." Running perpendicular to, and in front of, BUILDING #1 are several parking spaces. All of the parking spaces are marked "reserved," with the exception of three spaces to the south, marked "visitor." Also visible from North Georgia Avenue is a side entrance on the south side of BUILDING #1. The side entrance is located approximately six to eight feet from the front of BUILDING #1, and has six steps leading up to the door from two sides.

BUILDING #2

c. BUILDING #2 is located on the SUBJECT PREMISES and is immediately to the south of BUILDING #1. BUILDING #2 is a pale blue corrugated metal building with three large sliding metal doors that face North Georgia Avenue and are protected by two chain link fences positioned directly in front of the metal doors. BUILDING #2 has a sign on the south side of the front facade written in black letters on a yellow background that reads "Lindsey Shipping & Receiving" with an arrow pointing north on North Georgia Avenue. BUILDING #2 has another sign written in black letters on a yellow background attached to the southeast corner of the building that reads "South Yard."

BUILDING #3

d. BUILDING #3 is located on SUBJECT PREMISES and is immediately to the south of BUILDING #2. BUILDING #3 is a

blue corrugated metal structure that faces North Georgia Avenue and is separated from BUILDING #2 by two gates and a tan brick wall that runs in between the two gates. The two gates between BUILDING #2 and BUILDING #3 are made of chain link, topped with barbed wire, and have warning signs indicating hazardous materials and private property. The tan brick wall between BUILDING #2 and BUILDING #3 is also topped with barbed wire, and has bushes running in front of it. BUILDING #3 has a door in the center of the building and a window on each side of the door. The numbers "730" are affixed towards the top of the door. Above the door and the numbers "730" is a sign written in black letters with a yellow background that reads "Lindsey."

BUILDING #4

e. BUILDING #4 is located on the SUBJECT PREMISES and is immediately to the north of BUILDING #1. BUILDING #4 is a blue building that faces North Georgia Avenue and is separated from BUILDING #1 by a small space of approximately two feet. BUILDING #4 has a door centered in the middle of the building, with two windows on each side of the door and a single step leading up to the door. There are bushes in front of all the windows. There is a light high above the door of BUILDING #4 and another light attached at the southeast corner of BUILDING #4. At the northeast corner of BUILDING #4 there is a sign written in black letters on a yellow background that reads "North Yard."

BUILDING #5

f. BUILDING #5 is located on SUBJECT PREMISES and is north of BUILDING #4. A chain link gate runs between BUILDING #4 and BUILDING #5, just to the north of BUILDING #4. The chain link gate connects to a tan brick wall that continues all the way to the north end of the SUBJECT PREMISES. Both the gate and wall that run between BUILDING #4 and BUILDING #5 are topped with barbed wire. BUILDING #5 is located immediately behind the brick wall and to the north of the chain link gate. BUILDING #5 is a blue structure with the words "Shipping & Receiving" written in white letters directly on the structure just below the roof line.

g. SUBJECT PREMISES include buildings 1, 2, 3, 4, and 5, and all attached and unattached rooms, attics, basements, garages, storage areas, computers, safes, lockers, containers, trash areas, surrounding grounds and outbuildings assigned to or a part of the SUBJECT PREMISES.

ATTACHMENT B

THE ITEMS TO BE SEIZED

The items to be seized at the SUBJECT PREMISES constitute evidence of violations Title 18, United States Code, Section 371 (Conspiracy), Title 15, United States Code, Section 78dd-1, et seq. (Corrupt Payments to Foreign Officials), and Title 18, United States Code, Sections 1956 and 1957 (Money Laundering), and are described as follows:

1. For the years 2003 through the present, the following items are to be seized:

RECORDS

a. Business records relating to STEVE LEE, GRUPO, Sorvill, Asset Management Plus, CFE Mexico, ENRIQUE AGUILAR, ANGELA AGUILAR, NESTOR MORENO and/or CESAR MORENO and/or any agent or employee of any of the above (hereinafter collectively referred to as "SUBJECT PERSONS AND/ENTITIES"), including financial records, address lists, personal diaries, ledgers, general ledgers, logs, telephone records, board minutes, memoranda, informal notes of meetings, brochures, promotional literature, incorporation and business license papers, documentation of ownership, corporate filings, and other documents relating to or reflecting the operation of a business involved in contracting with foreign governmental entities or with intermediaries;

b. Bank records relating to the SUBJECT PERSONS AND/OR ENTITIES, including applications, bank statements, cancelled checks, deposit slips, withdrawal transactions, records of wire transfers, wire transfer instructions, cashier's checks, certificates of deposits, and other financial instruments and commercial paper;

c. Records of income relating to the SUBJECT PERSONS AND/OR ENTITIES, including sales invoices, receipts, cash register tapes, and sales journals;

d. Records of expenses relating to the SUBJECT PERSONS AND/OR ENTITIES, including receipts, invoices, expense reports, account books of entry, records of payments to employees and others, cancelled checks, journals and ledgers of expenditures, and other means of keeping track of money;

e. Financial statements relating to the SUBJECT PERSONS AND/OR ENTITIES, including income statements, profit and loss statements, statements of cash flow, balance sheets, and income and expense projections;

f. Contractual documents relating to the SUBJECT PERSONS AND/OR ENTITIES, including bidding documents, requests for proposals, contracts, agreements, amendments, variances, purchase orders, laws or rules applying to bidding, and other similar documents;

g. Budget documents relating to the SUBJECT PERSONS AND/OR ENTITIES, including budgets and budget preparation

materials, financial projections, revenue estimates, cost estimates, and other similar documents;

h. Inventory records relating to the SUBJECT PERSONS AND/OR ENTITIES, including purchase receipts, shipping information, and inventory journals);

i. Tax records relating to the SUBJECT PERSONS AND/OR ENTITIES, including preparation materials, payroll tax information, tax forms, completed returns, and supporting documentation;

j. Travel records relating to the SUBJECT PERSONS AND/OR ENTITIES, including passports, visas, visa applications, travel itineraries, expense reports, airline receipts, hotel receipts and entertainment records;

k. Contact information relating to any LINDSEY or LINDSEY INTERNATIONAL business, including lists of client companies, credit references, business cards, Rolodexes, electronic organizers and address books;

l. Correspondence relating to the SUBJECT PERSONS AND/OR ENTITIES, including emails, facsimiles, letters, and logs of correspondence;

m. Telephone records relating to the SUBJECT PERSONS AND/OR ENTITIES, including bills, logs, and records of telephone calls;

n. Media reports relating to the SUBJECT PERSONS AND/OR ENTITIES; and

o. Audio/visual materials relating to the SUBJECT PERSONS AND/OR ENTITIES, including photographs, videotapes, and audio records.

SHREDDED DOCUMENTS

2. In order to search for documents that may have been destroyed, law enforcement personnel will seize all shredded paper and shredders.

DIGITAL DATA

3. As used above, the terms records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form, including in digital form on any digital device. The term "digital device" includes any electronic device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media; and security devices.

4. In searching for data capable of being read, stored or interpreted by a digital device, law enforcement personnel executing this search warrant will employ the following procedure:

i. Upon securing the premises, the law enforcement personnel executing the search warrant will, to the extent possible without requiring the use of special training in searching and seizing digital data, seek to determine if any digital device contains data falling within the scope of the items to be seized in the warrant. If they can make this determination without jeopardizing the integrity of the digital data and a digital device contains data falling within the scope of the items to be seized in the warrant, that digital device will be seized. If they cannot make this determination, or they believe they cannot make this determination, without jeopardizing the integrity of the digital data, law enforcement personnel trained in searching and seizing digital data (the "computer personnel") will be consulted (either on-site or off-site) to determine whether the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data contained on the digital device.

ii. If the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, it will be searched on-site and seized only if the search reveals it to contain any data that falls within the list of items to be seized set forth herein.

iii. If the digital device cannot be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, then the computer personnel will

determine whether it is practical to create a forensically sound image of the data contained on the digital device during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve that data. If it is practical, and the digital device cannot be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the computer personnel will make a forensically sound image of the data contained on the digital device (a "data image") during the execution of this search and shall seize the data image rather than the digital device itself.

iv. If the computer personnel determine it is not practical to perform an on-site search of the digital device or make an on-site data image within a reasonable period of time and without jeopardizing the ability to preserve data, then the digital device will be seized and transported to an appropriate law enforcement laboratory for review. The digital devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

v. In searching the digital device or data image[], the computer personnel may examine all of the data contained in the digital device or data image to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover

"deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

vi. If the computer personnel seize the digital device pursuant to subparagraph iv above or make a data image pursuant to subparagraph iii above, the computer personnel will initially search the digital device or data image within a reasonable amount of time not to exceed 60 days from the date of execution of the warrant. If, after conducting such an initial search, the case agents determine that the digital device or data image contains any data falling within the list of items to be seized pursuant to this warrant, the government will either (1) return the digital device, keeping a data image for further analysis, provided that, prior to such return, the owner and user(s) of the digital device stipulate individually and in writing to the authenticity and accuracy of the data image or (2) seek an order of the Court allowing the government to retain the original digital device for further analysis. If the digital device or data image does not contain any data falling within the list of the items to be seized pursuant to this warrant, the government will return the digital device or delete the data image. If the government needs additional time to determine whether the digital device or data image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the

Court within the original sixty day period from the date of execution of the warrant.

5. In order to search for data that is capable of being read or interpreted by a digital device, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

i. Any digital device capable of being used to commit, further or store evidence of the offense listed above;

ii. Any equipment used to facilitate the transmission, creation, display, encoding or storage of digital data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices and optical scanners;

iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones and personal digital assistants;

iv. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software used in the digital device;

v. Any applications, utility programs, compilers, interpreters and other software used to facilitate direct or indirect communication with the digital device;

vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or data stored on the digital device.