

United States District Court

STATE AND DISTRICT OF MINNESOTA

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

2400 Interlachen Road, Suite 316 Spring Park, Minnesota 55384

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Case Number:

08-MS-134 JSM

Att:

Clif Burns

FAX

202-674-7272

From:

I: Dan Browning

I2: 612-673-4493

as (name, dt)

I say:

believe that on the person of or on the premises known

2400 Inter

55384

in the State and District of Minnesota there is now concealed a certain person or property,
namely (describe the person or property)

Please see Attached List of Items to be Seized and Addendum.

which is (state one or more bases for search warrant and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

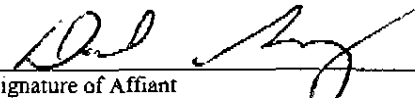
property that constitutes evidence of the commission of a crime, contraband, fruits of criminal activity, and/or means
of committing a crime

concerning a violation of Title 22, United States Code, Section(s) 2778.

The facts to support a finding of Probable Cause are as follows:

See Affidavit attached hereto and incorporated herein by reference.

Continued on the attached sheet and made a part hereof. Yes No



Signature of Affiant
DANIEL D. SCHWARZ, Special Agent
BICE

Sworn to before me, and subscribed in my presence

3/26/08 7:10 p.m.


Date and Time Issued

at Minneapolis, MN

City and State

The Honorable Janie S. Mayeron
UNITED STATES MAGISTRATE JUDGE

Name and Title of Judicial Officer



Signature of Judicial Officer
APR 07 2008
RICHARD D. SLETTEN
JUDGMENT ENTD
DEPUTY CLERK.

1

27

**LIST OF ITEMS TO BE SEIZED
ATTACHMENT A**

1. Books, records, receipts, notes, ledgers, diaries, journals, designated codes and other papers relating to violation of the Arms Export Control Act, Title 22, U.S.C., Section 2778.

2. Books, records, receipts, tax returns, bank statements, bank records, financial statements, credit card statements, money drafts, bank records, safe deposit box keys, safe deposit box documents, storage unit documents, safe combinations, storage unit keys, records and agreements for payment, and other documents and items evidencing the illegal Export of Arms from the United States.

3. United States Currency and financial instruments.

4. Photographs and/or drawings depicting any and all business related activities such as parts, merchandise, and records depicting business related exports from the US.

5. Sales receipts for items evidencing the expenditure of currency or currency equivalents related to violations of the Arms Export Control Act.

6. Documents, books, and papers reflecting names, addresses and/or telephone numbers of coconspirators, clients, or related business associates in and outside the US.

7. Books, records, receipts, notes, ledgers, invoices, bank records, purchase records, cash receipts, disbursement journals,

inventory records and other records relating to business operations.

8. Beepers and their memory, beeper records, telephone calling cards, telephone credit cards, cellular phones and their memory, cellular phone records, personal telephone books, telephone toll records, and records relating to the acquisition or use of communication devices, telephone answering machine tapes and their content.

9. Safes (agents may drill).

10. Computer equipment as described below:

Based upon my training, experience and information related to me by Agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to

conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing fifteen gigabytes of data are now commonplace in desktop computers.

Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 7.5 million pages of data, which, if printed out, would completely fill a 10' x 12' x 10' room to the ceiling.

Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading file names and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file, which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant may employ the following procedure:

Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

If the computer equipment and storage devices cannot be searched on-site, and it has been determined that the items are not instrumentalities or fruits of the offenses stated above, do not contain contraband, and are not otherwise illegally possessed, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data.

If the computer personnel determine it is not practical to perform an on-site search or make an on-site copy of the data, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage 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.

If law enforcement personnel determine, either on-site or during a subsequent off-site search, that any computer equipment, storage device or data (1) is an instrumentality of the offense stated above, meaning that it was designed or intended for the use of, or is being or has been used, as the means of committing the offense; (2) contains any contraband, such as counterfeit or stolen software, child pornography, national security information, or unauthorized access devices such as stolen credit card numbers; (3) is the fruits of criminal activity; or (4) is otherwise criminally possessed, the property shall be seized and not returned pursuant to Federal Rule of Criminal Procedure 41 (b).

Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above.

In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices 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.

If the computer personnel determine that the computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), the government will return these items within a reasonable period of time not to exceed 60 days from the date of seizure.

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

Any computer equipment and storage device capable of being used to commit, further or store evidence of the offenses listed above.

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

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, and personal digital assistants;

Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;

Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

11. Aerospace parts, accessories and business related inventory of aerospace parts and accessories contained within the business, whether known to be on the United States Munitions List or not; to include opened and unopened parcels, crates, and/or packages.

12 All the above described records whether stored on paper, on magnetic media such as tape, cassette, disk, diskette, or on

memory storage devices such as optical disks, programmable instruments such as telephones, electronic address books, electronic organizers, calculators, or other storage media, or in personal calculators, portfolios of the persons associated with the enterprise, together with indication of use, ownership, possession, or control of such records,

All of which are fruits, evidence and instrumentalities of a crime against the US, in violation of the Arms Export Control Act, Title 22, United States Code, 2778.

SEARCH WARRANT ADDENDUM

1. In conducting the search authorized by this warrant, the government shall make reasonable efforts to utilize computer search methodology that avoids searching files, documents or other electronically stored information which is not identified in the warrant.

2. If electronically stored data or documents have been identified and seized by the government pursuant to this warrant, the government may retain the original hard drive or other data storage mechanism. The person from whom the data storage device has been seized may request that the government provide him or her with electronic copies of the electronically stored data or documents by making a written request to the United States Attorney's Office, identifying with specificity the files, data, or software sought to be copied. The government must respond to all such requests within a reasonable amount of time, and must provide a copy of the electronically stored data or documents requested unless the copies requested constitute contraband, instrumentalities, or property subject to forfeiture.

3. Nothing in this warrant shall limit or prevent the government from seizing the computer as contraband or an instrumentality of a crime or commencing forfeiture proceedings against the computer and/or the data contained therein. Nothing in this warrant shall limit or prevent the owner of the computer from (a) filing a motion with the Court pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the Return of Property or (b) making a request of the government to return certain specified files, data, software or hardware.

4. The government shall establish a search methodology governing the review of seized data to ensure that no attorney-client privileged communications will be inadvertently reviewed by the prosecution team. In the event that documents or other records seized pursuant to this warrant are identified by the government as possibly containing attorney-client privileged communications, an Assistant United States Attorney, who is not a member of the prosecution team and who is not participating in the search, shall act as a "taint team" to set up a "Chinese wall" between the evidence and the prosecution team that will prevent any privileged material from getting through.

STATE OF MINNESOTA)
) SS AFFIDAVIT OF DANIEL D. SCHWARZ
COUNTY OF HENNEPIN)

I, Daniel D. Schwarz, being duly sworn, depose and states as follows:

1. I am a Special Agent assigned to the Department of Homeland Security, Immigration & Customs Enforcement (ICE), Special Agent in Charge, Minneapolis, Minnesota office. I have been a Special Agent with ICE, since March 1989. As a Special Agent with ICE, I have received training related to identifying the techniques, methods, and procedures employed by groups, organizations, companies, corporations, and individuals, to export goods and commodities in violation of United States export laws. In addition, I have received advanced instruction and training on how to conduct criminal investigations associated with export law violations, which included investigations associated with violations of the Arms Export Control Act (AECA), Title 22, U.S.C., Section 2778, and the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Part 120, et seq.

2. I make this Affidavit in support of an application for a search warrant for the premises located at 2400 Interlachen Road, Suite 316, Spring Park, Minnesota 55384, such property being the primary business location of Global Engineering Associates (GEA), a.k.a Global Trading. The primary business location will be referred to hereinafter as "the premises." There is also a

MBA
807-5771

952-471-9743
239-948-4328

Long Lake, MN
Martin Left 77 2/16/37
Wauzata
471-8205
952-412-389-5402 - avans

Bozith Springs
239-998-4328
239-992-8793
mag

suboffice associated with GEA located at 3333 Renaissance Blvd, Suite 212, Bonita Springs, Florida, 34134, referred to hereinafter as the "sub-office." Based on the following, I believe that at the premises, there will be found documents, records, and evidence related to the purchase, acquisition, sale, shipment, exportation, and/or control of United States Munitions List (USML) items, all of which constitute the instrumentalities and evidence of violations of the Arms Export Control Act, Title 22, United States Code, Section 2778.

3. The statements contained in this affidavit are based upon my personal knowledge and/or on information provided to me by other domestic and foreign law enforcement officers, agents, and personnel, as well as my experience, background and training. Because this affidavit is being submitted for the limited purpose listed above, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts I believe to be necessary to establish probable cause to support the search warrant sought at the premises.

BACKGROUND

4. Pursuant to the ITAR, certain materials and items, which are designated as USML items, require authorization, in the form of registration and licensing, by the United States Department of State (DOS), Directorate of Defense Trade Controls (DDTC), prior to

exportation from the United States. Based upon my training and experience, I know that U.S. based companies and individuals that act as intermediaries for the illegal transfer of USML material out of the United States, acquire USML items from domestic (U.S.) manufacturers and military surplus vendors. In order to facilitate and conceal the illegal transfer of the material abroad, the U.S. intermediary, in many instances, prepares commercial documentation that will allow the intended shipment to blend into the stream of legal exports leaving the United States. The referenced commercial documents can include any combination of purchase and sales orders, invoices, packing lists, bills of lading, and manifests, which serve to re-characterize and conceal the nature of the USML material, thereby presenting the appearance of legal business activity.

5. Based on my training, experience, and discussions with other agents who have been involved in the investigation of export related offenses, I know that it is common practice for exporters to retain records relating to their shipments, including records that are associated with illegal shipments of export-restricted items. Moreover, I know that exporters are required by law and regulation to retain various documents relating to the exportation of goods and services from the United States. Pursuant to the Export Administration Regulations (EAR) and the ITAR (22 C.F.R.

§123.22), generally, before shipping any defense article, an exporter must file a Shipper's Export Declaration (SED) with the District Director of Customs and Border Protection (CBP) at the port of exit. Additionally, the EAR requires exporters to keep and maintain records related to exports of commodities, software, or technology from the United States and any known re-exports, transshipments, or diversions of items exported from the United States. The EAR specifically requires that the following class of records must be maintained: (a) export control documents, as defined in part 772 of the EAR; (b) memoranda; (c) notes; (d) correspondence; (e) contracts; (f) invitations to bid; (g) books of account; (h) financial records; (i) restrictive trade practice or boycott documents and reports; and (j) other records pertaining to the types of transactions described in § 762.1(a) of this part, which are made or obtained by a person described in § 762.1(b) of this part. Moreover, all of the records required to be maintained by the EAR must be retained for five years from the latest of the following times: (a) the export from the United States of the item involved in the transaction to which the records pertain or the provision of financing, transporting or other service for or on behalf of end-users of proliferation concern as described in §§ 736.2(b)(7) and 744.6 of the EAR; (b) any known re-export, transshipment, or diversion of such item; (c) any other termination

of the transaction, whether formally in writing or by any other means; or (d) in the case of records pertaining to transactions involving restrictive trade practices or boycotts described in part 760 of the EAR, the date the regulated person receives the boycott-related request or requirement.

6. Additionally, based upon my training and experience, I know that one of the techniques used by persons, who illegally export USML material, is to prepare false documents for small shipments, which they export through commercial courier services such as DHL, Federal Express and the United Parcel Service. The combination of false, misleading or generic descriptions of the merchandise (as discussed previously), small shipment size, and the speed and volume of merchandise moving through the courier services, provides a high likelihood that the illegal shipments will avoid scrutiny by export enforcement authorities. Further, in the event that a parcel is inspected, few, if any, of the USML parts that I have experience with would be immediately recognizable as USML controlled items.

THE INVESTIGATION

7. In February 2008, the ICE office in Fort Myers (ICE RAC/FM), Florida initiated an investigation related to evidence suggesting that Martin Leff, President/CEO, of GEA, was attempting to acquire USML items that appeared to be intended for illegal

export. The ensuing investigation of GEA revealed that Leff is at the center of a scheme to, knowingly and willfully, export USML parts from the United States without the required registration and licensing, in violation of the AECA and the ITAR.

8. In an effort to obtain information and evidence related to the possible violations of the AECA, the ICE RAC/FM began to analyze the export shipments originating from the sub-office, which is located within the RAC/FM AOR. The ITAR, Section 127.4, authorizes ICE and Customs and Border Protection (CBP) to investigate, detain, or seize any export or attempted export of defense articles or technical data. The section allows ICE and CBP the opportunity to inspect the loading and/or unloading of any vessel, vehicle, or aircraft.

9. On March 6, 2008, ICE agents encountered an export shipment at the DHL Fort Myers Station, 10089 Amberwood Road, Fort Myers, FL 33913, which was picked up from the sub-office on this date. The shipment reflected the shipper as Global Trading, Martin Leff, 3333 Renaissance Blvd, Bonita Springs, Florida, 34134, United States. The consignee was Ultramare Singapore Pty, attention Vincent Teo, 8C Harvey Ave., Singapore, 489479. The export shipment was traveling on airway bill number 8875366555 and consisted of 3 boxes weighing approximately 84 pounds. According to the DHL driver the shipment was acquired from the sub-office

following a pick-up request from Leff. Upon further inspection of the export, ICE agents had acquired the commercial invoice, which was provided to DHL by Leff. The invoice contained 20 line items categorized as Propellers and Rotors and Parts Thereof. Additionally, Leff had provided information on the airway bill, which stated the shipment contained "civil" aircraft parts. The invoice reflected a sum total cost of \$45,403.00. During the course of the export inspection, ICE agents opened the packages to inspect the parts within. The packages contained a variety of aircraft parts. The invoice contained inside the packages did not mirror the commercial invoice provided to DHL by Leff. The invoice within the packages stated the shipment contained 20 line items and each was identified by a part number (p/n). According to Section 127.4(a) of the ITAR, ICE and CBP officers may take appropriate action to ensure observance of the subchapter as to the export or the attempted export of any defense article or technical data. This applies whether the export is authorized by license or by written approval issued under this subchapter. The ICE agents detained the export shipment from DHL for licensing review, which was documented on Customs Form 6051D # 0012815.

10. The RAC/FM researched the shipment to determine if the export contained any items or p/n categorized on the USML. The initial research suggested that the export shipment contained 1

p/n, totaling 7 separate pieces, categorized on the USML. The part is identified as p/n 617 01312, National Stock Number 6620001600834, Pressure Indicator. Vibro-Meter Inc., 144 Harvey Road, Londonberry, New Hampshire, 03053, manufactured the part. According to the manufacturer of the item, p/n 617 01312 was manufactured for the United States Navy on or about the year 1991. On March 12, 2008, the RAC/FM submitted a license determination request via the Exodus Accountability Referral System (EARS). On March 13, 2008, the request was sent to the DDTC/DOS. On March 13, 2008, the DDTC/DOS confirmed that p/n 617 01312 is on the USML, Category VIII (h), Aircraft and associated equipment, which is defined as components, parts, accessories, attachments, and associated equipment (including ground support equipment) specifically designed or modified for the articles in paragraphs (a) through (e) of category VIII, excluding aircraft tires and propellers used with reciprocating engines.

11. On March 12, 2008, ICE agents encountered a second shipment at the DHL Fort Myers Station, 10089 Amberwood Road, Fort Myers, Fl 33913, which was picked up from the sub-office on this date. The shipment reflected the shipper as Global Trading, Martin Leff, 3333 Renaissance Blvd, Bonita Springs, Florida, 34134, United States. The consignee was Ultramar Singapore Pty, attention Vincent Teo, 8C Harvey Ave., Singapore, 489479. The export

shipment was traveling on airway bill number 8877120103 and consisted of 4 boxes weighing approximately 114 pounds. According to the DHL driver the shipment was acquired from the premises following a pick-up request by Leff. Upon further inspection of the export, ICE agents had acquired the commercial invoice, which was provided to DHL by Leff. The invoice contained 16 line items categorized as Propellers and Rotors and Parts Thereof. Additionally, Leff had provided information on the airway bill, which stated the shipment contained "civil" aircraft parts. The invoice reflected a total cost of \$77,788.00. During the course of the export inspection, ICE agents opened the packages to inspect the parts within. The packages contained a variety of aircraft parts. The invoice contained inside the packages did not mirror the commercial invoice provided to DHL by Leff. The invoice within the packages stated the shipment contained 16 line items and each was identified by a p/n. The ICE agents detained the export shipment from DHL for licensing review, which was documented on Customs Form 6051D # 0007142.

12. The RAC/FM researched the shipment to determine if the export contained any items categorized on the USML. The initial research suggested that the export shipment contained 3 items, totaling 15 pieces, categorized on the USML. At the time of the writing of this affidavit, only 1 license determination has been

returned from the DDTC/DOS. The part is identified as p/n 522-3828-00, National Stock Number 5826002251028, Radio Mount. Endicott Precision, Endicott, New York, 13760, manufactured the part. The shipment contained two p/n 522-3828-00. According to Ronald Oliveira, General Manager at Endicott Precision, p/n 522-3828-00 was last manufactured in 2004 on contract number SPO451-04D-5P83 for the United States Government Purchasing Department. A license determination was made by the DDTC/DOS on p/n 522-3828-00. The DDTC has determined that p/n 522-3828-00 is on the USML, Category XI (c), Military Electronics, which is described as components, parts, accessories, attachments, and associated equipment specifically designed or modified for use with the equipment in paragraphs (a) and (b) of this category, except for such items as are in normal commercial use. Following the license determination associated with the two aforementioned shipments, the ICE RAC/FM requested a license history associated with Leff and/or GEA to determine if Leff was either registered and/or licensed to export from the US. The DDTC/DOS provided documentation, which states that Leff was registered with the DDTC/DOS on an initial date of June 6, 1999, but the registration expired because the form was never completed satisfactorily. The registration reflected the address related to the premises.

*Mil
elec*

14. The elements that a violation has been committed under Title 22, United States Code, 2278 are as follows: (a) export/re-export and/or conspiracy to export/re-export (b) a licensable defense article/service, commodity or technical data (c) with specific intent, knowing the requirements of the DOS registration and licensing. Elements (a) and (b) have been substantiated in the aforementioned paragraphs outlined in this affidavit. Element (c) requires the Federal Government to prove that Leff and GEA had specific intent to export licensable USML items.

15. On April 9, 2003, the ICE RAC/FM interviewed Leff at the sub-office located in Bonita Springs, FL. An ICE initiated national program, Project Shield America, was established to educate and inform exporters/businesses throughout the United States on the exporting registration and licensing requirements relative to controlled exports. The Project Shield America outreach was documented on ICE report number FM06SR03FM0001034. According to the report, the ICE RAC/FM interviewed and informed Leff for approximately 90 minutes. An excerpt from the report states, "Special Agent Cramsey and Leff discussed the Project Shield America program in detail and exchanged business cards. Leff was given copies of the Project Shield America brochures for his review. Leff stated that he would be happy to review the literature to ensure his company was in compliance with all US export laws and

Project Shield America

regulations. Special Agent Cramsey stated that Leff should contact the DOS and/or DOC using the numbers identified in the literature to inquire about all shipments before exporting the items to ensure he was in compliance." During the interview, Leff stated that GEA is registered with the DOS, but he has never applied for an export license. Leff is retired from Lycoming, which is now called Honeywell. According to Leff, Lycoming manufactured jet engines and engines for American military helicopters and tanks. It was this background that led him to start Global Engineering Associates. Leff was advised of the licensing requirements related to items categorized on the ITAR. The literature provided was simply a resource for Leff to refer to. The details of the literature were discussed in detail.

16. On March 18, 2008, the consignee located in Singapore contacted the DHL customer service to inquire about the aforementioned shipments. The consignee questioned the delay of delivery of the shipments. DHL advised the consignee that the shipments were being held by "customs." On March 19, 2008, Leff had a domestic shipment arriving at the sub-office via UPS valued at \$18,000. Leff informed the UPS driver that he would not accept the shipment or any further shipments for an indefinite period of time. Leff had informed the UPS driver that he would contact him when he would start receiving packages again. Additionally, on

March 24, 2008, Leff scheduled a DHL pick-up, which was to be made at the sub-office. Upon the DHL driver's arrival, Leff had informed him that he didn't have a shipment, but rather, provided the driver with all of his DHL packaging supplies, such as packing slip pouches, labels, and associated supplies. Up until this point, shipments were being delivered to GEA on a daily basis. There is no record associated with Leff or GEA contacting "customs" to inquire about the nature of the delay or potentially lost shipments.

17. According to a search of the Minnesota Secretary of State database, GEA is incorporated in Minnesota, which is related to filing number 7X-147. The search stated that GEA originated on August 3, 1993 as a domestic corporation. The filing number indicates that the domestic corporation is active as of 2008. A search of the Florida Department of State, Division of Corporations, was negative for Martin Leff and/or Global Engineering Associates.

18. On March 18, 2008, UPS received one drop-off package at the UPS store located at 24600 S Tamiami Trail, Bonita Springs, FL, which was assigned tracking number 1Z 555 E94 03 9560 024 2. The shipment consisted of one package weighing 18 pounds, which was categorized as containing invoices. According to the information provided by the shipper, GEA, the package originated at 3333

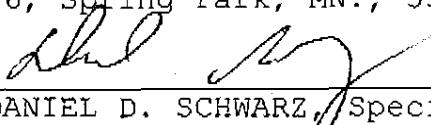
Renaissance Blvd, Suite 212, Bonita Springs, Florida, 34134. The consignee of the package was GEA, 2400 Interlachen Road, Suite 316, Spring Park, MN 55384.

19. According to the April 9, 2003 interview conducted by the RAC/FM, Leff stated that the main office is located in Spring Park, Minnesota, where the company is incorporated. During this same interview, Leff described the Bonita Springs office as the sub-office. Leff stated that he is a seasonal resident of Southwest Florida. Leff stated that he employs a full-time administrative assistant at the Minnesota office. According to Leff, the administrative assistant is responsible for the administrative functions and he himself handles all the business, including dealing with overseas customers.

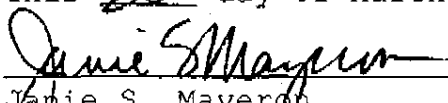
20. The ICE RAC/FM has determined that each and every shipment, which has been encountered to date, has enclosed invoices containing the letterhead of GEA, 2400 Interlachen Road, Spring Park, MN 55384. Also, the invoices contained prices, quantities, and monies due. As referenced in paragraph 19, Leff previously stated that the administrative assistant handles all administrative functions. Therefore, based on previous interviews with Leff, the RAC/FM believes the invoices are created as an administrative function. Based on my experience and training, smaller companies which are co-located interact and function as one entity either by

electronic correspondence, telephonically, and/or by mail. According to the UPS web site tracking system, tracking number 1Z 555 E94 03 9560 024 2 was delivered on March 21, 2008, at the premises.

21. Based on the facts contained herein, there is probable cause to believe, that GEA, through their agents and representatives, have exported, or caused the export, from the United States to Ultramare Singapore Pty., Singapore, certain USML items without the approval and licensing of the DDTC/DOS. Furthermore, GEA in fact has acquired USML items, more specifically described as 7 pieces of p/n 617 01312 (Pressure Indicator) and 2 pieces of p/n 522-3828-00 (Radio Mount), and caused these parts to be exported from the United States without proper authorization from the DOS/DDTC, in violation of Title 22, U.S.C., Section 2778. Further, there is probable cause to believe that there is evidence and instrumentalities of the offense, which will be found at, 2400 Interlachen Road, Suite 316, Spring Park, MN., 55384.


DANIEL D. SCHWARZ, Special Agent
U.S. Department of Immigration and
Customs Enforcement

SUBSCRIBED and SWORN to before me
this 21st day of March, 2008.


Jamie S. Mayeron
United States Magistrate Judge

SEARCH WARRANT ADDENDUM

1. In conducting the search authorized by this warrant, the government shall make reasonable efforts to utilize computer search methodology that avoids searching files, documents or other electronically stored information which is not identified in the warrant.

2. If electronically stored data or documents have been identified and seized by the government pursuant to this warrant, the government may retain the original hard drive or other data storage mechanism. The person from whom the data storage device has been seized may request that the government provide him or her with electronic copies of the electronically stored data or documents by making a written request to the United States Attorney's Office, identifying with specificity the files, data, or software sought to be copied. The government must respond to all such requests within a reasonable amount of time, and must provide a copy of the electronically stored data or documents requested unless the copies requested constitute contraband, instrumentalities, or property subject to forfeiture.

3. Nothing in this warrant shall limit or prevent the government from seizing the computer as contraband or an instrumentality of a crime or commencing forfeiture proceedings against the computer and/or the data contained therein. Nothing in this warrant shall limit or prevent the owner of the computer from (a) filing a motion with the Court pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the Return of Property or (b) making a request of the government to return certain specified files, data, software or hardware.

4. The government shall establish a search methodology governing the review of seized data to ensure that no attorney-client privileged communications will be inadvertently reviewed by the prosecution team. In the event that documents or other records seized pursuant to this warrant are identified by the government as possibly containing attorney-client privileged communications, an Assistant United States Attorney, who is not a member of the prosecution team and who is not participating in the search, shall act as a "taint team" to set up a "Chinese wall" between the evidence and the prosecution team that will prevent any privileged material from getting through.