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

UNITED STATES DISTRICT COURT

for the

District of Hawaii

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

94-542 Kupuohi Street, #204,
Waipahu, Hawaii 96797

Case No. Mag. No. 16-1537 RLP

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
94-542 Kupuohi Street, #204, Waipahu, Hawaii, 96797

located in the Honolulu District of Hawaii, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachments "A" and "B".

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2339B	Providing, or attempting, or conspiring to provide material support or resources to a designated foreign terrorist

The application is based on these facts:
See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☑ Delayed notice of 365 days (give exact ending date if more than 30 days: 12/13/2017) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Stephen B. Biggs, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: Dec. 13, 2016

Judge's signature

City and state: Honolulu, Hawaii

KEVIN S. C. CHANG, U.S. MAGISTRATE JUDGE
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR DISTRICT OF HAWAII

IN THE MATTER OF THE SEARCH OF: 94-542 Kupuohi Street, #204, Waipahu, Hawaii 96797	Mag. No. 16-1537 RLP

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Stephen B. Biggs, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 94-542 Kupuohi Street, #204, Waipahu, Hawaii 96797, hereinafter "PREMISES," further described in Attachment A, and for the things described in Attachment B. Based on the facts set forth in this affidavit, there is probable cause to believe that the PREMISES contain evidence of violations of 18 U.S.C. § 2339B (Providing, or attempting, or conspiring to provide material support or resources to a designated foreign terrorist organization); § 1113 (Attempt to commit murder within the special maritime and territorial jurisdiction of the United States); 18 U.S.C. § 1114 (Attempt to kill any officer or employee of the United States); and 18 U.S.C. § 115 (Threatening a federal official), among other offenses. This Court has authority to issue a warrant for property outside the District of Hawaii pursuant to Fed. R. Crim. P. 41(b)(3).

2. I am a Special Agent of the Naval Criminal Investigative Service ("NCIS") and have been since January 2008. I am currently assigned to the NCIS Hawaii Field Office located

in Honolulu, Hawaii. Since 2014, I have been assigned as a Task Force Officer to the Federal Bureau of Investigation, Honolulu Division, Joint Terrorism Task Force. My responsibilities as an FBI Task Force Officer include but are not limited to the investigation of domestic and international terrorism matters with a nexus to the U.S. Department of Defense. As an FBI Task Force Officer, I have utilized court-authorized search warrants, conducted physical surveillance, utilized confidential informants and interviewed subjects and witnesses during domestic and international terrorism investigations. As an FBI Task Force Officer, I have interviewed witnesses, executed court-authorized search warrants, and used other investigative techniques to determine the methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. As an FBI Task Force Officer, I have received advanced training on the conduct of international terrorism investigations, maritime counterterrorism operations and investigations, and counterterrorism online investigations. I was previously assigned to the NCIS Southeast Field Office as a member of the South Florida High Intensity Drug Trafficking Area Task Force. Because of my training and experience as an NCIS Special Agent, I am familiar with United States Criminal Code and the Uniform Code of Military Justice. In past investigations, I have used court-authorized search warrants for the installation of tracking devices on vehicles to assist physical surveillance, determine patterns of life, and observe criminal activity. In past criminal investigations, I have executed search warrants that resulted in valuable physical and digital evidence collection, seized assets, and numerous subjects agreeing to cooperate with the government. I have completed basic and advanced law

enforcement training courses at the Federal Law Enforcement Training Center at Brunswick, GA and at the Federal Bureau of Investigation Training Academy at Quantico, VA.

3. My experience as an NCIS Special Agent and FBI Task Force Officer includes, but is not limited to, counterterrorism matters, investigations of drug trafficking organizations, the sale of illegal firearms, and the distribution of firearms by prohibited persons. I am experienced in physical surveillance, interviews of witnesses, the use of search warrants, and the use of confidential informants.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. On October 7, 2016, the U.S. District Court for the District of Hawaii issued a warrant for the installation of a vehicle tracking device on a vehicle owned by U.S. Army Staff Sergeant Ikaika Erik Kang ("KANG").

6. On October 11, 2016, the U.S. District Court for the District of Hawaii issued an order authorizing the installation of pen registers and trap-and-trace devices, as well as acquisition of approximate location information, for KANG's cellular telephone, number (785) 223-3273.

7. On October 11, 2016, the U.S. District Court for the District of Hawaii issued an order authorizing the installation of pen registers and trap-and-trace devices on KANG's email addresses, ikaika.kang@yahoo.com and st8of808souljah@yahoo.com.

8. On November 3, 2016, the U.S. District Court for the District of Hawaii issued an order authorizing a search of KANG's temporary residence at Ft. Rucker, Alabama, where he was attending a military training course. KANG returned to Oahu from the training course on or about December 5, 2016. Execution of the search of KANG's temporary residence at Ft. Rucker occurred on November 7, 2016 and yielded the seizure of electronic information from KANG's computer and an external storage device. Due to the large volume of electronic information seized on November 7, 2016, forensic analysis is continuing. Preliminary analysis of seized data revealed KANG's computer contained violent videos and other content which corroborates information previously provided by CS1.

9. This application is for a search of KANG's permanent residence in Waipahu, Hawaii.

PROBABLE CAUSE

10. On October 15, 2004, the United States Secretary of State designated al-Qa'ida in Iraq ("AQI"), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization

("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224.

11. On May 15, 2014, the Secretary of State amended the designation of AQI as a FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under Section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name. The Secretary also added the following aliases to the ISIL listing: the Islamic State of Iraq and al-Sham ("ISIS"), the Islamic State of Iraq and Syria ("ISIS"), ad-Dawla al-Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the ISIL listing: Islamic State, ISIL, and ISIS. To date, ISIL remains a designated FTO.

12. U.S. Army Staff Sergeant Ikaika Erik Kang is trained as an air traffic controller. KANG is assigned to the 25th Infantry Division, Combat Aviation Brigade, at Schofield Barracks, on Oahu. In November 2015, Kang allegedly made threatening remarks in support of ISIL. The Army ultimately conducted government records checks pertaining to Kang. The checks revealed that in 2011, Kang's security clearance was revoked after Kang threatened to kidnap, beat up, and shoot his platoon sergeant and platoon leader, while they were deployed. As a result of Kang's statements in 2011, Kang was demoted in the Army, his security clearance was revoked, and he was referred to behavioral health for evaluation. Kang requested reconsideration for security clearance reinstatement in July 2012 and underwent an Army mental health evaluation in April 2013. Ultimately, Kang received reinstatement of his security

clearance. In or about August 2016, the Army requested that the FBI review this case to determine if Kang posed a threat, based on his past behavior and statements. The FBI has been working closely with the Army to assess and address the threat of violence posed by Kang.

13. In August 2016, a Confidential Source ("CS1") observed KANG watching videos at KANG's residence, 94-542 Kupuohi St. #204, Waipahu, Hawaii. KANG invited CS1 into his room and told him the videos depicted ISIL fighters. KANG was excited to share the videos with CS1. KANG told CS1 that he admired suicide bombers and their sacrifice, describing them as fearless. KANG showed CS1 such videos three times in August 2016 and twice in September 2016.

14. CS1 remembered one video that depicted a row of men in a warehouse hanging upside down by shackles around their ankles. An ISIL member walked by and cut off their heads. Another video depicted what appeared to be a child soldier with a gun, killing a row of men. CS1 relayed that KANG was especially excited to show CS1 a beheading video of a row of men kneeling while having their heads cut off. In my training and experience, beheadings of this nature are a common execution method used by ISIL. In my training and experience, it is common for ISIL to produce videos of this nature as propaganda to recruit followers to further its cause, including by committing acts of violence. CS1 remembered feeling sick to his stomach, while KANG laughed and insulted the victims.

15. CS1 described KANG as "obsessed" with the videos, which are of beheadings, shootings, suicide bombings, fighting, and other ISIL violence. CS1 said that KANG typically

watches these videos approximately four to five hours each day during the week, and probably more on the weekends.

16. During the first week of September 2016, CS1 recalled KANG telling him that if he were to do something like shoot up a large gathering, it would be out of his hatred for white people, the wicked, and non-Muslims. KANG further stated that it "would be for the cause." In my training and experience, KANG's comment about acting "for the cause" means committing an act of violence on behalf of ISIL.

17. On or about the first or second week of September 2016, at KANG's residence after KANG had returned home from work, CS1 observed that KANG was angry. CS1 asked KANG how his day was, and KANG told CS1 that he had discussed ISIL with a fellow soldier who supported ISIL's mission to fight common enemies of the United States, but did not support ISIL's general mission and violence. KANG told CS1 that he was angry because the fellow soldier "had no idea" and deserved to die because he "didn't understand." KANG told CS1 that he wanted to go back to work and shoot the fellow soldier. CS1 suggested KANG might get arrested and maybe just beating him up was a better alternative, and KANG laughed and said "Nope, I just want to end him."

18. On or about the last week in September 2016, KANG discussed with CS1 shootings at a shopping mall that had killed six people.[1] KANG told CS1 that if KANG were to have done it, KANG would have killed a lot more people because he could get more shots off, and he would have waited until they were all gathered together. KANG told CS1 that if the movie "The Purge" were real, he would pick an "asshole military guy," toss a grenade at him, and blow him up.[2] KANG later told CS1 that he does not have any friends, but if he had a group of friends, they would be like KANG and would go out killing people. Your affiant believes that KANG's statement about using a grenade to commit an attack means that KANG may have access to a grenade, or other explosive devices, through his access to military bases. On October 6, 2016, CS1 told KANG that CS1 was considering buying a gun. KANG told CS1 that KANG had a handgun and a rifle, and looked in the direction of a long, black, hard-shell container with a combination lock propped near KANG's television. CS1 believes that KANG's rifle is inside this container. KANG told CS1 that KANG needed to renew his firearms permit or else he could get into trouble.

---

[1] Your affiant believes this incident is actually referring to an attack at a shopping mall in St. Cloud, Minnesota on September 17, 2016, during which a lone attacker stabbed 10 people with steak knives, causing serious injury. The attacker was killed by law enforcement.

[2] "The Purge" is an American dystopian horror film series that is about a 12-hour period each year, during which all crime is legal and all emergency services are unavailable. The film series depicts widespread, notably graphic violence and murder.

19. Review of state firearms registration records by the FBI shows that KANG is the registered owner of two firearms, including a .40 Caliber Smith & Wesson M&P handgun and a 5.56mm Smith & Wesson M&P15 (AR-15 style) rifle.

20. KANG told CS1 that CS1 should get a rifle instead of a handgun, because he could kill more people with a rifle. KANG explained that the "cops" train with handguns, and that if CS1 had a rifle, CS1 could fight the cops and kill a lot of them before CS1 died. Based on CS1's interactions with KANG, CS1 is afraid for his safety around KANG. Specifically, CS1 told the FBI that he does not want to become "victim number 1."

21. Another individual, CS2, who works with KANG, noticed an increase in KANG's discussions of a violent interpretation of Islam during the beginning of September 2016. CS2 has heard KANG talk about religion, anti-government topics, and ISIL. On one occasion, when CS2 and KANG were in the car together, KANG was playing an audio recording of an Arabic speaker through the car stereo using his cellular telephone. When CS2 asked KANG what he was listening to, KANG stated that he was listening to a prophet reciting the Quran. KANG further stated that the speaker had been killed in the early 2000's, but KANG could not remember if he had been killed by a bomb or was a suicide bomber.

22. CS1 asked KANG what had been happening with the war overseas, and KANG told CS1 that ISIL was fighting a "holy war." CS1 inquired if KANG would join ISIL if asked, to which KANG responded "Yeah, hell yes!" Kang said that his plan was to stay in the military

long enough to get promoted to E7,[3] and then he would separate from the military, move to the Middle East, join ISIL, become a Muslim, study Arabic, and follow the Quran. KANG was excited about going to the Middle East to "join the cause." KANG said that he was "only in the military for a paycheck." KANG explained that he began researching the Muslim religion in 2014 and had continued studying over the past year. Based on my training and experience, individuals interested in extremism and ISIL like KANG, often collect documents, pamphlets, and printed or published information about (or from) terrorist organizations, and store said items in their residence for future reference. Many of these items may be purchased and shipped to the individual, thus a search of the residence may also recover waybills, air bills, bills of lading, receipts, delivery notices, and other shipping documentation related to the date, time, and contents of such shipments.

23. KANG told CS1 that, if KANG became a member of ISIL, he would be a suicide bomber and would attack Schofield Barracks on Oahu, Hawaii. In my training and experience, individuals who plan violent attacks such as suicide bombings typically create notes, letters, or other written plans of attack, and often keep them at their residences.

24. KANG showed CS1 the website, www.jihadology.net. In my training and experience, jihadology.net serves as both an academic site for jihadi source material and promotes a violent interpretation of Islam, and is often used for research by individuals who later

---

[3] "E7" is an enlisted rank in the military. In the U.S. Army, E7 is a Sergeant First Class.

self-radicalize and attempt to conduct violence in the name of radical Islam. CS1 said that KANG seemed to be absorbing the information about ISIL, "like a sponge." It appeared to CS1 that KANG had downloaded several pages from jihadology.net and saved those pages to his computer desktop. Based on my knowledge and communication with other law enforcement personnel, individuals involved in web searches and online communication with potential terrorists or terrorist recruiting sites often employ electronic measures to shield their identity or communications from discovery by law enforcement or others. An individual going to this length to hide his or her identity may keep records or information related to these constructed identities in handwritten or printed out form in their residences. These hard copy records may include information related to email accounts, search history and password, online identities for social media platforms, or other information regarding aliases and online identities.

25. KANG further expressed his desire to commit violence, when KANG told CS1 that he wanted to attack his stepfather with a knife, by stabbing him one hundred times and killing him. KANG said that he hated his entire family. KANG relayed a time in the past when KANG put on a hooded sweatshirt and then drove with his handgun to either his parents' or grandparents' house. KANG parked his car out front of the house, with the intention of going inside and shooting all of them, "including the kids." KANG told CS1 that he decided not to commit the attack because he did not want to get caught. Based on my knowledge, training and experience, along with frequent communication with other law enforcement personnel, individuals like KANG who are involved in the visualizing and planning stage of committing a

violent act often take photos or videos of themselves with weapons, at the locations they plan to conduct an attack or act of violence. Such individuals also often take photos or videos of their targeted victim or victims. In my training and experience, these photos or videos are often stored physically or on a digital device in the person's residence.

26. KANG also admitted to CS1 that he had interest in moving overseas. In my training and experience, people like KANG who consider relocating often visit the location ahead of time; plan future travel to the location; make contacts in the region; and conduct research regarding the location and associated cost of living. This type of planning and research often results in calendar entries, daily planner notations, or other written documentation regarding the relocation plan and travel schedule. Such information is of significant value to law enforcement and public safety, because it allows law enforcement to attempt to disrupt the threat posed by the subject before the travel actually takes place. Additionally, such individuals may retain airline or ground transportation tickets, bills, or receipts of past or future travel. Because much of this planning is ongoing, these travel- and schedule-related items are generally stored in such individuals' residences or on computing devices.

27. KANG shared violent images, suicide bomber videos, ISIL videos, extremist websites, and music with CS1 from KANG's laptop computer and/or cellular telephone. CS1 observed that KANG spent several hours a day consuming these images and related information in his room. In my training and experience, individuals involved in gathering images and information that may depict criminal activity often utilize multiple methods of communication to

find websites and online forums where this information is not available to the general public. To protect their criminal behavior from being traced back to a particular user, subjects will frequently switch between different methods of communication. In addition, individuals engaged in criminal activity that is unknown to their friends or family members will utilize multiple methods of communication with co-conspirators to avoid detection. Records checks confirmed that KANG has at least two known email addresses, ikaika.kang@yahoo.com and st8of808souljah@yahoo.com; however it is highly likely that KANG has other unknown email addresses, online profiles, and/or applications he utilizes for communication about illegal activity on his computer or in his home. From my training and experience, I know that most households contain electronic storage media, standard household computers, laptop computers, tablets and smart phones that store records of telephonic and digital communication. In my training and experience, and common knowledge, most individuals keep and maintain such devices at their personal residence. In addition to communication records, these devices frequently provide information and evidence, including geo-location information, records of contacts, Internet search records, photographic evidence, personal notes, and calendar information.

28. On or about October 17-18, 2016, KANG traveled from Hawaii to Ft. Rucker, Alabama to attend the Senior Leader Course, a military training course for senior non-commissioned officers. The training course lasted approximately six weeks, until December 2, 2016. KANG's temporary residence during the training course was Building #314, Room #218, Fort Rucker, Alabama 36362.

29. In my training and experience, individuals involved in the above-mentioned crimes typically keep physical handwritten or printed diaries, journals, notebooks, composition books, scrap paper, or printouts that document and reflect that person's affiliation or familiarization with foreign terrorist organizations, such as ISIL.

30. In residential searches executed in connection with criminal investigations in which I have been involved, the following kinds of personal property that tend to identify the person(s) in residence, occupancy, control of ownership of the subject premises have typically been recovered: keys, rental agreements and records, property acquisition records, utility and telephone bills and receipts, photographs, telephone answering pads, storage records, vehicle or vessel records, canceled mail envelopes, correspondence, opened or unopened, financial documents such as tax returns, bank records, safety deposit box records, cancelled checks, and other records of incomes and expenditures, credit card and bank records.

31. The foregoing facts establish probable cause to believe that: (1) evidence, fruits, or contraband can be found at the PREMISES, including the records described in Attachment B; (2) such evidence, fruits, or contraband is stored on each computer or storage medium that will be searched / seized, and (3) that the computers themselves are contraband or instrumentalities.

TECHNICAL TERMS

COMPUTERS, CELLULAR TELEPHONES, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

32. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, a cellular telephone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

33. *Probable cause.* I submit that if a computer, cellular telephone, or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer, cellular telephone, or storage medium, for at least the following reasons:

a. Based on my knowledge, training and experience, I know that subjects who conspire, attempt, or threaten to commit violent acts and murder keep web-enabled computer devices and cellular telephones on their persons, in their vehicles, in their offices, or in their residence, or other readily accessible places. As stated above, KANG has shared ISIL propaganda videos and audio files with

CS1, using KANG's computer and KANG's cellular telephone, in KANG's residence and vehicle.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system

configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

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

34. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers and cellular telephones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer, cellular telephones, and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer, cellular telephone, or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was

remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it

relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system ("GPS") technology for determining the location of the device.

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

e. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a computer or cellular telephone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example,

the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the

warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

37. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING AND DELAYED NOTIFICATION

38. It is respectfully requested that this Court issue an order sealing all papers submitted in support of this application, including the application and search warrant, until further order of the Court. Additionally, it is respectfully requested that this Court permit delayed notification pursuant to 18 U.S.C. §§ 3103a(b)(3) and 2705, until further order of the Court or up until a later date certain of one year following the date of the issuance of the order. I believe that sealing this document and delaying notification are necessary because the items and information to be seized are relevant to an ongoing criminal investigation that is neither public nor known to the subject of the investigation, and its disclosure would alert the subject to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested order or search warrant will seriously jeopardize the investigation, including by giving the subject an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, notify confederates, or cause harm to others. *See* 18 U.S.C. § 2705. Some of the evidence in this investigation is stored electronically. If alerted to

the investigation, the subject under investigation could destroy that evidence, including information saved to that person's personal computer(s). Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Disclosure of the contents of this affidavit and related documents, or notification at this time, may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Stephen B. Biggs
Special Agent
Naval Criminal Investigative Service
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me
on December 13, 2016:

KEVIN S. C. CHANG
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 94-542 Kupuohi Street, #204, Waipahu, Hawaii 96797, further described as an apartment in a multi-family dwelling. Unit #204 is located inside the Kulana Knolls, gated community in Royal Kunia. Kulana Knolls consists of numerous stand-alone buildings containing multiple units, inside an access-controlled gate. A peach-colored, two-story building stands to the immediate right after passing through the key-coded, gated entry off of Kupuohi Street. Unit #204 is contained in the blue colored two-story building facing the parking lot, past the peach two-story building. A footpath to the right of the building connects it to the parking area. The stairs leading to the second story landing are in the middle of the building on the right side. The unit is a second floor, corner, end unit, with no back neighbors. The unit is approximately 759 sq. ft. and includes two bedrooms and two bathrooms. The front door opens off of the second story landing into an open living area. The living area includes a sliding glass door leading to an approximately 66 sq. ft. lanai, overlooking green space behind the building. The kitchen is off of the living area opposite the sliding glass door and balcony.

ATTACHMENT B

Property to be searched or seized

1. Photographs of all records relating to violations of 18 U.S.C. § 2339B (Providing, or attempting, or conspiring to provide Material Support to a Foreign Terrorist Organization); § 1113 (Attempt to commit murder within the special maritime and territorial jurisdiction of the United States); 18 U.S.C. § 1114 (Attempt to kill any officer or employee of the United States); and 18 U.S.C. § 115 (Threatening a federal official), those violations involving IKAIKA ERIK KANG, including:

a. Physical handwritten or printed diaries, journals, notebooks, composition books, scrap paper, and printouts;

b. Textbooks, books, pamphlets, and printed or published information regarding radical Islam or terrorist organizations;

c. Handwritten notes containing information regarding passwords, online identities, email addresses, Facebook addresses, Twitter accounts, Instagram accounts or any other information regarding alias online identities;

d. Any records regarding past or future travel by Ikaika Erik Kang, including schedules of past or future travel, airline or ground transportation tickets, bills, or receipts;

e. Waybills, air bills, bills of lading, receipts, delivery notices, and other shipping documentation from the U.S. Postal Service, small package carriers, or common carriers which indicate the shipment of packages and parcels to and from the Mainland U.S. and Hawaii, or to or from the United States and any foreign country;

f. Records and information relating to KANG's e-mail accounts;

g. Records and information that KANG has saved on his computer or cellular phone regarding ISIL tactics and techniques, any information provided to KANG by ISIL, or records of communication between KANG and ISIL;

h. Records and information relating to KANG's search history and downloads;

2. Photographs of any and all documents, magazines, newspapers, web pages, writings, postings, photographs, videos, or other materials, in electronic or digital format, related to ISIL, terrorist organizations, firearms, weapons of mass destruction, and the reporting about (or advocacy of) any acts of violence, as well as any such materials that show KANG's state of mind as it relates to the crime under investigation.

3. Weapons, firearms, ammunition, and any related paperwork (including licenses, permits, receipts, shipment-related documents, addresses, phone numbers, or any other identifying information), and lock-boxes, safes, or other containers used to store firearms or ammunition;

4. Photographs of components used to create an improvised explosive device or improvised weapon, and any grenades or explosive materials;

5. Photographs of documents and articles of personal property showing (or containing data showing) the identity of persons occupying, possessing, residing in, owing, frequenting, or controlling the premises to be searched or property therein, including keys, rental agreements and records, property acquisitions records, utility and telephone bills and receipts, photographs, telephone answering pads, storage records, vehicle or vessel records, canceled mail envelopes, correspondence, opened or unopened, financial documents such as tax returns, bank records, safety deposit box records, canceled checks, and other records of incomes and expenditures, credit card, and bank records;

6. Photographs and seizure by copying of computers, cellular telephones, or storage media used as a means to commit the violations described above, including any threats against federal officials made via computer-based communications;

7. Photographs and seizure by copying of any computer, cellular telephone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cellular telephone, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER AND ELECTRONIC DEVICES"):

a. evidence of who used, owned, or controlled the COMPUTER AND ELECTRONIC DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER AND ELECTRONIC DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the COMPUTER AND ELECTRONIC DEVICES were accessed or used to determine the chronological context of COMPUTER AND ELECTRONIC DEVICES access, use, and events relating to crime under investigation and to the COMPUTER AND ELECTRONIC DEVICES user;

e. evidence indicating the COMPUTER AND ELECTRONIC DEVICES user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER AND ELECTRONIC DEVICES of other storage devices or similar containers for electronic evidence;

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

h. evidence of the times the COMPUTER AND ELECTRONIC DEVICES were used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER AND ELECTRONIC DEVICES;

j. documentation and manuals that may be necessary to access the COMPUTER AND ELECTRONIC DEVICES or to conduct a forensic examination of the COMPUTER AND ELECTRONIC DEVICES;

k. records of or information about Internet Protocol addresses used by the COMPUTER AND ELECTRONIC DEVICES;

l. records of or information about the COMPUTER AND ELECTRONIC DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. Contextual information necessary to understand the evidence described in this attachment;

8. Routers, modems, and network equipment used to connect COMPUTER AND ELECTRONIC DEVICES to the Internet;

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "COMPUTER AND ELECTRONIC DEVICES" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.