COPY AUSA

UNITED STATES DISTRICT COURT

for the
Central 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)* LG (VX9100) cellular telephone	) Case No. CR 13-	13-2895M

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11-4-13 11:30 am

ALICIA G. ROSENBERG
Judge's signature

City and state: Los Angeles, California

Alicia G. Rosenberg, U.S. Magistrate Judge
Printed name and title

USA: Patrick R. Fitzgerald
PRF

Return		
Case No.: CR 13-	*Date and time warrant executed:*	*Copy of warrant and inventory left with:*
Inventory made in the presence of :		

Inventory of the property taken and name of any person(s) seized:

[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The SUBJECT TELEPHONE is a LG (VX9100) cellular telephone. Possession of the SUBJECT TELEPHONE was voluntary relinquished by the vehicle owner described ~~above~~ below Aff, and is currently in the custody of the FBI.

ATTACHMENT B

ITEMS TO BE SEIZED

1. ~~Based on the foregoing, I respectfully submit that~~ there is probable cause to believe that the following items, which constitute evidence fruits, and instrumentalities of violations of (1) murder of a federal officer, in violation of 18 U.S.C. § 1114; and (2) violence at international airport, in violation of 18 U.S.C. § 37, will be found in the SUBJECT TELEPHONE:

a. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show the actual user(s) of the digital device at any period of time;

b. Records, documents, programs, applications or materials, relating to the Los Angeles International Airport ("LAX");

c. Records, documents, programs, applications or materials, relating to the Transportation Security Administration ("TSA");

d. Records, documents, programs, applications or materials, relating to any plans by PAUL ANTHONY CIANCIA ("CIANCIA") or anyone else to engage in any violent crimes, including writings, manifestos, or other evidence of intent or

motive to violate 18 U.S.C. § 1114 or 18 U.S.C. § 37, or otherwise to cause harm to United States agencies or employees;

e. Records, documents, programs, applications or materials, relating to CIANCIA's views on the legitimacy or activities of the United States Government, including the existence of a plot to impose a New World Order ("NWO");

f. Records, documents, programs, applications or materials, relating to CIANCIA's mental state, including any thoughts or plans of suicide;

g. Records, documents, programs, applications or materials, indicating the identity of persons who have been in contact with CIANCIA since January 1, 2012;

h. Records, documents, programs, applications or materials, reflecting or instructing on law enforcement techniques and tactics and how to avoid the same;

i. Records, documents, programs, applications or materials, explosive materials, explosive devices, or chemicals, including suppliers and manuals;

j. Documents, media, or other materials reflecting or instructing on target locations, maps, schematics, operational plans, and tools for executing;

k. Documents, media, or other materials, relating to training in how to use weapons, including but not limited to evidence reflecting use of or access to firearms ranges;

1. Documents, media, or other materials relating to CIANCIA's finances as they relate to any of the items set forth above, including the source or purpose of any funding, transfers, or payments related to the acquisition of any of the above-referenced items of evidence, and other records relating to the purchase of weapons or other items.

SEARCH PROCEDURE FOR DIGITAL DEVICES

2. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device on-site or seize and transport the device to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. The government may retain a digital device itself, and/or entire forensic copies of it, until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device and/or forensic copies of it (or while an application for such an order is pending). Otherwise, the government must return the device and delete or destroy all forensic copies thereof.

h. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

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

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

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

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

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

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

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

A F F I D A V I T

I, Special Agent David A. Collazo, being duly sworn, hereby state as follows:

INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI"), and have been so employed since October 2012. I am currently assigned to the FBI Los Angeles Field Office Counterterrorism Team, where I investigate international terrorism and other violations of federal law, to include threats to U.S. citizens and American interests both within the United States and overseas. I had 14 years experience in law enforcement with the California Department of Justice and I have investigated several cases involving the murder of American citizens, including those involving the use of firearms and explosives. In preparing this affidavit, I consulted with fellow law enforcement agents with extensive technical expertise in criminal and terrorism matters.

2. From my training and experience, and from consultation with other law enforcement agents, I know that cellular telephones often contain stored data that may prove useful in criminal investigations. This data includes text messages, email communications, contact information, and other personally identifying information.

3. From my training and experience, and from consultation with other law enforcement officers, I also know that individuals who plan or commit violence against governmental targets commonly use the Internet to research potential targets and methodologies, plan activities, and communicate with others about intentions and activities, including but not limited to communications by email, chat, blog postings, and comments. In such cases, a footprint of some or all of this research, planning, and communications activity may be recovered from devices capable of accessing the Internet. Furthermore, even where certain such communications take place via the Internet - such as by means of email or social media - individuals involved in such activities also often maintain telephone contact with the same persons.

PURPOSE OF AFFIDAVIT

4. The facts set forth in this affidavit are based on my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. Because this affidavit is submitted for the limited purpose of supporting a request for the Court to authorize a search warrant for the subject property, as described below, I have not set forth each and every fact learned during the course of this investigation, nor have I summarized each and every fact deemed pertinent to the case. Rather, I have set forth only

those facts that I believe are necessary to establish probable cause for the requested search warrant.

5. This affidavit is specifically made in support of an application to search a LG (VX9100) cellular telephone, (herein "SUBJECT TELEPHONE") voluntarily provided to the FBI by a witness in the investigation outlined below, for evidence of the following criminal activity: (1) murder of a federal officer, in violation of 18 U.S.C. § 1114; and (2) violence at an international airport, in violation of 18 U.S.C. § 37. On November 2, 2013, the Honorable Jacqueline Chooljian, United States Magistrate Judge, authorized the filing of a criminal complaint containing these charges against PAUL ANTHONY CIANCIA ("CIANCIA"). I am seeking to search the SUBJECT TELEPHONE because, as discussed below, I believe that CIANCIA owned and used the SUBJECT TELEPHONE and there is probable cause to conclude that concealed within the SUBJECT TELEPHONE is evidence of the above-specified criminal violations.

PROPERTY TO BE SEARCHED

6. The property to be searched is described in Attachment A.

PROBABLE CAUSE

7. In the course of this investigation, I learned from other law enforcement agents the following information:

a. On November 1, 2013, CIANCIA approached a Transportation Security Administration ("TSA") security checkpoint at Terminal 3 of the Los Angeles International Airport ("LAX") armed with an assault rifle. CIANCIA fired his weapon at a uniformed TSA screener then on duty, fatally wounding the screener. CIANCIA then fired his weapon toward at least two other TSA screeners, wounding them.

b. CIANCIA was apprehended by law enforcement officers and is currently being treated for wounds sustained during his apprehension.

c. From a bag that CIANCIA was carrying, law enforcement officers obtained a handwritten note bearing CIANCIA's name, which professed a desire to kill multiple TSA employees and made reference to his concerns about a New World Order (NWO). Near the location where CIANCIA was apprehended, law enforcement officers also recovered a LG-brand battery for a cellular telephone.

8. After the aforementioned shootings, law enforcement officers identified CIANCIA's place of residence and interviewed one of his roommates. I have reviewed reports of the interview and spoken by phone to one of the FBI Special Agents who conducted the interview. From these sources I have learned the following:

a. During the interview, the roommate stated that on the morning of November 1, 2013, CIANCIA entered his room unannounced and asked to be driven to LAX. The roommate agreed and transported CIANCIA in his black Hyundai Accent to the Virgin Airlines airport terminal. The roommate stated that he only learned of the shooting incident upon returning to his apartment.

b. The roommate provided interviewing law enforcement officers with consent to search his vehicle for any evidence that might be of assistance to the investigation. While searching the vehicle, law enforcement officers recovered the SUBJECT TELEPHONE, and, upon questioning the roommate, learned that the SUBJECT TELEPHONE did not belong to him. Furthermore, the roommate stated that he believed the phone belonged to CIANCIA.

c. Upon inspecting the SUBJECT TELEPHONE, law enforcement officers noticed that the battery was missing from the SUBJECT TELEPHONE's battery housing.

9. Based on the roommate's statements, the SUBJECT TELEPHONE'S recovery in the vehicle that reportedly transported CIANCIA to LAX prior to the shooting incident, the absence of a battery in the SUBJECT TELEPHONE, and the recovery of an LG battery near CIANCIA's person at the time of his apprehension, I believe there is probable cause to conclude that the SUBJECT

PHONE belongs to CIANCIA, and as described below, may contain evidence of the criminal violations described above.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES

10. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including the SUBJECT TELEPHONE. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can require special procedures so that it can be searched properly, as set forth below. Some of these considerations typically apply to computer hard drives, but I believe that the procedures set forth in Attachment B should be followed for the SUBJECT TELEPHONE because at this time, without having reviewed the contents of the SUBJECT TELEPHONE, its operating system, storage capacity, and other functionalities are not yet known.

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs 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 be necessary to consult with specially trained personnel who have specific expertise in

the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the property. 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 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, 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 hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, 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. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular

user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive 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 digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal

information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a

controlled laboratory environment, and can require substantial time.

ITEMS TO BE SEIZED

11. Upon search of the SUBJECT TELEPHONE, items to be seized shall include information constituting evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1114 and 37, as set forth in Attachment B.

CONCLUSION

12. Based on the foregoing, I believe there is probable cause to believe that the SUBJECT TELEPHONE contains evidence, fruits and instrumentalities of the charged violations.

DAVID A. COLLAZO
Special Agent, FBI

Subscribed and sworn to before
me on November 4, 2013.

HON. ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE