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)

Dell Inspiron Laptop, Serial Number 9QCHPR1, Seagate External Hard Drive (NA7GT233), Audio, Visual Files, Records or Media Located Therein

Case No. Mag. No. 17-1012 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)*:

Dell Inspiron laptop, serial number 9QCHPR1, Seagate external hard drive (NA7GT233), audio, visual files, records or media located therein.

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

Applicant's signature

Jimmy Chen, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 30 August 2017

Judge's signature

City and state: Honolulu, Hawaii

RICHARD L. PUGLISI, 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: DELL INSPIRON LAPTOP, SERIAL NUMBER: 9QCHPR1, SEAGATE EXTERNAL HARD DRIVE (NA7GT233), AUDIO, VISUAL FILES, RECORDS OR MEDIA LOCATED THEREIN	Mag. No. 17-1012 RLP **AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

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

I, Jimmy Chen, 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 Dell Inspiron laptop computer bearing serial number: 9QCHPR1, and the Seagate external hard drive bearing serial number: NA7GT233. These items will be referred to as the "SUBJECT COMPUTER DEVICES" from here on and will be listed in Attachment A. The property to be searched will be further described in Attachment B. Based on the facts set forth in this affidavit, I believe that the "SUBJECT COMPUTER DEVICES" contain evidence in furtherance of violations of 18 U.S.C. § 2339B (Providing material support to a foreign terrorist organization); and that there is probable cause to believe that the search of the "SUBJECT COMPUTER DEVICES" and any files, folders, records or other electronic media located therein, will lead to evidence, fruits, and

instrumentalities of the aforementioned crimes, as well as to the identification of individuals who are engaged in the commission of those and related crimes.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been so employed for approximately 12 years. I am currently assigned to the Honolulu Field Office. As a result of my training and experience as an FBI Agent, I am familiar with federal and state criminal laws. My responsibilities as an FBI Special Agent include, but are not limited to, the investigation of domestic and international terrorism matters. As an FBI Special Agent, I have utilized court-authorized search warrants and arrest warrants, conducted physical surveillance, utilized confidential informants, and interviewed subjects and witnesses during international terrorism investigations.

3. 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.

4. This application is for a search of the laptop, external hard drive and other electronic storage devices belonging to IKAIKA ERIK KANG (KANG) that may be located therein.

PROBABLE CAUSE

5. On or about October 15, 2004, the United States Secretary of State designated Al-Qaeda in Iraq (AQI), then known as Jam 'at al Tawid wa' al-Jahid, as a Foreign Terrorist Organization (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.

6. On or about May 15, 2014, the Secretary of State amended the designation of AQI as an 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 of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham ("ISIS" – which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furquan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

7. U.S. Army Staff Sergeant KANG is trained as an air traffic controller. KANG is assigned to the 25th Infantry Division, Combat Aviation Brigade, at Schofield Barracks, on Oahu. KANG lives off-base in an apartment in Waipahu, Hawaii.

8. While in the U.S. Army, as far back as 2011, KANG has made threatening statements. He was reprimanded on several occasions for threatening to hurt or kill other service members, and for arguing pro-ISIS views while at work and on-post. Due to these remarks and

threats, KANG's security clearance was revoked in 2012, but reinstated the following year after KANG complied with military requirements stemming from the investigation. In early 2016, it appeared that KANG was becoming radicalized and in or about August 2016, the Army referred this matter to the FBI.

9. At or around the beginning of September 2016, a Confidential Human Source (CHS 1) noticed an increase in KANG's discussions of radical Islam. CHS 1 heard KANG talk about religion, anti-government topics, and ISIS. On one occasion, when CHS 1 and KANG were in a vehicle together, KANG played an audio recording of an Arabic speaker through the car stereo using his cellular telephone. When CHS 1 asked KANG what he was listening to, KANG said 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 became a suicide bomber. Based upon the aforementioned facts, your affiant believes KANG was listening to "Nasheeds."

10. Based on my training and experience, individuals who become radicalized often begin the radicalization process by listening to "Nasheeds." Nasheeds are religious sermons produced by Islamic religious leaders and in some instances foreign terrorist organizations who subscribe to beliefs which stem from radical Islam. Your affiant knows that Nasheeds are a work of vocal music that is either sung a cappella or accompanied by percussion instruments. Nasheeds are popular throughout the Islamic world and the material and lyrics make reference to Islamic beliefs, history, religion as well as current world events.

11. On or about March 1, 2017, KANG told CHS 1 that he had been conducting research online about the most effective and painful ways people had been tortured. KANG added that he was still angry at a civilian who had taken away his air traffic controller's license, and that he wanted to torture him. KANG said that if he ever saw him again, he would tie him down and pour draino in his eyes.

12. In March 2017, CHS 1 and KANG were discussing the shooting at Pulse Nightclub in Orlando, Florida. KANG told CHS 1 that the shooter did what he had to do and later said that America is the only terrorist organization in the world. Later in March 2017, KANG told CHS 1 that Hitler was right, saying he believed in the mass killing of Jews.

13. In May 2017, KANG advised CHS 1 that a U.S. Intelligence Agency had gotten into his cellular telephone and saw his "video". CHS 1 asked KANG what type of video he has on his cellular telephone, to which Kang advised CHS that he has a "*bayat*" or "*bayat*" video on his phone. Based on training and experience, your affiant knows that "*bayat*" is a pledge of allegiance to a religious leader. Your affiant knows that it is common practice for persons who support ISIS, to pledge *"bayat"* to the group's purported leader Abu-Bakr Al-Baghdadi. Your affiant also knows that it is also common for these persons and ISIS to maintain these types of videos on more than one electronic device (such as a cellular telephone and laptop computer) and release the videos to the public.

14. On or about October 17, 2016, KANG traveled to Ft. Rucker, Alabama for a six-week military training course for senior enlisted leaders, the Air Traffic Control Operator Senior Leadership Course.

15. On or about November 3, 2016, the FBI conducted a court-authorized search of KANG's lodging at Ft. Rucker. The FBI conducted a full data extraction from KANG's external Seagate hard drive, and a partial data extraction from KANG's Dell Inspiron laptop, which contained a 500GB hard drive.

16. The FBI later conducted a forensic review of the extracted data. The external Seagate hard drive contained, among other things, 18 military documents marked "SECRET."

17. A subsequent classification review by military subject matter experts confirmed that 16 of those 18 documents remain classified today. The metadata of these files shows that they were first created on June 18, 2013, and were burned onto a CD (discussed below) on June 21, 2013.

18. Subsequent FBI forensic review of the external Seagate hard drive showed that it contained approximately 486 documents that referenced ISIS, ISIL, or violence. These documents included 13 issues of Inspire Magazine. One issue was entitled "Assassination Operations," and another entitled "Targeting."[1] The external Seagate hard drive also contained approximately 1,221 video files that referenced ISIS, ISIL, or violence.

---

[1] Inspire Magazine is an online, English-language magazine published by Al-Qaeda in the Arabian Peninsula (AQAP). The publication glorifies acts of terrorism and is aimed at inciting

19. Subsequent FBI forensic review of SUBJECT COMPUTER DEVICES to include KANG's Inspiron laptop hard drive showed that it contained, among other things, approximately 146 videos and 671 graphics files that referenced ISIS, ISIL, violence, or war.

20. On December 13, 2016, the U.S. District Court for the District of Hawaii issued an order authorizing a search of KANG's residence in Waipahu, Hawaii. Execution of the search of KANG's residence occurred on December 14, 2016 and yielded the seizure of electronic information from SUBJECT COMPUTER DEVICES. Additionally, the FBI found a CD marked in handwriting with the words "SECRET" and "SIPR."[2]

21. The CD in KANG's residence contained, among other things, 18 military documents marked "SECRET." A subsequent review by military subject matter experts confirmed that 16 of those 18 documents remain classified today.

22. The metadata of the foregoing files shows that the documents were copied to KANG's external Seagate hard drive on April 18, 2015, when KANG was stationed in Hawaii. The hash values show that they are the same files as the 18 classified documents found on the CD labeled "SECRET," discussed above.

---

violence among would-be terrorists in Western, English-speaking countries. Based on my training and experience, Inspire Magazine is often read by individuals in the United States who are self-radicalizing.

[2] "SIPR" is a reference to the U.S. military's Secret-level classified computer network.

23. On or about June 20-23, 2017, FBI Undercover Employees (UCEs) traveled to Honolulu and met with KANG.

24. On or about June 21, 2017, three FBI UCEs met with KANG at a hotel room in Honolulu and brought a micro-SD card. KANG drove his personally owned vehicle to the hotel, and brought his external Seagate hard drive to the hotel. UCE1 told KANG that he had saved documents from his prior service in the military onto a micro SD card, and that he to planned travel overseas and provide the micro-SD card with those military documents to ISIS. KANG offered to provide materials of his own, which were contained on his external Seagate hard drive.

25. On or about June 21, 2017, KANG provided unclassified military documents to the UCEs for the purpose of ultimately providing them to ISIS. KANG plugged the external Seagate hard drive into a computer provided by the UCEs, and KANG transferred numerous documents from the external Seagate hard drive to the micro-SD card. The documents included unclassified "for official use only" ("FOUO") military documents, as well as unclassified military documents that had been approved for dissemination, such as military manuals on various topics. KANG verbally described the documents that he was providing to the UCEs, and detailed how they would be helpful to ISIS. For example, KANG described a Soldier's Manual for Common Tasks, which he said provides "checklists" for how to "react to contact, you know hasty fighting positions." KANG said that "knowing how to react to contact and communicate will help them [ie: ISIS members] a lot."

26. KANG indicated that he knew the materials were not publicly accessible. UCE 1 asked KANG if he could find "this stuff" on the Internet. KANG responded that "everything has to be CAC'd now," referring to a military Common Access Card, which is an identity card used to log into military computer systems, and that he got it from a private military drive.

27. On or about June 22, 2017, UCE 1 told KANG that he could not open some of the files, and KANG offered to bring his external hard drive back the following day. UCE 1 told KANG that he wanted to look at them, and get to the bottom of asking "how can this help the Islamic state?" KANG responded that, when he got home, he would sort out the videos for viewing on June 23, 2017 so that he can give it to them on Saturday morning, June 24, 2017.

28. On or about June 22, 2017, KANG also described how he could benefit ISIS by conducting combatives training. KANG told UCE 1 that ISIS fighters were "extremely effective" at martial arts, but that they don't have any "jazz" with their technique. UCE 1 asked KANG what he could do differently. KANG responded that from watching their videos (referring to ISIS propaganda videos), there wasn't much grappling, and that they weren't showing any ju-jitsu arm bars or anything like that. KANG described what he saw in the videos as just stand-up kickboxing, without specialized techniques that he described to UCE 1.

29. On or about June 23, 2017, KANG returned to the hotel room via his vehicle, transporting his external hard drive and cellular telephone. KANG then provided 14 classified military documents to UCE 1 for the purpose of ultimately providing them to ISIS. KANG once again met with the three UCEs in the same hotel room in Honolulu. Kang ran searches on his

hard drive using military search terms suggested by the UCEs.[3] The searches revealed classified military documents which KANG provided to the UCEs.

30. KANG attempted to provide ISIS with classified military documents by copying the documents from his external Seagate hard drive onto the micro-SD card provided to him by the UCEs, which he believed the UCEs would, in turn, later pass on to ISIS. When the UCE 2 asked if these documents would help ISIS, KANG said, "It will, definitely." KANG also identified a document that pertained directly to the U.S. Army mission in Afghanistan.

31. FBI forensic analysis of the 14 classified military documents on the micro-SD card confirmed that they were 14 of the 18 classified military documents that KANG retained at his residence on the CD marked "SECRET," and later transferred to his external Seagate hard drive. The hash values show that they are the same files. The metadata of the foregoing files shows that the documents were first created on June 18, 2013. Eighteen (18) documents were burned to the CD labeled "SECRET" on June 21, 2013. The same 18 documents were copied and pasted from the CD to KANG's external Seagate hard drive on April 18, 2015. KANG then copied 14 of the 18 documents onto the micro-SD card provided to him by the UCEs on June 23, 2017. All 14 of those documents remain classified. Of the four files that were not copied, two remain classified, and two are no longer classified.

---

[3] Based on a prior court-authorized search, the UCEs were aware that the hard drive contained classified information.

32. On or about June 23, 2017, UCE 3 asked KANG what was the most important thing that KANG had given, in terms of being able to give to ISIS. KANG responded that it was the combatives portion. The UCEs discussed the possibility of introducing an actual member of ISIS to KANG, and KANG expressed interest in the idea. UCE 2 told KANG that they would be coming back to Hawaii in two weeks, and invited KANG to stay with them. KANG responded "Hell yeah." KANG said that he could make a combatives video with the ISIS member, and that KANG would remove any affiliation, so that way it would not be incriminating.

33. On or about July 6, 2017, UCE 1, UCE 2, and UCE 3 returned to Hawaii. KANG met them at a house in Honolulu. They introduced KANG to a person who they identified as a member of ISIS, CHS 2. The UCEs also advised KANG that he would meet somebody the following day, and that "He's the real deal."

34. On or about July 7, 2017, KANG was observed going a store that sells tactical gear. KANG entered the store, and asked the clerk about the availability of various items to include magazine pouches, load bearing gear, long sleeve camouflage shirts, and BDU trousers. The clerk showed KANG around the store to look at the items, and KANG advised he was "looking for two of everything." KANG walked around the store carrying at least one package of balaclavas, and KANG looked at a rack containing molle-type vests and other equipment. KANG then purchased several items and returned to his residence carrying one white plastic shopping bag. KANG later arrived at the residence in Honolulu. KANG transported in his personally owned vehicle, his AR-15 type rifle, his pistol, a folding knife, masks, camouflage

pants, vests, and a case of water. KANG's vest had holsters that held his pistol and knife. KANG was introduced to UCE 4, who was described to KANG as, and who he believed to be, an ISIS leader. KANG played several hours of ISIS videos, and eventually moved to more graphic videos, to include a video that KANG described as his favorite, which depicted beheadings.

35. UCE 4 told KANG that he wanted to know who KANG was, and whether he was with the U.S. Army, or with the Islamic State. KANG responded that he was with the Islamic State. UCE 4 asked KANG whether, if he only had one bullet, and was faced with an American soldier who he did not know, and CHS 2 (who KANG believed was a member of ISIS), which of them he would shoot. KANG replied that he would shoot the soldier (referring to the U.S. soldier.)

36. On or about July 8, 2017, KANG, UCE 4, and CHS 2 discussed the purchase of a drone at a retail store. KANG knew that CHS 2 planned to take the drone back to the Islamic State. KANG discussed how to fit the drone into a suitcase.

37. KANG, UCE 4, and CHS 2 drove in CHS 2's car to the retail store. KANG purchased a Go-Pro Karma drone with a Go-Pro camera for $1,151.82. KANG also purchased extra batteries, propellers, and a 64gb micro-SD card for a total of $227.45. KANG paid for the items with his debit card. KANG accepted $700 in cash from UCE 6 (splitting approximately half of the cost).

38. Upon returning to the residence, KANG gave an example of how the drone could allow ISIS fighters to escape a battle involving U.S. tanks. KANG advised that U.S. tank crews are highly trained and difficult to defeat. Therefore, a drone would allow ISIS to view the battlefield from above to find tank positions and avenues for escape.

39. Also, on July 8, 2017, KANG swore "*bayat*" to Abu Bakr al-Baghdadi, the purported leader of ISIS. UCE 4 read the pledge in English. KANG accepted the pledge. CHS 2 then gave KANG a gift—a folded ISIS flag—and then recited an Arabic version of the pledge, which KANG repeated verbatim in Arabic. The pledge ended with a hug and a kiss from UCE 4.

40. On July 8, 2017, KANG was arrested by the FBI without a warrant, based on probable cause that he had committed the crimes described herein, having just sworn *bayat* to ISIS and expressed a desire to kill "a bunch of people."

41. Following his arrest, KANG orally waived his *Miranda* rights and signed a written *Miranda* waiver. KANG admitted that he knowingly transferred classified information to ISIS, but minimized his conduct by claiming that the information was old and no longer posed any harm to the United States. KANG claimed he thought he was only helping a non-governmental organization (NGO), not ISIS.

42. KANG also provided oral and written consent for FBI to search his Dell Inspiron laptop computer bearing serial number: 9QCHPR1, and the Seagate external hard drive bearing serial number: NA7GT233.

43. SUBJECT COMPUTER DEVICES are currently in the lawful possession of the FBI. They came into the FBI's possession after KANG was arrested and with his consent. Therefore, while the FBI might already have all necessary authority to examine SUBJECT COMPUTER DEVICES, your affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of the SUBJECT COMPUTER DEVICES will comply with the Fourth Amendment and other applicable laws.

44. SUBJECT COMPUTER DEVICES are currently in storage at the FBI Honolulu Division Office, located at 91-1300 Enterprise Avenue, Kapolei, HI 96707. In my training and experience, I know that the SUBJECT COMPUTER DEVICES have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT COMPUTER DEVICES first came into the possession of the FBI.

45. On July 9, 2017, KANG orally waived his rights to prompt presentment, and signed a written waiver of those rights, known as a *Corley* waiver. KANG orally waived his *Miranda* rights and signed another written *Miranda* waiver. KANG was confronted with a video recording of the loyalty oath that he swore. KANG made the following admissions:

46. KANG admitted that he had pledged loyalty to the leader of ISIS, Abu Bakr al-Baghdadi. KANG said that he was not forced to pledge loyalty to the leader of ISIS. KANG admitted that he did so voluntarily.

47. KANG said that he took the CD labeled "SECRET" from his desk drawer at Hickam in 2015 (referring to Joint Base Pearl Harbor-Hickam, where KANG was stationed in 2015). KANG admitted that he knew the CD was SECRET. KANG admitted that he had kept the CD at his residence. KANG admitted that he copied the CD with the classified documents onto his external hard drive.

48. KANG admitted that the documents he transferred to the UCEs were classified.

49. KANG initially said that he did not intend for the files he transferred to UCEs to go to ISIS. He initially said that he intended them to go to the NGO. Later in the interview, KANG admitted that when he was transferring the classified documents to the UCEs, he knew the documents would eventually be provided to the ISIS.

50. KANG said that he knew that UCE 4 and CHS 2 were affiliated with ISIS when he was first introduced to them at the house. KANG agreed that UCE 4 and CHS 2 did not say they were affiliated with the NGO.

51. KANG admitted training CHS 2 in weapon tactics, grappling techniques, and ground fighting. KANG confirmed that CHS 2 did not force KANG to do the training.

52. KANG admitted that the training videos would provide CHS 2 with the best skill set so that CHS 2 could take it back to the Middle East to train ISIS members.

53. KANG stated that CHS 2 was going to take the drone to the Middle East for use by ISIS.

54. KANG said that he believed CHS 2 was going to train ISIS members with the combatives video.

55. KANG admitted that he became interested in ISIS in 2015 when he began researching religion. KANG said that he wanted to help the Islamic State as early as late 2015, because he saw how ill equipped they were for fighting. KANG confessed that he wanted to provide the Islamic State with weapons training as early as late 2015.

56. The foregoing facts establish probable cause to believe that: (1) evidence, fruits, or contraband can be found in the SUBJECT COMPUTER DEVICES, including but not limited to videos, electronic files and the records described in Attachment B; (2) such evidence, fruits, or contraband is stored on the SUBJECT COMPUTER DEVICES that will be searched.

TECHNICAL TERMS

LAPTOP COMUTER, EXTERNAL HARD DRIVE, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

57. As described above and in Attachment B, this application seeks permission to search for records that might be found in the "SUBJECT'S COMPUTER DEVICES", in whatever form they are found. Thus, the warrant applied for would authorize the search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

58. *Probable cause.* I submit that on the SUBJECT'S COMPUTER DEVICES there is probable cause to believe those records will be stored for at least the following reasons:

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

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

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has

used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

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

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

e. 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.

f. 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).

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

h. 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.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

60. *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:

j. 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.

k. 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.

l. 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.

61. *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

I submit that this affidavit supports probable cause for a warrant to search the "SUBJECTS COMPUTER DEVICES" described in Attachment A and items described in Attachment B.

Respectfully submitted,

Jimmy Chen
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on August 30, 2017:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is a Dell Inspiron Laptop, Serial Number: 9QCHPR1, and External Seagate Hard Drive (SN: NA7GT233).

ATTACHMENT B

Property to be searched

1. All electronic records relating to violations of 18 U.S.C. § 2339B (Attempting to provide Material Support to a Foreign Terrorist Organization); involving IKAIKA ERIK KANG, including:

   a. Electronic textbooks, books, pamphlets, and printed or published information regarding radical Islam or terrorist organizations;

   b. Electronic records containing information regarding passwords, online identities, email addresses, Facebook addresses, Twitter accounts, Instagram accounts or any other information regarding alias online identities;

   c. Any electronic 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;

   d. Electronic 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;

e. Electronic records and information relating to KANG's e-mail accounts;

f. Electronic files that KANG has saved on his computer or external hard drive regarding ISIS tactics and techniques, any information provided to KANG by ISIS, or records of communication between KANG and ISIS;

g. Electronic records and information relating to KANG's search history and downloads;

2. Any and all files, magazines, newspapers, web pages, writings, postings, photographs, videos, or other materials, in electronic or digital format, related to ISIS, terrorist organizations, firearms, weapons of mass destruction, and the reporting about (or advocacy of) any acts of violence;

3. Any electronic 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. Electronic 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. Electronic 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. Electronic evidence of the lack of such malicious software;

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

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

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

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

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

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

l. Electronic 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; and

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