

7

AO 106 (REV 4/10) Affidavit for Search Warrant

AUSAs Vikas Didwania, Barry Jonas, Melody Wells,  
(312) 353-5300

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

Case Number:

18 M650

All electronic devices in the possession of ASHRAF AL  
SAFOO, further described in Attachment A-2

**APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT**

I, Jennifer M. Hergenroeder, a Special Agent of the Federal Bureau of Investigation, request a search warrant  
and state under penalty of perjury that I have reason to believe that on the following property or premises:

**See Attachment A-2**

located in the Northern District of Illinois, there is now concealed:

**See Attachment B**

The basis for the search under Fed. R. Crim. P. 41(c) is evidence and instrumentalities

The search is related to a violation of:

*Code Section*

Title 18, United States Code, Section 2339B

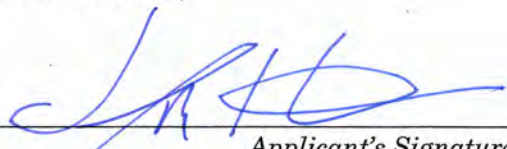
*Offense Description*

material support of a foreign terrorist organization,  
namely, ISIS

The application is based on these facts:

**See Attached Affidavit,**

Continued on the attached sheet.

  
Applicant's Signature  
JENNIFER M. HERGENROEDER, Special Agent, Federal  
Bureau of Investigation  
Printed name and title

Sworn to before me and signed in my presence.

Date: October 16, 2018

  
Judge's signature

City and State: Chicago, Illinois

M. DAVID WEISMAN, U.S. Magistrate Judge  
Printed name and title

FILED

OCT 16 2018

OCT 16 2018

M. DAVID WEISMAN  
MAGISTRATE JUDGE  
UNITED STATES DISTRICT COURT

UNITED STATES DISTRICT COURT       )  
  )  
NORTHERN DISTRICT OF ILLINOIS       )

**AFFIDAVIT**

I, Jennifer M. Hergenroeder, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately August 2016.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to international terrorism, including the provision and attempted provision of material support or resources to terrorists and foreign terrorist organizations, in violation of Title 18, United States Code, Sections 2339A and 2339B. In addition, I have conducted numerous investigations involving the use of the Internet, email and social media to further criminal activity. I have participated in the execution of multiple federal search warrants.

3. This affidavit is made in support of an application for a warrant to search the apartment located at 5225 N Virginia Avenue, Apartment 2, Chicago, Illinois, described further in Attachment A-1 (the “**Subject Residence**”) and all electronic devices located on the person of ASHRAF AL SAFOO, (the “**Subject Person**”, collectively with the **Subject Residence**, the “**Subject Premises**”) described further in Attachment A-2, for evidence and instrumentalities described further in Attachment B, concerning material support of a foreign terrorist organization, in violation of Title 18, United States Code, Section 2339B.



4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of violations of Title 18, United States Code, Section 2339B, are located at the **Subject Premises**.

**I. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH**

5. On October 16, 2018, the undersigned submitted an affidavit in support of a complaint and arrest warrant charging ASHRAF AL SAFOO with conspiracy to provide material support to ISIS, in violation of Title 18, United States Code, Section 2339B (the **Subject Offense**). That affidavit is attached as Exhibit C and its contents are incorporated by reference.

6. As described below and in Exhibit C, there is probable cause to believe that AL SAFOO has committed and is committing the **Subject Offense**; that AL SAFOO uses multiple mobile telephones and other electronic devices to further commission of the **Subject Offense**; and that such devices, as well as other evidence and instrumentalities of the **Subject Offense** are likely to be found in the **Subject Residence** and on the **Subject Person**.

7. Based on a review of AL SAFOO's driver's license, physical surveillance and utility records, AL SAFOO resides at the **Subject Residence**.

8. As described in Exhibit C, an FBI employee, acting in an undercover capacity (UCE-1), has communicated with a user of Social Media Application, whom law enforcement believes is AL SAFOO.<sup>1</sup> As described below, law enforcement has observed AL SAFOO using several different mobile devices between November 2017 and October 2018.

9. In addition, AL SAFOO has discussed his use of operational security measures, meant to conceal his identity, including his use of a separate electronic device when he engages in activities in support of ISIS, including his use of Social Media Application. AL SAFOO's use of operational security measures is further supported by the results of a Customs and Border Protection search of a mobile device AL SAFOO was carrying when he returned to the United States from Iraq which indicated that the device had been "sterilized," or stripped of its contents before he crossed the border.

10. Based on this information, and as described below and in Exhibit C, I believe AL SAFOO possesses multiple mobile devices, all of which may contain evidence and instrumentalities of the **Subject Offense**, and that these devices may be found at the **Subject Residence** or on his person.

---

<sup>1</sup> The government has redacted the name of the application used but can provide it to the Court if necessary.



**A. SURVEILLANCE OF AL SAFOO INDICATES HE USES MULTIPLE MOBILE ELECTRONIC DEVICES**

11. Law enforcement officers have surveilled AL SAFOO on several occasions between November 2017 and October 2018 and have observed AL SAFOO using multiple mobile electronic devices at different times. For example:

a. On November 24, 2017, CBP observed AL SAFOO carrying an Apple iPhone 5S (bearing serial F2LLT7XEFNJJ and IMEI 358753054455631) during an inbound secondary exam. CBP performed a border search of this device.

b. On January 13, 2018, CBP observed AL SAFOO carrying a Samsung Galaxy S5 (bearing IMEI 353502063297129) during an inbound secondary exam. CBP performed a border search of this device.

c. On April 5, 2018, law enforcement officers observed AL SAFOO holding a white iPhone with a black case on a CTA train. Similarly, on April 11, 2018, law enforcement officers observed AL SAFOO holding a white iPhone at a CTA bus stop.

d. On June 18, 2018, law enforcement officers observed AL SAFOO at his place of work using a black cellular telephone.

e. On October 12, 2018, law enforcement officers observed AL SAFOO holding a black cell phone with a black leather case on a CTA train. Later that day subject was observed on a CTA train holding what appeared to be the same black cell phone with a black leather case.

f. On October 15, 2018, law enforcement officers observed AL SAFOO with two mobile devices on a CTA train. The first device was a black cell phone with a black leather case that flips open like a book. The second device was a gold iPhone.

12. I believe an “iPhone 6 GOLD 16 GB Verizon” (the Subject Phone), bearing serial number C39NWN9UG5MF and IMEI 354444065251649, is used by AL SAFOO to commit the **Subject Offense**. Based on Apple’s records, the description of the Subject Phone, which is a gold iPhone, is consistent with law enforcement officers’ observation of AL SAFOO’s use of a gold iPhone on October 15, 2018. It is also consistent with the description below provided by AL SAFOO of his use of an older phone with 16 GB of data for his ISIS support activities. AL SAFOO also indicated that the Subject Phone is not in his name. According to Lycamobile records, the Subject Phone is linked to a prepaid account with no subscriber records. AL SAFOO also indicated he uses a separate phone for his ISIS support activities. As described above, AL SAFOO uses two separate phones, and records for the Subject Phone indicate it was not used to send or receive calls between January 5, 2018 and May 28, 2018.<sup>2</sup>

---

<sup>2</sup> There also were no data transmissions during this period. The government is continuing to investigate the lack of data transmissions but believes it may be due to AL SAFOO using a separate device or service for data transmissions to/from the Subject Phone.



13. Other information also indicates that AL SAFOO uses the Subject Phone. For example, the Subject Phone is linked to iCloud account shami\_2@icloud.com (iCloud Account 1). The name of this account is similar to the account "shami\_02@tutanota.com," which is used by AL SAFOO based on a search of his phone by the U.S. Customs and Border Protection.<sup>3</sup> It is also similar to the PalTalk account shami\_01@tutanota.com, which is used by AL SAFOO, as described in paragraphs 157 and 158 of Exhibit C. It is also consistent with AL SAFOO's promotion of Shaykh Abu Maysara Al-Shami, as described in paragraph 67 of Exhibit C.

14. According to Apple records, the identifiers for the Subject Phone were also linked to another iCloud account (iCloud Account 2).

15. Additionally, the subscriber information for both iCloud Accounts are false. Specifically, iCloud Account 1's subscriber is "Shami Shami" at address "123 N Main, Orlando, HI," which are a false name and false address. iCloud Account 2 similarly has the subscriber "Shami Syria" at address "123, Maryland, MD," which are similarly false name and address. Based on my training and experience, I know that individuals engaged in criminal activity often use false subscriber information to evade law enforcement. Thus, I believe the false subscriber information for the

---

<sup>3</sup> On or about November 24, 2017, CBP conducted a search of AL SAFOO's Apple cellular phone as he was entering the country. According to Apple records, the Apple cellular phone, IMEI 358753054455631, had been linked to Apple account shami\_02@tutanota.com, which was created on September 2, 2017. The account subscriber was identified as "Iraqi Shami," address "123 N North Ave, Los Anglos [sic], CA."

iCloud Accounts is further indication that AL SAFOO is using the Subject Phone linked to these accounts for illegal activity, which is consistent with AL SAFOO's description of his use of a gold iPhone for ISIS-related activity.

16. iCloud Account 2 was accessed from IP address 73.8.18.136 on June 28, 2018, June 29, 2018, September 20, 2018, September 26, 2018, September 30, 2018, October 1, 2018, October 2, 2018. According to Comcast records, IP address 73.8.18.136 is assigned to the **Subject Residence**.

17. Based on my training and experience, I believe that AL SAFOO has used the Subject Phone to access the internet from the **Subject Residence**, has carried the Subject Phone on his person, and uses the Subject Phone for the commission of the **Subject Offense**.

**B. AL SAFOO STATED THAT HE USED MORE THAN ONE MOBILE DEVICE AND DESCRIBED HIS OPERATIONAL SECURITY MEASURES**

18. On or about February 19, 2018, the following Social Media Application conversation took place between UCE-1 and AL SAFOO:<sup>4</sup>

UCE-1: Peace be upon you. How are you? I hope everything is going well with you, my good brother.

AL SAFOO: Peace be upon you. I'm well, how about you?

---

<sup>4</sup> The conversations described in this affidavit took place between UCE-1 and Social Media Application user Abu Al-'Abbas Al-Iraqi. For the reasons described in Attachment C, law enforcement believes that AL SAFOO is Abu Al-'Abbas Al-Iraqi. For ease of reference Abu Al-'Abbas Al-Iraqi is referred to herein as AL SAFOO. The communications are in Arabic and I have reviewed draft translations of many of the communications.



UCE-1: Praise be to Allah for everything. I'm well too. Do you think [Social Media Application] is not safe, and if so, then what do you advise [for contact]?

AL SAFOO: Do you have vpn? Have both of them always on, and you will be safe by the will of Allah.

On or about February 20, 2018, the conversation continued:

UCE-1: Yes, I do use Tor VPN. It's good, and it is not free. Security is very important, and I'm careful about that. You can advise me if you have something else in mind.

AL SAFOO: These are all reasonable measures, but our security is in Allah's hands. If you are truthful with Allah, He will be at your side. Brother, why don't you make nafir [travel for the purpose of joining jihad]? If you have an excuse, just say it. I don't want to embarrass you with personal things.

UCE-1: No, my good brother, there's no embarrassment but I'm wounded in my eye. I was with the brothers...it's a long story, and maybe it's not safe telling it here. My stay here is temporary anyway...

AL SAFOO: May Allah grant you success. Do you know about secret chat--

UCE-1: Maybe private chat...

AL SAFOO: --on Social Media Application...Yes.

UCE-1: Yes, the secret chat.

AL SAFOO: It is encrypted.

UCE-1: Yes.

19. Based on my training and experience, the training and experience of other agents involved in this investigation, information from UCE-1 and the content and context of these conversations, I believe AL SAFOO was instructing UCE-1 on how to use services that can hide one's identity and location online, such as a VPN or Tor services, which make it more difficult for others to trace a user's identity and location. Similarly, as explained above, secret chats are encrypted and disappear, which can make it more difficult to use incriminating communications as evidence. Criminals use these tools to hide their criminal activity and to evade law enforcement. Also, AL SAFOO asked UCE-1 about joining jihad, which can have a variety of meanings but, based on the context and use of the word "nafir," I believe AL SAFOO asked UCE-1 why he/she had not yet traveled to join ISIS and fight with ISIS. In a later conversation not quoted above, UCE-1 also explained that he/she had been fighting but was injured and therefore was temporarily staying elsewhere.

20. The suggested use of VPN services by AL SAFOO is consistent with the apparent use of VPN services by AL SAFOO. Specifically, according to IP data<sup>5</sup>

---

<sup>5</sup> Based on my training and experience and conversations with other agents with experience investigating computer crimes, I know that the Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. IP addresses typically have looked like a series of four numbers, each in the range 0–255, separated by periods (e.g., 121.56.97.178). Recently, IP addresses may also appear as a series of six hexadecimal digits separated by colons. Every computer attached to the Internet must be



obtained from email service providers, AL SAFOO's email addresses repeatedly connect to the same overseas Internet Service Providers, which suggests AL SAFOO's use of VPN services. In other words, typically, a user's home Internet account is assigned a specific IP address for a specific time. This information can later be used to determine which home Internet account logged into a particular email account at a particular time. In AL SAFOO's case, the government is aware that AL SAFOO uses Comcast broadband Internet service at home. Yet, the IP data associated with his email accounts instead traces to an international service provider, likely because AL SAFOO used a VPN or similar service to re-route the traffic from his home Internet connection and disguise the IP address associated with his home Internet.

21. On or about February 23, 2018, the following Social Media Application conversation took place between UCE-1 and AL SAFOO:

AL SAFOO: My device is full. I just deleted a video from it.

UCE-1: Okay, brother.

AL SAFOO: My device is 16 GB. I use it to support [ISIS], and it is not in my name. It is not that great of a device.

22. Based on my training and experience, the training and experience of other agents involved in this investigation, and the content and context of these conversations, I believe AL SAFOO was explaining that he used a separate

---

assigned an IP address so that Internet traffic to and from that computer may be properly directed from its source to its destination.

smartphone for his activities in support of ISIS, including his use of Social Media Application. AL SAFOO indicated the device was not registered to him, which is a method used by criminals to evade law enforcement. According to AL SAFOO, the device was not that great of a device, which I assess to mean did not function well.

**C. AL SAFOO WAS CARRYING A SANITIZED PHONE WHEN HE RETURNED TO THE U.S. FROM IRAQ**

23. According to government records, on January 5, 2018, AL SAFOO departed the United States for Baghdad, Iraq, connecting in Doha, Qatar. On January 13, 2018, AL SAFOO returned to the United States. Based on my training and experience, and the training and experience of other agents involved in this investigation, I know that ISIS has had a significant presence in Iraq, including in Mosul, where al-Baghdadi declared the creation of a Caliphate. According to a press statement by the United States Secretary of State dated July 10, 2017, the Iraqi government declared that Mosul had been “liberated” from ISIS.

24. Upon AL SAFOO’s return to the United States, he was interviewed by CBP. During the interview, AL SAFOO stated that he had traveled to Baghdad to bring back his mother, who was in Baghdad visiting his ill grandmother. AL SAFOO also told the CBP officer that he uses the phone number xxx-xxx-0055.

25. AL SAFOO also informed CBP that he was traveling with one cell phone, a Samsung Galaxy S5, which is an advanced smartphone capable of downloading social media applications, taking and retaining photos and videos, and storing documents and conversations. I know that owners of smartphones such as



the Samsung Galaxy S5 often store a variety of personal information on their phones, including photos, videos, text messages, social media messages, and a variety of applications. Often, the purpose of obtaining an advanced phone, such as the Galaxy S5, is to be able to operate powerful applications and store voluminous information.

26. According to the CBP report of the interview, AL SAFOO's phone contained only two photos of the horizon taken inside an aircraft and no other conversations or pictures. According to the report, the phone had been "sanitized," which, based on the context, I understand to mean that it had no third-party applications, no media, such as personal photos or videos, no personal documents, and no personal conversations.

27. During the interview, AL SAFOO informed CBP that he used the social media applications WhatsApp and Google Hangouts on his phone. He also said he had used Social Media Application, and had used it for the last time approximately six months ago. Yet, AL SAFOO's phone contained none of these social media applications. WhatsApp and Social Media Application are encrypted applications that are known to have been used by individuals involved in the support of terrorism or engaged in terrorism.

28. Based on the foregoing, I believe that AL SAFOO likely erased all of the data on his smartphone prior to traveling. Based on my training and experience, and the training and experience of other law enforcement, I know that those seeking to avoid detection of their activities, including those involved in terrorism, commonly

erase the data on their phones when entering the country in light of the publicly known CBP policy authorizing border searches of electronic devices when entering the country.

29. Accordingly, based on surveillance reports demonstrating the use of multiple phones by AL SAFOO, and AL SAFOO's operational security practices, I believe that one or more devices is likely to be found in the possession of the **Subject Person** and at the **Subject Residence**.

30. Furthermore, I believe these devices are likely to contain evidence or instrumentalities of the **Subject Offense**. Based on my training and experience, I know that a Social Media Application account can be used across multiple electronic devices. As described above and in Exhibit C, AL-SAFOO's role as a supporter of ISIS and a contributor, as well as supervisor of other contributors, to ISIS media production, including through Social Media Application, other social media applications, and websites requires the storage and transmission of digital communications and media. Thus, I believe AL SAFOO's electronic devices are likely to contain information related to these activities, including communications, photos, videos, and other media concerning ISIS. I believe the devices also are likely to contain information attributing AL SAFOO as the user of Social Media Application, including as described in Exhibit C and the use of operational security measures described above across multiple devices. I further believe AL SAFOO's devices may be instrumentalities of the **Subject Offense**.



**D. INFORMATION ABOUT THE SUBJECT RESIDENCE**

31. According to surveillance and driver's license records, AL SAFOO resides at 5225 N Virginia Avenue, Apartment 2, Chicago, Illinois.

32. The premises to be searched (the "**Subject Residence**") is the residence located at 5225 N Virginia Avenue, Apartment 2, Chicago, Illinois. 5225 N Virginia Avenue is a two-story detached building with light colored brick and a small addition off the back of the building with tan vinyl siding. The house number 5225 is displayed vertically on a white name plate on the left side of the front entrance of the house. The front entrance is located on the left side of the building at the top of four stairs leading to a concrete landing. According to the Cook County Assessor's website, the building contains two units.

33. Upon entering the building there is a tiny alcove approximately 5' x 4', with mailboxes on the right side (south wall). Upon entering the alcove, there are two doors, one on the left and one on the right. The door on the left appears to be a storage door. The door on the right provides access to the apartments. From the window of this door, one unit, which appears to be the first floor unit, is visible.

34. According to open source research, the **Subject Residence** is the second floor unit of 5225 N Virginia Avenue. Specifically, online real estate listings list Unit #2 as the second-floor unit in the building.

## **II. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA**

35. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (e.g. computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed



to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

36. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

37. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

38. In my training and experience, it is likely that the **Subject Premises** will contain at least one Apple brand device, such as an iPhone or iPad, because AL SAFOO has been observed by law enforcement using various Apple brand devices when travelling and commuting within Chicago.

39. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to

unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

40. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints, either their own or others', that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

41. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include when more than 48 hours have passed since the last time the device was unlocked. The Touch ID feature will also not work and entry of a passcode will be required if the device's user or someone acting on the user's behalf has remotely locked the device. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID, and execute the



search authorized by the requested warrant, exists only for a short time (*i.e.*, 48 hours or less, or until the device is given a remote lock command). Touch ID also will not work to unlock the device if the device has been turned off or restarted (*e.g.*, if the device's battery becomes fully depleted), or after five unsuccessful attempts to unlock the device via Touch ID are made. In addition, I also know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offers users the ability to remotely erase the contents of such devices.

42. The passcode or password that would unlock any Apple devices found during the search of the **Subject Premises** is not known to law enforcement. Thus, it likely will be necessary to press the finger(s) of the user of the Apple devices found during the search of the **Subject Premises** to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant.

43. Attempting to unlock the relevant Apple devices via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access or retrieve the data contained on those devices for the purpose of executing the search authorized by the requested warrant.

44. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it

is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers.<sup>6</sup> In the event that law enforcement is unable to unlock any Apple devices found in the **Subject Premises** as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

45. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of **ASHRAF AL SAFOO** at the **Subject Premises** to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found at the **Subject Premises** for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by the requested warrant.

### **III. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA**

46. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

---

<sup>6</sup> Law enforcement will select the fingers to depress to the Touch ID sensor to avoid compelling the user of the device to disclose information about his or her knowledge of how to access the device.



47. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

48. The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.



#### IV. CONCLUSION

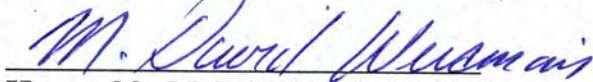
49. Based on the above information, I respectfully submit that there is probable cause to believe that AL SAFOO has engaged in material support of a foreign terrorist organization, in violation of Title 18, United States Code, Section 2339B, and that evidence and instrumentalities relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Premises**, as further described in Attachment A-1 and A-2. I therefore respectfully request that this Court issue search warrants for the apartment located at 5225 N Virginia Avenue, Apartment 2, Illinois, more particularly described in Attachment A-1, and the person of ASHRAF AL SAFOO, as further described in Attachment A-2, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

FURTHER AFFIANT SAYETH NOT.



Jennifer M. Hergenroeder  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn  
before me this 16th day of October, 2018



Honorable M. DAVID WEISMAN  
United States Magistrate Judge





**ATTACHMENT A-2**

**DESCRIPTION OF PREMISES TO BE SEARCHED**

All electronic devices in the possession of the SUBJECT PERSON, identified as follows:



**Name:** ASHRAF AL SAFOO, a/k/a Abu Al'-Abbas Al-Iraqi, Abu Shanab, Abbasi  
**DOB:** XX-XX-1984  
**Hair:** Black  
**Eyes:** Brown  
**DLN:** A42101384142





**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

Evidence and instrumentalities concerning violation of Title 18, United States Code, Section 2339B, as follows:

1. Items related to the Islamic State of Iraq and the Levant ("ISIL"), the Islamic State of Iraq and Syria ("ISIS"), Abu Bakr al-Baghdadi, jihad, terrorism, martyrdom, bi'a, weapons or physical training, and any individuals or organizations associated with the above.
2. Items related to Khattab Media Foundation.
3. Items related to foreign travel.
4. Computer hardware, software and applications that enable connection of electronic devices to the internet, enable user anonymization, disguise a user's identity, conceal files and file folders, securely delete data, and encrypt communications.
5. Computer hardware, software and applications used to edit text, image, video or sound files.
6. Items related to the commission of acts of violence in the United States or overseas, including justifications for such conduct, the selection of a target or targets, the logistics of such conduct, and any tools or weapons to be used in such conduct.
7. Items related to the purchase or use of cellular phones.

8. Items related to use or acquisition of social media accounts.

9. Items concerning ownership or use of any computer and cell phone recovered, including, but not limited to:

a. evidence of who used, owned, controlled, or copied the computer, cell phone, and related media at time the items to be seized were created, edited, or deleted, such as logs, registry entries, configuration files, email and email contacts, instant messaging logs, saved usernames and passwords, encryption keys, documents, photographs, and correspondence; and

b. evidence of internet use relating to the items to be seized, such as browsing history and cookies, user profiles, Media Access Control (MAC) addresses, connection records, firewall logs, caches, "bookmarked" or "favorite" web pages, search terms entered into a search engine, and records of user-typed web addresses.

10. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints of ASHRAF AL SAFOO onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device found at the **Subject Premises** in order to gain access to the contents of any such device.



### **ADDENDUM TO ATTACHMENT B**

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.





**ATTACHMENT C**

**AFFIDAVIT**

I, Jennifer M. Hergenroeder, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed since approximately August 2016. I am currently assigned to the Federal Bureau of Investigation's Joint Terrorism Task Force. As part of my duties as a FBI Special Agent, I investigate criminal violations relating to international terrorism, including the provision and attempted provision of material support or resources to terrorists and foreign terrorist organizations, in violation of Title 18, United States Code, Sections 2339A and 2339B. As a result of my training and experience, to include information provided by other federal agents with applicable knowledge, I am familiar with the tactics, methods, and techniques used by terrorist networks and their members. As part of my job, I have participated in the execution of multiple federal search warrants. In addition, I have conducted numerous investigations involving the use of the Internet, email and social media to further criminal activity.

2. This affidavit is submitted in support of a criminal complaint alleging that Ashraf AL SAFOO violated Title 18, United States Code, Section 2339B by conspiring to provide material support and resources, namely, personnel and services, to a designated foreign terrorist organization, namely, the Islamic State of Iraq in al-Sham, herein after "ISIS."

3. According to immigration records, Ashraf AL SAFOO is a 34-year-old naturalized U.S. citizen who was born in Mosul, Iraq and moved to the United States in September 2008. Based on physical surveillance, AL SAFOO's driver's license, and utility service records, AL SAFOO resides in Chicago, Illinois.

4. AL SAFOO and his co-conspirators are members of Khattab Media Foundation ("Khattab"). As explained in greater detail below, Khattab is an internet-based organization dedicated to the creation and widespread dissemination of ISIS propaganda, including edited video content, articles and essays, and infographics created through the use of video and photo editing and other similar software. Khattab has sworn bayat, or an oath of allegiance, to ISIS. Khattab posts its pro-ISIS propaganda across multiple social media platforms including Twitter, Facebook, YouTube, and Social Media Application.<sup>1</sup> Because the propaganda created and distributed by Khattab includes messages that promote violence, Khattab members frequently have their social media accounts suspended or deleted for violating the Terms of Service of those platforms. Because access to these platforms is critical to ISIS's and Khattab's mission, when Khattab members' social media accounts are suspended or terminated, they seek access to new accounts by hacking, or stealing, accounts of legitimate social media users and by creating accounts under fake names and identifiers. These accounts are distributed to Khattab members to use in disseminating ISIS propaganda.

---

<sup>1</sup> The government has redacted the name of the social media application but can provide it to the Court upon request. Social Media Application is described in further detail in Section II below.



5. In addition, Khattab members employed sophisticated operational security measures to conceal their identities online and elsewhere. For example, they shared information about how to maintain online anonymity, including TOR (The Onion Router) browsers and Virtual Private Networks, among other techniques and software.

6. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging AL SAFOO with conspiring to provide material support and resources to a foreign terrorist organization, and multiple related search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint and that there is evidence of the charged offense contained within the items to be searched.

7. This affidavit is based on my personal knowledge, training, and experience, information provided to me by other law enforcement agents, my review of communications of Khattab members including AL SAFOO captured by an FBI Undercover Employee (UCE1), and my review of publicly available information.

8. UCE1 has preserved conversations among members of Khattab that occurred on Social Media Application , as well as conversations UCE1 had with AL SAFOO on Social Media Application . Unless otherwise specified, all conversations described in this Affidavit were in Arabic. Usernames originally rendered in Latin characters are placed in quotation marks. All other usernames have been

transliterated from the original Arabic. Some of the preserved conversations have been translated and summarized in this Affidavit. The summaries of the conversations do not include all statements made or topics covered during the course of the conversations. I based the summaries and the language quoted from the preserved conversations on my initial review of draft transcripts prepared by FBI personnel and are not based on final, verbatim transcripts. At various points in the Affidavit, I also have indicated (sometimes in brackets) my interpretation of words and phrases used in the conversations. My summaries and interpretations are based on the context of the conversations, events occurring before or after the conversations, information received from UCE1, my knowledge of the investigation as a whole, my training and experience, and the training and experience of other law enforcement officers involved in this investigation.

#### **SUMMARY OF THE INVESTIGATION**

9. As described in more detail below, AL SAFOO, and members of Khattab, referred to herein as other CO-CONSPIRATORS or CCs, have conspired to provide material support and resources, namely, personnel and services, to ISIS, a designated foreign terrorist organization. Specifically, Al-Safoo and the CCs were working at the direction of and in coordination with ISIS and ISIS' media office, created and disseminated ISIS propaganda, recruited for ISIS, encouraged individuals to carry out attacks on behalf of ISIS, and supported violent jihad on behalf of ISIS and ISIS' media office.



## **PROBABLE CAUSE**

### **I. BACKGROUND ON THE ISLAMIC STATE OF IRAQ AND AL-SHAM**

10. On October 15, 2004, the United States Secretary of State designated al-Qa'ida in Iraq, then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization 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 al-Qa'ida in Iraq 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 Foreign Terrorist Organization 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 Foreign Terrorist Organization listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated Foreign Terrorist Organization.

12. Abu Bakr al-Baghdadi is the current leader of ISIS.

13. Based on my training and experience, I am aware that ISIS and other FTO's have official "media" components that produce and disseminate official communications. For example, I know that the media components of al-Qaeda in the Arabian Peninsula and ISIS have produced high quality magazines (e.g., Inspire and



Dabiq) and the media components of ISIS have used high quality editing, graphics and music to produce videos.

14. Based on my training and experience, I am aware that ISIS uses its respective "media" components to, among other things:

- a. Recruit mujahedeen fighters and other personnel including doctors, nurses, engineers, and other roles and professions;
- b. Solicit donations and other financial support;
- c. Call for attacks in the West and against other governments and civilian populations deemed enemies of ISIS;
- d. Intimidate governments, private entities and civilians that do not share ISIS's violent jihadist philosophy; and
- e. Claim responsibility for terrorist attacks.

15. Based on my training and experience, I am also aware that ISIS members have used social media applications, video-sharing sites, blogs and other internet-based sites and applications to distribute their official communications inexpensively, safely, and broadly. In addition, I am aware that ISIS and other foreign terrorist organizations use these online tools to communicate (publicly and privately) with sympathizers and potential recruits, and to distribute their respective messages to legitimate media outlets, in order to draw attention to the organizations, recruit new members, raise money and promote violent jihad, all in an effort to carry out the terrorism-related goals of the organizations.

16. In August 2015, Al Himmah Library, an official media operation for ISIS, published online a document titled, “You are a Mujahid, O Media Man,” about the importance of ISIS propaganda.<sup>2</sup> In the publication, ISIS proclaimed, “the media has far-fetched impact in changing balances of battles waged . . . because the media publishes or disseminates the victories of Muslims against their enemies, shows support for them, and their heroism in addition to bestowing praise on them. These issues are bound to invigorate the mujahidin . . . .”

17. In this same publication, ISIS further proclaimed that the “jihadi media” is “no less important than engaging in battle,” and argued that that it “is necessary to attain media victory to go along [with] the escalating military victory.” The publication equated the importance of ISIS’s military victory and victory in the “propaganda war that the Crusader US and its allies are waging against the Islamic State,” arguing that “(half the battle) is a media battle” and “the power of words is sharper (stronger) than atomic bombs.” The publication repeatedly equated the work of ISIS propagandists to ISIS soldiers waging violent jihad: “Inciting jihad is equal to (waging) jihad . . . . He who incites (people) is a mujahid in the cause of Allah Almighty. He will earn the same wages like the brother who goes into jihad . . . .” Towards the end, the publication again declared, “So, my dear unknown media soldier, know how valuable your role is in attaining victory. . . . [Y]ou are a mujahid for the cause of Allah . . . .”

---

<sup>2</sup> According to open source information, the al Himmah Library is the official media arm of ISIS responsible for the release of written material.



18. To succeed in the media battle, the publication instructed the “jihadi media” to “frighten [the infidels], threaten them with death, manifest their defects, and expose their suspicions. Simultaneously, the morale of the soldiers is to be elevated, the news of their victories disseminated.” And it described the tasks of the jihadi media and necessary effort to accomplish ISIS’s goals:

It is no secret – brother media man – that your jihad by the spoken word is not limited to talking only, but also includes statement, written word, printed word, audio clips, and the preparation of the scenarios for the releases... etc. All these require exertion of immense physical effort.

19. According to the publication, this task was not “simple” but required an “army of media men” who disseminated “jihadi media news” on “electronic websites.”

20. The publication further instructed propagandists to obey ISIS media officials: “Therefore, if you obey him [the media official], you obey Allah; and if you disobey him, you disobey Allah.”<sup>3</sup>

## **II. BACKGROUND ON SOCIAL MEDIA APPLICATION A**

21. Based on my training and experience, I have learned that Social Media Application is a mobile and desktop messaging application. It can be used on smartphones, such as Apple iOS and Google Android devices, and on desktop

---

<sup>3</sup> Members of Khattab appear to have been aware of this publication and heeded its call. For example, on or about October 11, 2017, CC11 posted a message to members of a Khattab group on Social Media Application (described in more detail below), including AL SAFOO, instructing members to, “Prepare to support your religion and state and to embitter the life of Allah’s enemies” and ended the message with the hashtag “#Journalist\_you\_are\_a\_Mujahid.” Based on my training and experience and the content and context of this conversation, it appears that this hashtag refers to the title of the Al-Himmah publication. Similarly, on or about October 16, 2017, CC11 wrote, “So, o soldiers of the media, dedicate all your time to almighty Allah for the soldiers of the Islamic Caliphate are thrilled and they are cheering and glorifying Allah over your media productions.” He included the hashtag “#Journalist\_you\_are\_a\_Mujahid.”



computers, by users to send messages and media to each other.

22. To sign up for Social Media Application, a user must provide a phone number. Social Media Application verifies the phone number through a text message sent to the phone number. Social Media Application users can also select a username but are not required to. Usernames are unique, meaning only one user can have a username. Social Media Application users can find other users by searching for the username or by using the known phone number of a user. However, users cannot view the phone number associated with a username. Users can also select a display name, such as a first and last name. Display names are not unique.

23. Social Media Application offers a variety of communication methods for its users:

24. **Chats.** Users on Social Media Application can communicate with each other through chats. They can send each other text messages, photos, videos, any files, and make voice calls.

25. **Secret Chats.** Secret chats use end-to-end encryption, which means only the sender and recipient have the ability to view the content of the chats. These secret chats also disappear and can be set to self-destruct.

26. **Groups.** Social Media Application allows collections of users to communicate with each other in chat rooms called groups. Groups may be invitation only.

27. Social Media Application has advertised that it has over two hundred million active monthly users. Several newspaper articles have described Social Media Application as the “app of choice” for terrorists, especially ISIS.

28. Social Media Application has advertised that it has never disclosed any user information to third parties, including governments. According to Social Media Application, it has accomplished this in part by using a “distributed infrastructure,” which means data is stored in multiple data centers around the world.

### **III. OVERVIEW OF KHATTAB MEDIA FOUNDATION**

29. As explained below, Khattab Media Foundation is an internet-based organization dedicated to supporting ISIS’s mission of violent jihad through the creation and dissemination of pro-ISIS propaganda.

30. ASHRAF AL SAFOO is a leader of Khattab. SAFOO and other Khattab members agreed to work in coordination with and at the direction and control of ISIS and ISIS’ media office to create and disseminate ISIS propaganda consistent with ISIS’s declaration promoting the “jihadi media.” SAFOO and other Khattab members communicated via closed Social Media Application groups. Through means described in greater detail below, the FBI has determined that AL SAFOO is the user of Social Media Application monikers “Abu Al’-Abbas Al-Iraqi,” “Abu Shanab” and “Abussi.”<sup>4</sup>

31. Khattab members coordinated their activities through various private groups on Social Media Application, each of which served a different function within

---

<sup>4</sup> The attribution of these monikers to AL SAFOO is discussed in detail in Section V below. The posts attributed to AL SAFOO on Social Media Application in this affidavit were made using one of these monikers.



the organization. I will refer to two particular groups in this affidavit as the “Staff Group” and the “Writer’s Group.” UCE1 has reviewed and preserved copies of communications among Khattab members in the Staff Group and Writers Group, to include AL SAFOO. The statements ascribed to Khattab members in this affidavit, including AL SAFOO, are taken from the Staff Group and Writers Group.

32. The Staff Group is a group on Social Media Application and was created on or about June 30, 2017. Although called the “Public Group” by Khattab members, the Staff Group was an invitation-only group, which based on posts made within the group, appears to include Khattab staff members. As of approximately April 2, 2018, the Staff Group had approximately 21 members, including AL SAFOO. According to posts made within the group and viewed by UCE1,<sup>5</sup> the group discussed and disseminated ISIS propaganda, in the form of graphic designs, videos, audio recordings and written articles, among others. Some of the propaganda was created by Khattab members.

33. The Writer’s Group is a Social Media Application group created on or about June 30, 2017 and included approximately 13 members, including AL SAFOO. According Writer’s Group postings, the Writer’s Group was responsible for coordinating, drafting, and publishing Khattab’s ISIS propaganda. This group was not public and new members needed administrator approval to join.

---

<sup>5</sup> AL SAFOO facilitated UCE1’s invitation into this group. Specifically, on or about March 11, 2018 after a discussion with AL SAFOO about assisting with proofreading draft publications, UCE1 was added to the “Writer’s Group” and “the Staff Group” group on Social Media Application which provided UCE1 all communications that remained in these groups going back to June 30, 2017, which total over 1000 pages. The communications are in Arabic and I have reviewed draft translations of many of the communications.



34. All posts identified in this affidavit from both the Writer's Group and the Staff Group are visible to all members of those groups, including AL SAFOO.

**A. Purpose of Khattab Media Foundation<sup>6</sup>**

*Khattab Pledged An Oath of Allegiance to ISIS*

35. Khattab members formalized the organization's support of ISIS by renewing Khattab's bayat, or oath of allegiance, to Abu Bakr Al-Baghdadi, the leader of ISIS. In or about March 2018, an administrator of the Writer's Group, using the account "Khattab Media Foundation" posted a statement entitled, "The Renewal of Bi'a." It stated:

To enrage the kuffar<sup>7</sup> and to terrorize them, we renew our bi'a to the commander of the believers and the caliph of Muslims sheikh Abu Bakr Al-Baghdadi, may Allah preserve him, to listen and to obey in what is desirable and undesirable and in times of hardship and prosperity, and to endure being discriminated against and to not dispute the orders of those in charge, unless I witness a clear apostasy, for which Allah has shown me a clear proof, and Allah is my witness.

36. I further understand that through this statement members of the Khattab Media Foundation Writer's Group, including AL SAFOO renewed their oath of allegiance, or bi'a, to ISIS, via its leader Abu Bakr Al-Baghdadi, and pledging to "listen and obey" and to "not dispute the orders of" ISIS leaders.

---

<sup>6</sup> The information contained in this Complaint describing Khattab Media Foundation is based my training and experience, my review of open source materials, my review of communications between AL SAFOO and UCE1, my review of material collected by UCE1 from groups on Social Media Application to which UCE1 had accessthat were devoted to the coordination of Khattab's ISIS propaganda activities.

<sup>7</sup> Kuffar means non-believer.

37. On April 2, 2018, AL SAFOO reposted this oath of allegiance in at least three Social Media Application groups, including 'Arin Al-Mwahidin [The Den of Monotheists], Baqia Wa Tatamadad [It is Here to Stay] and Jayish Al-Mujahidin (meaning, "The Army of the Mujahidin"). Based on the content and context of the reposting, I understand that AL SAFOO was publicizing Khattab and its members' support of ISIS to their audience.

38. Khattab's renewal of bi'a was also publicized in other Social Media Application groups. For example, on April 2, 2018, the renewal of bi'a was posted in a Social Media Application group that was not affiliated with Khattab.

*Khattab was formed to support ISIS's Propaganda Efforts*

39. Khattab was formed to create and disseminate propaganda on behalf of ISIS. Khattab members have stated that the images, articles and videos created and distributed by Khattab are meant to, *inter alia*, spread fear and recruit for ISIS.

40. For example, on or about June 30, 2017, CC2, a self-described online administrator for Khattab, wrote that Khattab Media Foundation was:

administered by many production brothers [Khattab members] who work to deliver, through experience and Allah's help, the idea. It is concerned with supporting those who are unjustly treated among the nation of Islam, and its oppressors through the true shari'a method. It is also concerned with supporting the Islamic Caliphate and its methodology.

41. Khattab's logo, depicted below, includes the black ISIS flag attached to the gold Khattab logo:





42. On or about May 23, 2018, Khattab released an organizational design, below, with a reaffirmation of their support for ISIS, with the accompanying message: “A new design, Khattab Media Establishment, titled (Soon in Baghdad), let the far and the near, the East and the West know that we have sworn and determined that without the Islamic State there is no security and no peace in Iraq or al-Sham.”

43. The FBI located a copy of the “Soon in Baghdad” design that was publically distributed on a Twitter account that has since been suspended.



44. Even before the renewal of the oath, Khattab members made clear that they were acting at the direction and in support of ISIS and ISIS’ media offices. For example, on November 4, 2017, AL SAFOO reposted in the Staff Group an encouragement for people to help ISIS in any way possible, to include by offering money or themselves. AL SAFOO wrote, “Thus, it was incumbent on us to support



them verbally and with money and soul and by inciting others to target the tyrants and expose the evil scholars and the Saudi rulers. Therefore, a media campaign was launched to support # land of\_two sanctuaries. So, we urge the supporters to back their brethren with their writings and verbally and with their inciting video clips and designs or through re-posting the campaign of # O\_Land\_ of revelation endure and #Fight\_ the Imams\_ of infidelity as well as the official and supportive releases that are relevant to this blessed campaign.”

45. On December 12, 2017, AL SAFOO reposted in the Staff Group additional encouragement for the Khattab media operatives to work harder to satisfy and support ISIS and ensure the success of ISIS, including by using propaganda to attack ISIS’s enemies. More specifically, he wrote:

Twitter #

My Brother/Al-Ansar

- You’re not dedicating more time for Twitter..!
- What’s going on?!
- Accounts are available, praise Allah, so what are you waiting for?!
- Don’t let the weakness afflict you. Get rid of your laziness, and..., o dear
- And how can they defeat us while we’re so many, praise Allah?!
- Be careful with the accounts and increase it, and spoil the lives of the infidels

46. On or about December 14, 2017, CC12, on the Staff Group, acknowledged that Khattab Media Foundation was representing ISIS when he sent the following: “A message to all the followers, especially the designers: I advise you to master your work and increase designs. By Allah, it’s a blaze that will devour the cross worshippers. Don’t forget you are the ones who represent the Islamic State on

the Internet, so present it in a fine way and terrorize Allah's enemies. Don't belittle your support for us because its impact is more intense than arrows."

47. Similarly, or about January 3, 2018, AL SAFOO posted an audio message on the Staff Group from Abu Musab al Zarqawi.<sup>8</sup> With the audio message, AL SAFOO encouraged other members of the Group to respond to ISIS's direction to spread ISIS's message as widely as possible on social media, specifically he stated:

Dear brother, the supporter, pay attention; when our State [ISIS] publishes and announces a new release and say, "Soon, Allah willing," in your opinion, what do you think it wants from us. They want us to spread the announcement on the widest scale because it is an important release. So what are you going to do? Gather your strength and set Twitter ablaze."

48. On or about January 28, 2018, CC1 published in the Staff Group an audio message entitled "Media war." CC stated that the message was from the "Islamic State" and that "The infidels have designated a large sum of money to stop the Islamic State Media and its supporters. The more the infidels restrict the media of our State [ISIS], the more we know that we are defending a great cause."

49. On or about May 23, 2018, AL SAFOO posted the following message on multiple Social Media Application groups, including the Staff Group, about Khattab's operations and the goals of its propaganda efforts: "Brothers, roll up your sleeves! Cut video publications into small clips, take still shots, and post the hard work of your brothers in the apostate's pages and sites. Participate in the war, and spread fear. The Islamic State doesn't want you to watch these publications only, rather IS [ISIS]

---

<sup>8</sup> Abu Musab al Zarqawi was the founder of Al Qaeda in Iraq, which was the precursor to ISIS.



wants to mobilize you. If you can't, then work on mobilizing others for the cause. Know that your rewards will be doubled during religious holidays, and letting them [the mujahidin] down is a sin that all Ramadan fasting month will not be able to wash it."

50. On June 12, 2018, a Khattab member wrote on the Staff Group about Khattab's loyalty to ISIS. "Since the electronic support takes the shape of making releases, designs, and articles; therefore, we will have a direct connection with Media Diwan.<sup>9</sup> This means that we work with them, and as a result, we listen to them and obey them. They are more familiar with their reality and their jurisprudence, so we have no right to interfere in their affairs, or dictate to them, or be disobedient unless they order us to sin at which point there will be no obedience anymore."

*Khattab's Rules of Dissemination of Information Online required acting at ISIS's direction and in support of ISIS and ISIS' Media Office*

51. As explained below, Khattab's rules stated that members, acting at the direction and control of ISIS and ISIS' media office, had to disseminate only information supportive of ISIS.

52. On or about November 30, 2017, CC17 published on the Staff Group Khattab Media Foundation's "rules for dissemination of information online." Specifically, he wrote:

Publishers should adhere to the following:

---

<sup>9</sup> Based on my training and experience, and my discussions with Arabic linguists, I understand divan or diwan to mean "office." In this context, I understand it to refer to ISIS's official media offices.

1. It's prohibited to disseminate any article that contains slander or self-promotion.
2. Disseminate whatever benefits the Islamic State: News, releases, articles, and tweets.
3. Any individual is allowed to disseminate, and his rights will not be violated as long as his postings support the Islamic State.
4. Commitment to the official [ISIS] announcement stipulating that it's not allowed to claim responsibility for any operation or attack which hasn't been announced by the State, may Allah glorify it.

53. On March 24, 2018, AL SAFOO reposted an admonishment to the Staff Group that members of Khattab must adhere to ISIS's official media statements and act in accordance with ISIS's instructions:

Dear supporter:

Why do we insist on saying, "Adhere to the official media?"

The answer simply is;

We are in a fierce media-war in which rumors are the main commodity for the apostates, Crusaders, the thwarted, and the suspicious.

The official media department has a reason for not publishing certain news.

It knows when to publish or to avoid publishing; which means not every news is good for publishing.

This means: Don't be an ear and a tongue for the enemy, without your knowledge!

Here— and sorry to say— there are sick individuals who seek fame at the expense of the Jihadists.

Don't be a burden on your brothers!

The Islamic State — and thanks to Allah— has media partners who will go into the battlefield with their cameras to show the truth, so help them and don't be a burden on them.

*Khattab coordinated with ISIS in its attempted merger with another ISIS propaganda group*

54. As explained below, between October 2017 and December 2017, members of Khattab discussed the possibility of a merger with another ISIS propaganda group, Al Wafa, but eventually abandoned the merger at ISIS's instructions. Al Wafa, like Khattab, disseminated ISIS propaganda on Social Media



Application. These events, further described below, illustrate that Khattab acted at the direction and control of ISIS and ISIS' media office.

55. On or about October 17, 2017, CC1 posted in the Staff Group, requesting that Khattab members schedule a time to discuss "a project to join or merge our foundation with another." AL SAFOO responded on or about October 18, 2017, providing dates and times that he was available to discuss the proposed merger.

56. On or about December 9, 2017, CC3 reposted an unknown individual's post in the Staff Group stating: "a statement about the return of Khattab Media Foundation to normalcy and being preoccupied with what's important and what satisfies the Lord of the Worlds. We're at the service of our Emirs and the Caliphate State [ISIS] (Allah bestows it unity), and to back down on any issue that might split the Monotheists<sup>10</sup>."

57. On or about December 9, 2017, CC1 posted the following to the Staff Group: "We would like to inform you and ask you, may Allah bless you, to leave [Al-Wafa' Foundation] in response to the order of the brothers, to whom we raised the matter as is, and they ordered us to leave with our people. The brief response was (At your service), and we're well intended."

58. On December 10, 2017, AL SAFOO posted the following statement to the Writer's Group discussing the failed merger:

The decision of merger was not in violation neither to Shar'iah nor to the State [ISIS] and it was done based on mere media discretion, therefore correction or mistakes made by any side are subject to personal discretion, because there is no measure to determine the correctness. So no one has the right to say that you made a mistake by the merger,

---

<sup>10</sup> Muslims who believe in the Oneness of Allah; One God.

because doing a mistake is a relative matter, besides, the State did not warn about the foundation before the merger.

And the decision to split [not to proceed with the merger] was in accordance with the State's [ISIS's] instructions; therefore, it was a right decision and all should now agree with you, and the management is thanked for this.

59. On or about December 10, 2017, CC1, to whom the above statement was directed, responded, in part "And thanks be to Allah alone, the brothers inside [ISIS] are aware of the matter."

60. On or about December 10, 2017, AL SAFOO responded to CC1's statement by posting the following statement:

I would say, brother, you did what you had to do. So don't let our foundation be driven away from its superior goal, which is our support for the Mujahidin, and let the foundation return to where it was, working under the direction of the [ISIS media] office not to be occupied with the chitchat. Don't forget, Allah defends those who believe. May Allah bless you and be generous in rewarding you.

#### **B. Structure and membership of Khattab**

61. Based on messages posted to the Staff and Writer's Groups, Khattab was organized into divisions, each with a different function within the organization. On June 30, 2017, CC1 announced the formation of the audio and writers division. CC1 directed that "the division is administered by brother [CC2] the crew functions according to the vision of the foundation in respect to audio and text. The composition and writing down the articles, drafting and completed here. If needed, they will be recorded and presented as audio. The brothers receive the audio and the text, record them and engineer them before handing them to the person in charge [CC2] who will make the proper decision about the product."



62. Sometime later, the audio and writers division were split into two divisions. In addition to those two divisions there was a design division, a production division, and an uploading and publishing division. Each division was led by a different Khattab member. On April 2, 2018, Khattab administrator CC1 informed the Staff Group that a product begins with the writers division and proceeds, in order, to the design, production and audio divisions before being sent to the uploading and publishing division for dissemination to multiple social media outlets in order to be “more harmful and more successful, and our message will be received and our work will not be lost this way and not just for the supporters.”

63. Some of the services provided by Khattab members included, based on their expertise, authoring articles, editing articles, creating and editing videos, sound editing and photoshopping images.

64. In order to spread their message of violent jihad as widely as possible, Khattab translated its propaganda into multiple languages. On occasion, Khattab designers used online translation programs which did not work as they planned. For example, on December 19, 2017, a Khattab member instructed other members to be careful about translations: “Two days ago, a design was circulated and the designer translated it from google. Instead of writing ‘Beheading’ Trump, he wrote kissing and hugging Trump. The Americans started laughing at the Islamic State. The image has circulated and it became a joke.” Accordingly, a translation department staffed by several Khattab members was dedicated to translating Khattab’s pro-ISIS

propaganda material into multiple languages including English, French, Bengali and Italian.

**C. AL SAFOO's Role in Khattab**

65. Prior to March 2018, based on communications within the Writer's Group, AL SAFOO was an active member. In March 2018, AL SAFOO was promoted to head writer in the Writer's Group. On or about March 22, 2018, CC3 announced in both the Writer's Group and the Staff Group that "Brother Abu-al-'Abbas Al-'Iraqi, Allah willing, and will be in charge of all the writers plus scenario writing, and would coordinate work between the writers."

66. On or about March 22, 2018, AL SAFOO responded to CC3's post in the Staff Group. AL SAFOO wrote, "... May Allah assist us on this duty. Welcome to the new writers. Oh Allah, brothers, for the support of your religion and State. Don't let an hour pass without having a share in support. If you can't, then don't let a day pass without supporting those who spent their blood and wealth, and keep your prayers." I understand that AL SAFOO was encouraging all Khattab operatives to support ISIS, through propaganda and other efforts, as extensively as possible.

67. On the same day, AL SAFOO responded to CC3's post in the "Writer's Group" announcing AL SAFOO's promotion and instructed:

Righteous brothers, the writers/  
Please observe the following as much as possible, when writing the articles:

Avoid duplication, and by duplication, I don't mean your articles only, rather, study the field, follow it, and write something distinctive, unique from the others, and put an effort in this. Our brother, Shaykh Abu Maysara Al-Shami used to stay up all night, researching one thing, and his articles were compiled in one book, so take from him by reading and learning.



68. On or about May 18, 2018, CC2 introduced a new member to the Writer's Group, and informed the new user that "Abu AL-Abbas is the head of the division here my gracious bother...Copies of articles will be here for review God willing, brother Abu AL-Abbas will brief you more into the topic detail." AL SAFOO responded and explained the workflow for the creation and dissemination of Khattab's ISIS propaganda: AL SAFOO wrote, "We have two reviewer brothers, Abu AL-BARA' and bother Ibrahim may God reward them good. Every article written by an author comes to me first then I forward it to the reviewers then it is forwarded to the designers then to classification/management/control then to upload and publishing." I understand the references to proofreaders, designers, coordination, uploading and publishing to be references to different roles within Khattab.

#### **IV. AL-SAFOO AND KHATTAB MEDIA FOUNDATION, FOLLOWING ISIS'S DIRECTION, CREATED AND DISSEMINATED ISIS PROPAGANDA**

69. I have reviewed publications and statements distributed by Khattab on various web forums including Social Media Application. The articles and videos, consistent with ISIS's direction, celebrate ISIS's terrorist acts and other activities, threaten terrorist attacks, and attempt to recruit and train ISIS terrorists and supporters.

##### **A. Khattab Created and Distributed ISIS Videos**

###### *The Brothers in Marawi*

70. On or about October 19, 2017, Khattab created and published a video called "The Brothers in Marawi" which was disseminated on multiple social media

forums.<sup>11</sup> The video appears to be a propaganda video glorifying death in battle on behalf of ISIS and encouraging individuals to fight for ISIS. The video is approximately three minutes in length and begins with a large depiction of the Khattab logo with the words “Khattab Media Foundation” under the logo. The title of the video appears next before an overhead shot of a town with the small picture of the ISIS flag superimposed in the upper right hand corner. The picture in the upper right hand corner alternates between the ISIS flag and the Khattab logo.

71. The video shows clips of individuals dressed in military garb holding weapons; engaging in battle; holding the ISIS flags; and finishes with injured and dead soldiers. In the background, a song in English plays with the words shown on the screen. The song praises the fighters of Marawi and states that “diamonds and pearls and palaces awaiting the man of Tawheed.” I know from my training and experience that Tawheed means, generally, that there is only one God.

*Our Gifts Are Ready*

72. On or about December 26, 2017, Khattab created and published a video called “Our gifts are ready” which was disseminated on multiple social media forums. I have reviewed the video. The Khattab Media Foundation logo appears in the upper right hand corner until the logo morphs into the ISIS flag. The video begins with a

---

<sup>11</sup> According to open source reporting, Marawi is a region of the Philippines that is controlled by the pro-ISIS Maute Group, formed in 2013 by brothers Omarkhayam and Abdullah Maute. In 2017, the Maute Group engaged in a five month long siege of Marawi that ended on October 23, 2017 with the intervention of the Philippine military.



computer-generated animation of families standing around a Christmas tree with presents underneath. In the background there is a large castle with a fireworks display; the castle appears to resemble a Castle in an amusement park. Next there is a brief clip of President Trump, stating: "You have to fight fire..." before the video cuts to explosions overseas<sup>12</sup> with images of dead and injured children being pulled from the rubble.

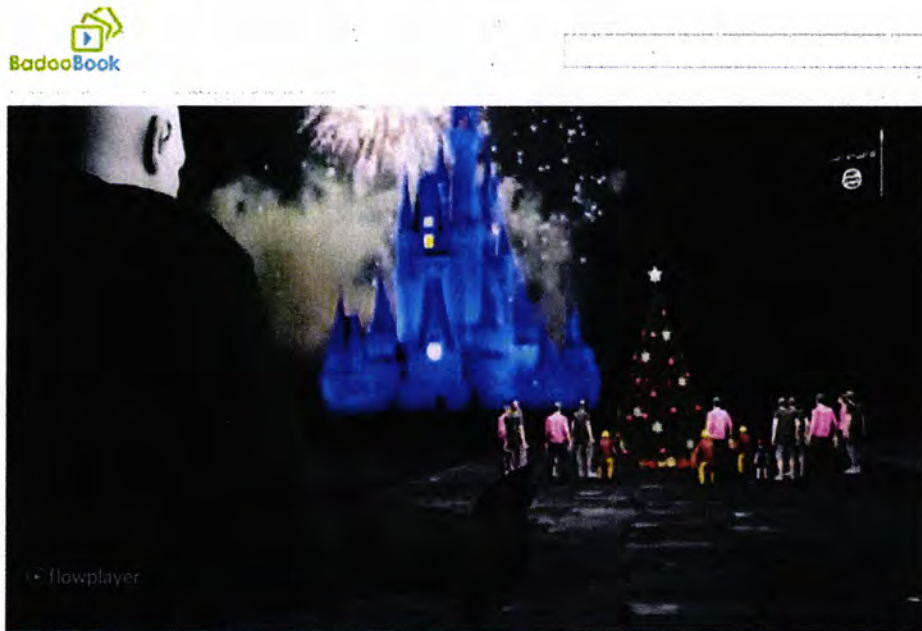
73. Next the video cuts to all black with the words "Now listen you dogs of hell. This is a message and more are going to follow. This is just the beginning. Our gifts are now ready." The video shows a present under the Christmas tree that contains a bomb with a timer ticking down before cutting to a news clip of a mass shooting taking place. The video returns to the animated families standing around the Christmas tree. Standing behind them is "The Khilafa soldir," dressed in all black and holding what appears to be a detonator. As he raises the detonator, the video flashes to various cities and iconic landmarks around the globe: Berlin, Brussels, London, Moscow, New York, Paris, and Sydney.<sup>13</sup> The soldier then detonates the bomb and the video is engulfed in flames. The final image is the Khattab Media Foundation logo. I understand that the publication of this video was in accordance with ISIS' direction to propagandists to strike fear in their enemies through propaganda.

---

<sup>12</sup> The explosions appear to be occurring in Syria.

<sup>13</sup> ISIS has claimed responsibility for terrorist attacks in all of these cities.

74. Below is a screenshot from the video



**OUR GIFTS ARE READY**

From: ascawss

Facebook

Twitter

Google+

75. On the Staff Group, CC15, instructed Khattab members to publish the video. "Now, now .....Shocking release from Khattab Media Foundation (Our Gifts are Ready) to encourage the lone wolves to attack the Crusaders and cause terror in their hearts. Post\_ O\_ Brothers\_ may Allah reward you with goodness. Video release by # Khattab Media Foundation titled [Our Gifts are Ready]."

76. On December 28, 2017, CC1 wrote to the Staff Group, "Praise be to Allah, the release has reached to some of the targeted ones." CC1 then distributed a review of the video by a third-party website. "In a new video...Da'ish [ISIS] threatens 7 Western states: 'Our gifts are ready now' Da'ish [ISIS] terrorist group threatened to carry out attacks in 7 Western states on Christmas via a video released today, Tuesday."



### *Shari'a Protectors*

77. Based on a communication reviewed and preserved by UCE1, on or about February 13, 2018, AL SAFOO, posted a 23-minute video titled "Shari'a Protectors" in Social Media Application group "Jayish Al-Mujahidin," which was another online group that publicized pro-ISIS propaganda. The video depicted the operations of ISIS against the Egyptian army in Sinai province. The video, which contains graphic footage of assassinations, close range combat and bloody scenes, warned the Egyptian people to stay away from polling stations during the upcoming presidential election in March 2018.

### **B. Khattab Created and Published Pro-ISIS Infographics**

78. Khattab frequently created and published infographics which combine photographs, computer generated images and texts. The infographics often contain threats in English that were addressed to Western countries and appear to be designed to inspire terrorist attacks.

### *Snipers*

79. On or about July 28, 2017, CC1 distributed to the Staff Group an infographic entitled "Strength is in Shooting."



80. The infographic promotes the virtues of being a sniper in furthering the goals of the Mujahidin. The upper portion of the infographic refers to a "PKK 190" which is an assault rifle, and states:

Some goals of the sniper...

Eliminating the leaders and surveillance patrols of the enemy army.

Eliminating specific individuals, based on confirmed intelligence and surveillance information.

Eliminating enemy channels, "There is no protection from a sniper, except another sniper."

Spying on the preparations and movements of the enemy.

Assisting the friendly forces to concentrate its shooting and directing it against the enemy, or to break a siege against the Mujahidin.

Protecting the leaders and patrols of the Mujahidin.

*September 11*

81. On or about September 11, 2017, Khattab distributed in the Staff Group the below infographic which stated "Our upcoming terror will make you forget what you saw in New Yoek (sp) and Washington Raids!":



OUR UPCOMING TERROR WILL MAKE YOU FORGET WHAT YOU  
SAW IN NEW YOEK AND WASHINGTON RAIDS !



### *Las Vegas Attack*

82. On or about October 2, 2017, CC3 claimed on the Staff Group that the attack on the concert in Las Vegas “was executed by one of the soldiers of the Caliphate.” C2 then directed members of Khattab to “launch of an interactive campaign along with the blessed operation that was executed by one of the soldiers of the Caliphate in the American city of Las Vegas.”

83. Later that day, Khattab published on The Staff Group the below infographic with the following message in Arabic “America has drowned and there is no rescuer. And it has become a prey for the Caliphate soldiers in every corner of Earth.” The infographic depicts the aftermath of the October 1, 2017, attack in Las Vegas. CC3 directed Khattab members to disseminate the infographic.



### *Khilafah's Presents*

84. On or about December 19, 2017, CC3 distributed in the Staff Group a photoshopped image of a headless Santa Claus sitting in a rocking chair next to a Christmas tree holding his head and with the message “New design# Khattab Media Foundation: Soon# the presents of the Caliphate State.” The infographic says, in English and Arabic, “The Khilafahs presents are on their way.”



85. The infographic of the headless Santa was publicly disseminated. On December 23, 2017, CC1 distributed on the Staff Group a report from a website which contained a photo of the infographic along with other photos with the caption “Pro-#Islamic State Media Outlets Circulating Posters Continues Threats Terror Attacks on #Christmas.” CC4 replied to CC1’s posting, “We ask Allah to help us turning our words into actions, making our intentions purely for His sake.”

86. On or about May 27, 2018, following the circulation in the Staff Group of a report by a United States based media organization regarding pro-ISIS groups threatening western cities and a U.S. theme park, and a link to an article by an online media organization entitled “Islamic Media Group Releases Infographic Video on Las Vegas Attack,” AL-SAFOO stated “Las Vegas video is destroying them. Our gifts are ready, my dear.”

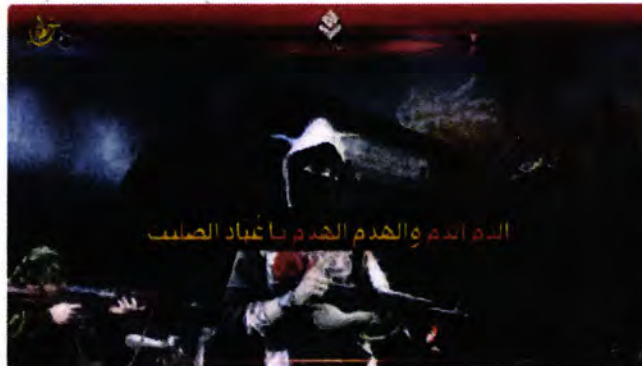
87. On or about May 22, 2018, AL-SAFOO encouraged Khattab members in the Staff Group to continue the work in support of ISIS when he uploaded a video called “Defeating the Enemy.” AL-SAFOO stated “work hard brothers. Cut the issue to short clips. Take the pictures out of it and publish the efforts of your brothers in



the pages of the apostates. Participate in the war. Spread fear. The State [ISIS] does not want you to watch it only. It incites you, and if it fails to do so, use it to incite others. Betrayal is a grave sin that cannot be forgiven even by fasting the whole month of Ramadan.”

*Hilween Attack*

88. On or about December 30, 2017, CC3 posted three infographics to the Staff Group that contain threats. The first was captioned, “New design title: Blood and destruction is on its way, O you worshipers of the Cross. #Khattab\_Media\_Foundation. #Hilwan\_Attack #MarMina\_Church.”<sup>14</sup>



89. The second infographic contained the caption, “#New design title ‘Do you think you will be safe on your #holidays and your planes are bombing Muslims!!! By Allah you will not enjoy your life as long as our hearts are beating’ #Khattab\_Media\_Foundation #MarMina\_Church.”

---

<sup>14</sup> The Hilweenn (Hilwan) attack was an attack on the Marmina Coptic Church in Cairo, Egypt on December 29, 2017. Nine people were killed and ISIS claimed responsibility for the attack.



90. The third infographic stated, “#New design title ‘O you Crusaders, O you Infidels and O you Atheists, by Allah, we will spoil your lives, our men enjoy drinking blood and enjoy the company of limbs’ #Khattab\_Media\_Foundation #Hilwan\_Church.”

*Call for Lone Wolf Attacks*

91. On December 30, 2017, CC3 posted to the Staff Group the infographic below that was created by Khattab and whose purpose appears to be to encourage “lone wolf” terrorist attacks in Western countries. The image depicted what appears to be a jihadi fighter standing in front of the Eiffel Tower. The caption accompanying the posting said, “To the Lone Wolves. #Khattab\_Media\_Foundation”





To The Lone Wolves

Get ready and prepare for this

Rely on Allah and rest assured that an infidel and his killer will never meet in the hellfire.

Raid them in their midst and break their hearts.

Spread joy in the hearts of your Muslim brothers. Avenge the widows and the orphans.

Do not stay still, rather ruin their lives and slaughter the last one of them.

Pray to Allah for steadfastness and acceptance in paradise

### **C. Khattab Created and Published Pro-ISIS Articles**

92. Khattab writers, including AL SAFOO, drafted articles that were designed to gather support for ISIS.

93. For example, in his article "From Inside," AL SAFOO praised jihad and martyrs who died for ISIS. AL SAFOO wrote, "Recognition of the truth of this false world and the beauty of jihad was not hidden from the young men in the land of the Caliphate who had just obtained the age of their religious obligation, so they sacrificed all that is dear in anticipation of what God has on offer." AL SAFOO

criticized those who have not committed jihad. He wrote, "You do not know that what prevented you from Jihad is nothing but sins; it is what imprisoned you just as an adversary imprisoned an opponent. It wasn't enough for you to watch the mujahidin who joined the march of the Caliphate...Even those with excuses are competing with the healthy ones in the arenas of battle. What is it that frightens you but does not frighten your sister? What is it that stops you but does not stop her?"

**D. AL SAFOO And His Co-Conspirators Staged Online "Raids" In An Effort To Flood Social Media With Pro-Isis Propaganda And Hid Their Identities With Anonymizing Software**

94. As explained in more detail below, AL SAFOO and Khattab members orchestrated "raids" on social media platforms in which they obtained social media accounts, and used those accounts, at scheduled dates and times, in an effort to post large volumes of pro-ISIS propaganda. As described below, AL SAFOO and other Khattab members were aware that social media platforms prohibit using their services to advocate violence or terrorism. As a result, they anticipated that accounts used in the raids would be suspended or shut down during or soon after the accounts were used to post pro-ISIS content. In an effort to access social media accounts, AL SAFOO and other Khattab members took steps to acquire access to as many accounts as possible to be used by ISIS supporters. They did this by creating social media account "banks," sharing individual accounts with Khattab members, and hacking the accounts of legitimate social media users. In addition, AL SAFOO and other Khattab members encouraged the use of software to hide the identities of Khattab members who posted pro-ISIS content online.



*Khattab Co-Conspirators Coordinated Twitter Raids*

95. On or about July 11, 2017, at approximately 1:37 p.m., CC3 posted to the Staff Group “We’ll have an attack today at six o’clock Mecca time” and asked “Who does want a Twitter account, brothers? So that we can start”. He stated that he “sent a private account” to CC6, who stated, “Yes, I got it.” CC also offered to give CC6 “the second one [account] to mount a secret attack.”

96. On or about July 15, 2017, CC1 coordinated another Twitter raid. He instructed, “[CC3]: Arrange the publications and the timing...While I get some accounts.” He asked, “Brothers: Do you need Twitter accounts? I have five of them with me as of now.” Based on the content and context of this conversation, CC1 was planning to share Twitter accounts with other Khattab members. Further, CC3 was arranging the timing of the raid and would provide pre-packaged links containing content to be posted during the raid.

97. Later the same day, CC3 wrote, “Brothers: We will carry out an attack today, Allah willing, at eleven o’clock Mecca time,” “Five minutes from now” and instructed the co-conspirators to “Be ready.” CC1 responded, “Let me de-activate the accounts, and activate VPN [Virtual Private Network]”. Based on my training and experience, I assess that de-activating the account and activating VPN was an effort to disguise the identities and locations of the co-conspirators participating in the raid.

98. CC1 coordinated similar Twitter raids with the Staff Group on or about September 28, 2017 and July 3, 2017. CC1 and C3 coordinated a Twitter raid on or about July 19, 2017. CC3 posted that there would be “an attack in Twitter” to the Writer’s Group on or about July 1, 2017.

99. On or about April 12, 2018, CC16 posted to the Staff Group, "I will launch an assault/invasion on Twitter and will post the tweets here." Approximately 37 minutes later, he announced the beginning of the raid, writing "Let us start brothers, Allah blesses you."

100. On or about May 20, 2018, CC13 announced a Twitter raid to the Staff Group, stating "Ready the accounts to invade active keywords on Twitter and Facebook." He said there was "A release from Khattab Media Organization. God willing." He posted a link to a Khattab video titled "Ramadan is invasion and jihad" to be posted during the raid.

*AL SAFOO and Co-Conspirators Knew That Social Media Platforms Closed or Suspended Pro-ISIS Accounts*

101. Based on open source material, I know that social media platforms including Twitter and Facebook have terms of service that prohibit the use of accounts to promote violence or terrorism.

102. As explained below, AL SAFOO and his co-conspirators were aware that social media accounts used to promote violence and terrorism would be suspended or closed. For example, on or about April 24, 2018, AL SAFOO re-posted an article in the Staff Group explaining that Facebook had "removed or put warnings on 1.9 million texts related to ISIS or al-Qaeda Organization during the first three months of the year" and "Facebook prohibits the terrorists from using its network." Based on my training and experience and the content and context of this message, I believe AL SAFOO was sharing this information with other Khattab members so that they would be aware that Facebook accounts linked to ISIS were likely to be shut down and allow



them to take additional steps to ensure that they could continue to post pro-ISIS content.

103. Other Khattab members shared similar information on Social Media Application. For example, on or about August 23, 2017, CC8, reposted information in the Staff Group about “the deletion against Islamic State supporters intensif[ying] on social media, such as #Twitter and #Facebook” as well as Social Media Application under the “pretense” of terrorism.

104. On or about February 12, 2018, CC1 wrote that a video “was removed for violation of YouTube[’s] policy, we ask Allah for obedience.” AL SAFOO responded, “Very normal.” Similarly, on or about February 12, 2018, AL SAFOO wrote in the Staff Group, “YouTube does not last. If you want it to last longer, You have to provide me with YouTube account. An unused one.” He added, “I lost my accounts. [sad face emoji]”. Based on the content and context of these posts, I believe that AL SAFOO was aware that Khattab’s and other pro-ISIS content violated YouTube’s policies and that accounts sharing pro-ISIS propaganda would be shut down quickly. A new, or unused, account would be needed to post pro-ISIS content.

105. Because the social media accounts used in Khattab’s raids were likely to be shut down, Khattab took steps to maximize efficiency in sending out pro-ISIS content by providing pre-packaged messages for raiders to copy and paste. For example, on or about July 3, 2017, CC1 provided instructions in the Staff Group on how to participate in the raids and acknowledged that the account would be removed.

106. Khattab members routinely provided sources for pre-packaged ISIS propaganda that could be posted to social media. For example, on or about September 25, 2017, CC8 posted in the Staff Group:

Archives Ammunitions of Tweets Channel ready for dissemination  
In reply to the Caliphate supporters' request, we provide its videos  
Invade [Social Media Application] to disseminate on Instagram and  
Facebook  
To save them the trouble of downloading clips from links  
Here, the releases are divided into small clips  
A search tool for any release in the channel

CC8 then provided a link to subscribe to the channel. Based on my training and experience and the content and context of this message, I understand that this channel included searchable pro-ISIS content available to be posted on social media and that CC8 was encouraging Khattab members to use this resource to spread ISIS's message of violent jihad. Further, because the content did not need to be "download[ed] from links," more messages could be sent out via social media before the Khattab members' accounts were closed for terms of service violations.

107. Khattab members routinely provided sources for pre-packaged ISIS propaganda that could be posted to social media. For example, on or about July 3, 2017 CC8 wrote that he had been given a Twitter account and asked "where do we find the postings that we need to disseminate?" In response, CC1 explained that tweets would be copied by CC3 and he provided a hashtag, "#End\_of\_ISIS\_lie," to be used in the campaign. CC1 also asked "Brothers. Do your part, even if it is just to set up your brothers. Give them to me, and I will throw with your arrows."

108. Similar messages sharing "tweets ready for posting" were shared by CC16 in the Staff Group on or about April 10, 2018.



*AL SAFOO And Co-Conspirators Used and Shared Hacked Social Media Accounts to Avoid or Delay Suspension of Pro-ISIS Accounts*

109. As described above, the policies and practices of social media platforms resulted in the suspension or closure of the pro-ISIS accounts used by AL SAFOO and other Khattab members. To circumvent these policies, AL SAFOO and other Khattab members discussed and shared methods of hacking into the social media accounts of legitimate users.

110. On or about June 8, 2018, CC14 engaged in a conversation in the Staff Group with AL SAFOO about using hacked Facebook accounts. CC14 wrote, "You need a seized Facebook account." AL SAFOO responded, "I need one provided that the owner is not a Muslim." CC14 responded, "No, a Crusader." Based on my training and experience and the content and context of this conversation, I understand that AL SAFOO wanted a hacked Facebook account that belonged to a non-Muslim Westerner [a Crusader] to use in promoting Khattab's pro-ISIS propaganda.

111. Similarly, on June 5, 2018, CC14, asked in the Staff Group "Does anyone need seized Twitter accounts?" AL SAFOO was the second person to respond, writing "and me too dear".

112. On or about April 12, 2018, CC13 discussed in the Staff Group the utility of hacking accounts with another Khattab user. This other user wrote that hacking an account "is better because it stays with you longer," and advised, "You are better off spending an hour hacking than a minute in creating an account. He then posted instructions, via a video link, to register accounts with an email service provider in order to hack Twitter accounts and wrote, "this technique is only for the supporters

of the Caliphate.” He further advised “Contact this bot” so you can be added to a channel that contains available emails. Access to the bot required proof that a user was an ISIS supporter, so CC13 advised “Tell him [the bot account] that you are from Khattab Establishment and he will add you.”

*AL SAFOO and Khattab Members Shared Methods to Conceal Their Identities to Avoid Detection by Law Enforcement*

113. On March 19, 2018, AL SAFOO reposted instructions in the Staff Group about maintaining anonymity and avoiding detection along with the hashtag #Your security\_is important to us. The instructions warned that ISIS supporters were being watched by government agencies. More specifically, he wrote:

Know this, oh supporter, that you are wanted by the security agencies of all the governments in the world. Imagine, if the sympathizer of a supporter is being arrested and humiliated, what do you think if it's the supporter himself?

The governments have thousands of methods to hack your device, their goal is to find out your geographic location and gather evidence against you.

The instructions continued:

You might wonder, ‘How can I protect myself then?’...

Don't do away with the secure VPN at all, no matter what, for there are codes that the hacker can discover you location through, if you don't run the VPN, without the use of any external applications. In the event you run the secure VPN, he will know your cyber location, without knowing your real location.

The secure VPN means encrypted and even the mother company can't give your file to any governmental party.

As for the unsecure VPN, it's unencrypted and your file will be given to the governmental party upon request.

If you were using a browser other than TOR<sup>15</sup>, don't forget to download applications to prohibit any leak of your personal IP, in any of the

---

<sup>15</sup> TOR (The Onion Router) is free software for enabling anonymous online communication.



circumstances, such as *WEBRTC* and *uBlock Origin*, and there are other applications that prohibit the leak of your personal IP.

114. On or about September 27, 2017, AL SAFOO reposted an advertisement in the Staff Group for a course in publication uploading: “Today, Wednesday, is the last chance to register for the second course of publication uploading, be a Mujahid and don’t be a spectator.” The advertisement included a link to the course and “suggest[ed] using the secured browser, TOR.” Based on the context of this post, I understand that the course was targeted to jihadists (“be a Mujahid and don’t be a spectator”). Further, AL SAFOO was encouraging fellow Khattab members to learn technical skills related to online publishing and to use TOR to protect their anonymity as participants in the course.

115. On or about March 26, 2018, AL SAFOO reposted, in the Staff Group, another warning to Khattab members to use VPNs to hide their identities. The post described the “widespread” practice among “the supporters” [of ISIS] to post links containing “publications” that are “from Naba’/ News or the [ISIS] official publications.” The post warned that a certain Website “gathers the materials related to Jihad from all the Jihadi groups in the world, in order to study it, submit ideas on how to fight the extremists, track the extremist, or take other measures. Every person who logs into the site or the posted link, his personal IP number will be stored within the site’s data, so the person can be tracked and information about him are gathered.” It continued, “Therefore, don’t access it except with a good VPN, or avoid it as much as possible. Don’t let your brothers fall in the traps of the enemy, warn them of the matter and guide them for what is beneficial and safe for them.”

**V. AL SAFOO is the User of Accounts “Abu Al’-Abbas Al-Iraqi,” “Abu Shanab,” AND “Abbusi”**

116. AL SAFOO has taken great measures to conceal his activity on Khattab’s social media accounts. For example, AL SAFOO uses Social Media Application, which uses end-to-end encrypted communications. AL SAFOO also informed UCE1 that he uses a second phone (Subject Phone 1), separate from his personal telephone, to conduct all his Khattab-related online activity. According to T-Mobile, this device is associated with a prepaid wireless service plan that appears to be paid in cash, which makes it more difficult to trace its user. As explained below, when AL SAFOO connects to the Internet through Subject Phone 1, he uses a Virtual Private Network (VPN),<sup>16</sup> which disguises SAFOO’s IP address by making it appear that his online activity originated at an IP address for a VPN service provider in the Netherlands. This allows him to mask his IP addresses and limits the ability to trace internet activity to his location. And, as described below, AL SAFOO also uses a variety of different email and other electronic accounts to hide his conduct.<sup>17</sup>

117. I have reviewed email provider records for multiple email accounts, information captured by UCE1 from the Khattab groups on Social Media Application, and the results of court-authorized searches of email accounts. Despite AL SAFOO’s attempts to conceal his identity and conduct, I have been able to determine that AL

---

<sup>16</sup> VPNs are used to maintain online anonymity. They assign temporary IP addresses to a user, which disguises that user’s true IP address when the user connects to websites or other online services.

<sup>17</sup> As discussed above, AL SAFOO’s efforts to conceal his identity are consistent with messages sent among Khattab members by AL SAFOO and other co-conspirators encouraging the use of VPNs and other measures to conceal their true identities.



SAFOO is the user of the monikers "Abu Al'-Abbas Al-Iraqi," "Abu Shanab" and "Abbusi" on Social Media Application.

118. Specifically, as set forth below, I have determined that "Abu Al'-Abbas Al-Iraqi," "Abu Shanab" and "Abbusi" are the same person, and that the person using these monikers also uses email accounts controlled by AL SAFOO. AL SAFOO has also used similar monikers for a PalTalk account associated with his telephone number. AL SAFOO also discussed his use of PalTalk on Social Media Application.

**A. Users "Abu Al'-Abbas Al-Iraqi," "Abu Shanab" and "Abbusi" on Social Media Application Are The Same Person**

119. As explained below, Social Media Application user @abuAl\_Abbas, with username, "Abu Al'-Abbas Al-Iraqi" is the same as the individual using username, "Abu Shanab."

120. According to review of the materials on the Staff Group, and illustrated by the examples below, AL SAFOO used the nickname "Abu Shanab" from approximately September 4, 2017 to November 12, 2017. AL SAFOO used the nickname "Abu Al'-Abbas Al-Iraqi" from approximately December 7, 2017 to approximately May 1, 2018. AL SAFOO used the nickname "Abbusi" from approximately May 2, 2018 to June 20, 2018.

121. For example, on September 8, 2017, a member in the Staff Group wrote, "Abu Al-'Abbas, how are you, good man??" Approximately thirteen seconds later, "Abu Shanab" responded to the query with, "Greetings, brother."

122. On or about October 19, 2017, a member in the Staff Group wrote the name, "Abu Al-'Abbas," in what appeared to be a roll call. Less than two minutes

later, "Abu Shanab" responded, "Absent," and then added, "I am present, I am not absent (smiley face emoji)."

123. On the same day, less than one minute later, CC3 wrote, "And upon you be peace, mercy and blessings of Allah, Greetings to you my dear brother, Abu al-'Abbas, May Allah bless you." Approximately 20 seconds later, group member "Abu Shanab" responded, "You just wanted us to worry about you."

124. On October 21, 2017, CC3 wrote, "Abu Al-'Abbas, you are right on time." Less than 30 second later, group member "Abu Shanab" wrote, "LOL, hello. Give me your order."

125. Similarly, "Abbusi" is the same as the individual using monikers "Abu Shanab" and "Abu Al-'Abbas Al-Iraqi".

126. On or about February 23, 2018, UCE1 began a private messaging conversation with AL SAFOO, who was using the moniker "Abu Al-Abbas" on Social Media Application. No other Social Media Application user was present in that chat session. The profile picture used by "Abu Al-Abbas" is depicted below:



127. On or about May 2, 2018, AL SAFOO's nickname changed to "Abbusi." Historical screenshots of the private chat between UCE1 from April 17, 2018 to May



9, 2018 show “Abbusi” used the same profile picture, depicted above, as “Abu Al-Abbas.”

128. In addition, Khattab members often responded to posts by “Abbusi” by addressing “Abbusi” as “Abu Al Abbas.” For example:

- a. On May 3, 2018, “Abbusi” posted in the Staff Group, “I think that I will post it.” A minute later, UCE1 responded to “Abbusi’s” post, “It is a beautiful voice...you are awesome Abu-al-‘Abbas my dear!”
- b. On May 18, 2018, CC2 introduced a new member of the Writer’s Group to “Abu al Abbas” and stated that “Abu Al Abbas” was “the head of the division here” and that “copies of articles will be here for review God willing. Abu al Abbas will brief you more.” Later, “Abbusi,” using the profile picture depicted above, and with the notation *admin* next to his name, responded to the new member “You are welcome gracious brother.”
- c. On May 29, 2018, “Abbusi” posted two paragraphs in the Staff Group titled, “The land of Iraq, the cradle of Caliphate.” An hour later, a Khattab group member was the first user to respond. That member wrote, “God bless you, Abu-al-‘Abbas.”
- d. On June 4, 2018, a user posted in the Staff Group, “Peace and mercy of Allah be upon you.” Less than 20 seconds later, “Abbusi” posted, “And upon you be peace and mercy of Allah.” Less than 5 seconds later, the

same member responded, "Greetings from Handalah to the beloved Aba al-'Abbas. How are you o dear?"

- e. In none of these instances did "Abbusi" tell UCE1 or other Khattab members that he was not "Abu al Abbas."

129. Based on the context of these communications, I believe that "Abbusi," "Abu Shanab" and "Abu Al'-Abbas Al-Iraqi" are the same person.

**B. AL SAFOO uses Subject Email Accounts 1, 2, 3, 4, 5 and 7, which are linked to posts on Social Media Application by "Abbusi," "Abu Shanab" and "Abu Al'-Abbas Al-Iraqi"**

130. I reviewed records for Subject Email Account 1; Subject Email Account 2; Subject Email Account 3; Subject Email Account 4; Subject Email Account 5; and Subject Email Account 7. As described below, AL SAFOO is the user of each of these accounts.

*AL SAFOO is the user of Subject Email Account 1.*

131. On or about January 13, 2018, AL SAFOO was interviewed by Customs and Border Protection (CBP). The interview was recorded. During the interview, AL SAFOO stated that he is the user of Subject Email Account 1. Based on a review of records from Google, the subscriber of Subject Email Account 1 is "Abo-Mohammad Ashraf" and the recovery email address is Subject Email Account 4. Based on my training and experience and review of records from Google, I know that a recovery email address is an email address registered by a user in case the user is locked out of the account.



*AL SAFOO is the user of Subject Email Account 2.*

132. According to Google records, Subject Email Account 1 is listed as a recovery email address for Subject Email Account 2. According to records, the subscriber name on this account is Abo Mohammad Al Iraqi, which indicates the user is from Iraq, consistent with AL SAFOO's background. According to information produced by Google, "cookies"<sup>18</sup> indicate that the same device accessed Subject Email Accounts 1 and 2.

*AL SAFOO is the user of Subject Email Account 3.*

133. According to Google records, Subject Email Account 1 is listed as a recovery email address for Subject Email Account 3. According to subpoena returns, the username and subscriber name ("Alsafoo Alsafoo") are consistent with AL SAFOO's name and similar to the username for Subject Email Account 1. Also, according to information produced by Google, "cookies" indicate that the same device accessed Subject Email Accounts 1 and 3.

*AL SAFOO is the user of Subject Email Account 4.*

134. According to Google records, Subject Email Account 4 is listed as the recovery email address for Subject Email Account 1 (and Subject Email Account 1 is the recovery email address for Subject Email Account 4). According to Google records, the subscriber name on the account is Ashraf al Safoo. The username, iraqimousl, is consistent with AL SAFOO's place of birth (Mosul, Iraq). According to information

---

<sup>18</sup> Based on my review of information received from Google, Google keeps records that can reveal accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites.

produced by Google, “cookies” indicate that the same device accessed Subject Email Accounts 1 and 4.

*AL SAFOO is the user of Subject Email Account 5)*

135. According to Google records, the subscriber name on the account is “Zoryna Mcckee” and the recovery email for the account is zyrasmith8@gmail.com.<sup>19</sup> The account was created on October 5, 2017, using IP address 5.79.76.77. According to open source searches, IP address 5.79.76.77 resolves to LeaseWeb, an internet service provider in the Netherlands that provides VPN services. As described in more detail below, SAFOO has used LeaseWeb.

136. According to information produced by Google, “cookies” indicate that the same device accessed Subject Email Accounts 5 and 7, which are both used by AL SAFOO.

*AL SAFOO is the user of Subject Email Account 7*

137. According to Google records, the subscriber name for Subject Email Account 7 is that of a known journalist who was killed by ISIS in 2014. According to information produced by Google, “cookies” indicate that the same device accessed Subject Email Accounts 1 and 7.

*Common IP Addresses Were Used to Access Subject Email Accounts 1-7*

138. IP addresses also demonstrate that AL SAFOO is the user of Subject Email Account 7. According to records obtained through a court-authorized search,

---

<sup>19</sup> Zyrasmith8@gmail.com is subscribed to by “Zyra Smith.” The recovery email address for zyrasmith82@gmail.com is shami\_01@tutanota.com. As described below, shami\_01@tutanota.com is an email address associated with a Paltalk account used by AL SAFOO.



Subject Email Account 7 was active from October 13, 2017 through January 2, 2018.

IP addresses used to log into Subject Email Account 7 were also used to log into Subject Email Accounts 1, 2, 4, and 5. For example:

- a. IP address 185.230.125.135 was used to log into Subject Email Account 7 between December 16 and December 19, 2017. The same IP address was used to log into Subject Email Account 4 multiple times on December 18, 2017.
- b. IP address 185.212.170.120 was used to log into Subject Email Account 7 multiple times on October 24, 2017. The same IP address was used to log into Subject Email Account 4 hundreds of times in December 2017.
- c. IP address 185.212.170.113 was used to log into Subject Email Account 7 twice on December 9, 2017. The same IP address was used to log into Subject Email Account 1 on November 1, 2017.
- d. IP address 185.212.170.119 was used to log into Subject Email Account 7 on November 10-11, 2017 and December 9-10, 2017. The same IP address was used to log into Subject Email Account 1 on November 12 and November 14, 2017.
- e. IP address 85.212.170.120 was used to log into Subject Email Account 7 on October 25, 2017. The same IP address was used to log into Subject Email Account 1 on October 26, 2017.

- f. IP address 185.212.170.119 was used to log into Subject Email Account 7 on November 10-11, 2017 and December 9-10, 2017. The same IP address was used to log into Subject Email Account 2 on November 14, 2017.
- g. IP address 94.75.250.216 was used to log into Subject Email Account 7 between November 5 and November 8, 2017. The same IP address was used to log into Subject Email Account 5 on November 6 and 7, 2018.
- h. IP address 85.212.170.120 was used to log into Subject Email Account 7 on October 25, 2017. The same IP address was used to log into Subject Email Account 5 on October 23, 2017.

139. All of the IP addresses referenced above belong to LeaseWeb, a Netherlands-based Internet service provider that also provides VPN services. Based on data from an internet service provider for AL SAFOO's home, AL SAFOO is a user of LeaseWeb's services. Similarly, Subject Email Accounts 1 through 4 and 7 all frequently were accessed through LeaseWeb IP addresses.

140. Moreover, LeaseWeb's records indicate many of these IP addresses were assigned by Leaseweb to ExpressVPN, another internet service provider that offers VPN services. AL SAFOO's financial records show payments to ExpressVPN.

141. AL SAFOO's use of VPN services is consistent with the operational security methods he advocated online. VPN services hide a user's online activities. For example, AL SAFOO encouraged UCE1 to use VPN services.



142. In light of the overlap between cookies, recovery email addresses, IP addresses, and use of VPN services, I believe that AL SAFOO is the user of Subject Email Accounts 1, 2, 3, 4, 5, and 7.

**C. AL SAFOO's Email Addresses are Connected to Social Media Application Users "Abu Shanab" and "Abu Al'-Abbas Al-Iraqi"**

143. I reviewed records for Subject Email Accounts 1, 2, 3, 4, 5 and 7 and Social Media Application postings by "Abu Shanab" and "Abu Al'-Abbas Al-Iraqi." This review connected AL SAFOO's email addresses with Social Media Application postings by "Abu Shanab" and "Abu Al'-Abbas Al-Iraqi."

144. First, records provide by Google show the user of Subject Email Account 5 posted YouTube videos on Social Media Application as Khattab user "Abu Shanab" and "Abu Al'-Abbas Al-Iraqi." On or about October 11, 2017, Social Media Application user "Abu Shanab" posted several URLs in the Staff Group. Under the URLs, "Abu Shanab" wrote: "New links uploaded by me. For the release. State of Al-Khyar."<sup>20</sup> One of the URLs was <https://photos.app.goo.gl/RnCFPqljOXhSqxXXXX> According to Google records, this URL ([photos.app.goo.gl](https://photos.app.goo.gl)) is for a Google Photos account for Subject Email Account 5.

145. Second, court-authorized searches of Subject Email Account 7 revealed that AL SAFOO posted ISIS propaganda to YouTube using Subject Email Account 7. Soon thereafter, users "Abu Shanab" and "Abu Al'-Abbas Al-Iraqi" posted the unique

---

<sup>20</sup> State of Al-Khyar is in reference to Dayr Az Zawr. Dayr Az Zawr is a town in Eastern Syria, which was an ISIS stronghold.

YouTube links for the same videos to Khattab groups on Social Media Application. Additionally, Khattab-created propaganda was found in Subject Email Account 7.

*The November 6, 2017 video*

146. On November 6, 2017, at approximately 2:26 p.m., “Abu Shanab” posted the URL: <http://www.youtube.com/watch?v=xXAs34AXXXX>, and a still shot of an ISIS beheading video in The Staff Group. The video displayed ISIS’s black flag in the corner.

147. On November 7, 2017, at approximately 1:33 a.m., AL SAFOO, using Subject Account 7, performed an internet search for the Arabic text contained in the hashtag of the video above. I believe AL SAFOO was searching to see if his video would come up in open source searches.

148. At approximately 2:02 a.m., on November 7, 2017, AL SAFOO, using Subject Account 7, received an email message containing the YouTube URL referenced above. This email confirmed that the user of Subject Account 7 (AL SAFOO) had successfully posted the video to YouTube. Approximately one hour later, Subject Account 7 received a message stating that the YouTube video was removed because its content violated YouTube’s guidelines.

149. Based on my training and experience, I believe that AL SAFOO used Subject Email Account 7 to post the YouTube video to the Staff Group on Social Media Application.

*The December 17, 2017 video*

150. On December 17, 2017, at 1:48 a.m., “Abu Al’-Abbas Al-Iraqi” posted a series of links to the Staff Group. Among them was “#Al-Hayat Media Center



presents | Visual: From Within 5" along with the URL <http://www.youtube.com/watch?v=6YdmY-zXXXX>. "Abu Al'-Abbas Al-Iraqi" then wrote, "Working Youtube links for posting." Based on my training and experience and the content and context of this post, I understand that AL SAFOO was sharing pro-ISIS content with Khattab members for them to repost on social media and other online platforms.

151. On December 17, 2017, at 2:35 p.m., AL SAFOO, using Subject Email Account 7, received an email from YouTube stating that YouTube user "Harabi," posted a "new comment on your video," located at URL <http://www.youtube.com/watch?v=6YdmY-zXXXX>.

152. Seventy-four minutes later, AL SAFOO, using Subject Email Account 7, received a message from YouTube stating the video located at URL <http://www.youtube.com/watch?v=6YdmY-zXXXX> was removed because its content violated YouTube's guidelines.

*The March 28, 2018 video*

153. On or about March 28, 2018, the Google Drive<sup>21</sup> account for Subject Email Account 7 contained a video file titled "libya\_1.mp4" which was a pro-ISIS propaganda video produced by Khattab. Khattab Media Foundation appears in writing in the video. The video showed, among other things, images of ISIS fighters fighting in Libya.

---

<sup>21</sup> Google account holders can store files, including but not limited to e-mails, documents, and image files, on servers maintained and/or owned by Google. The online data storage service is known as "Google Drive."

*The December 21, 2017 Pro-ISIS Newsletter*

154. On December 20, 2017, at 2:36 a.m., user “Abu Al’-Abbas Al-Iraqi” posted a link in the Staff Group to a pro-ISIS newspaper, “Al-Anfal, issue 4,” and noted that his article and Khattab’s media logo were published in this newsletter. On December 21, 2017, at 1:33 a.m., AL SAFOO’s Google Drive account for Subject Email Account 7 contained “Al-Anfaal, issue 4.”

**D. AL SAFOO Used Monikers Similar To “Abu Al’-Abbas Al-Iraqi” For His Paltalk Accounts**

*AL SAFOO is the user of Subject Email Account 8*

155. According to AL SAFOO’s immigration records, AL SAFOO provided Subject Account 8 as his email address on his passport application. According to Yahoo records, Subject Account 8 was subscribed to by Ashraf Al-Safuo, with recovery email address Subject Email Account 1 and telephone number XXX-XXX-0055.

*AL SAFOO is the user of Subject PalTalk Account 1.*

156. According to Paltalk records,<sup>22</sup> Subject Email Account 8 is the subscriber email address for a PalTalk account subscribed to by “Ashraf Al-Safuo” (“Subject PalTalk Account 1”). The nickname for the account was “3ra8e\_asel.”

---

<sup>22</sup> Based on my training and experience, I have learned that Paltalk is a proprietary video group chat service that enables users to communicate via video, internet chat, and voice. It offers chat rooms and the ability for users to create their own public virtual chat room. Paltalk users can also have private video chat sessions with up to fifteen other users. Paltalk Desktop is available on macOS and Windows while Paltalk Video Chat App is available for Android and iOS. To sign up, a user must provide an email address, and choose a nickname and password.



*AL SAFOO is the user of Subject PalTalk Account 2.*

157. A second PalTalk account was subscribed under email address shami\_01@tutanota.com (Subject PalTalk Account 2).<sup>23</sup> The username for Subject PalTalk Account 2 is “abo al abbas\_1” which is substantially similar to AL SAFOO’s moniker “Abu Al’-Abbas Al-Iraqi” on Social Media Application. According to PalTalk records, Subject PalTalk Accounts 1 and 2 logged in from the same device. On November 4, 2017, IP address 46.246.1.237 was used to access Subject Email Account 4 and Subject PalTalk Account 2. Two other IP addresses were used to access both accounts on different dates.

158. On November 24, 2017, as AL SAFOO was reentering the United States, a CBP search revealed that he was carrying an Apple mobile telephone. According to Apple’s records, this device was associated with email account shami\_02@tutanota.com, which is nearly identical to shami\_01@tutanota.com, the subscriber email for Subject Paltalk Account 2.<sup>24</sup>

*AL SAFOO is the user of Subject PalTalk Account 3.*

159. A third PalTalk account was subscribed under email address ash.aponte.84@tutanota.com (Subject PalTalk Account 3). The username for Subject PalTalk Account 3 is “Abo-Al\_Abbas”, which is substantially similar to AL SAFOO’s

---

<sup>23</sup> This is the same email address listed as the recovery email address for Zyrasmith8@gmail.com. Zyrasmith8@gmail.com is the recovery email address for Subject Email Account 5. Based on the connections between Subject Paltalk Account 2, Subject Email Account 5 and Zyrasmith8@gmail.com, I believe that each is used by AL SAFOO.

<sup>24</sup> This email address also is associated with a Skype account that has the identical profile picture as the Social Media Application profile picture of “Abu Al’-Abbas Al-Iraqi” and “Abussi.”

moniker "Abu Al'-Abbas Al-Iraqi" on Social Media Application. According to PalTalk, Subject PalTalk Accounts 1 and 3 logged in from the same device. Also, on August 20, 2017 (three instances), and December 3, 2017 (two instances), the IP addresses used to access Subject Email Account 4 were used to access Subject PalTalk Account 3.

*AL SAFOO is the user of Subject PalTalk Account 4.*

160. According to PalTalk, Subject PalTalk Account 4 is registered to email address abo.alabbas@bk.ru and uses the nickname "Abo al-abbas", which is substantially similar to AL SAFOO's moniker "Abu Al'-Abbas Al-Iraqi" on Social Media Application.

161. I know that internet users often use the same or similar moniker online across various online services. AL SAFOO's various PalTalk nicknames identified above are similar to the Social Media Application user "Abu Al'-Abbas." I therefore believe that AL SAFOO was the user of Subject PalTalk Accounts 1, 2 and 3 and Social Media Application account with username "Abu Al'-Abbas".

**E. AL SAFOO Discussed His Use of PalTalk on Social Media Application**

162. On October 18, 2017, "Abu Shanab" posted in the Staff Group "By Allah o my dear, it has been a very long time since I joined Paltalk." He further stated that he would try to access PalTalk on the following Sunday evening, October 22, 2017.

163. AL SAFOO, using Subject Email Account 8, received notifications from PalTalk on March 17, 2017, June 14, 2017, and September 14, 2017, addressed to "3ra8e\_asel," the username for Subject PalTalk Account 1. The notifications indicated that AL SAFOO had not recently used his PalTalk account and invited him to use the



service again. Subject Email Account 8 stopped receiving the above notifications after September 2017, indicating this user accessed and used Paltalk.

**VI. Conclusion**

For the reasons stated herein, there is probable cause to find that ASHRAF AL SAFOO has conspired to provide material support or resources to ISIS, in violation of Title 18, United States Code, Section 2339B.

FURTHER AFFIANT SAYETH NOT.

---

Jennifer M. Hergenroeder  
Special Agent, Federal Bureau of  
Investigation

SUBSCRIBED AND SWORN to before me on October 16, 2018.

---

M. David Weisman  
United States Magistrate Judge

AO 93 (Rev. 11/13) Search and Seizure Warrant

AUSAs Vikas Didwania, Barry Jonas, Melody Wells,  
(312) 353-5300

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

All electronic devices in the possession of ASHRAF AL  
SAFOO, further described in Attachment A -2

Case Number:

**18 M650 . 1**

**SEARCH AND SEIZURE WARRANT**

To: Jennifer M. Hergenroeder and 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 Northern District of Illinois:

**See Attachment A-2**

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

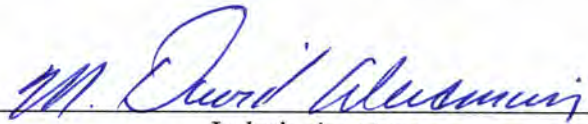
**See Attachment B**

**YOU ARE HEREBY COMMANDED** to execute this warrant on or before October 30, 2018 in the daytime (6:00 a.m. to 10:00 p.m.).

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 the issuing United States Magistrate Judge.

Date and time issued: October 16, 2018 @ 6:01 p.m.

  
Judge's signature

City and State: Chicago, Illinois

M. DAVID WEISMAN, U.S. Magistrate Judge  
Printed name and title



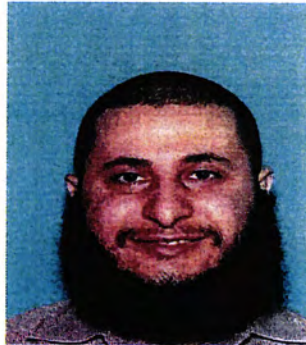
AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No:	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:		
<div style="height: 400px;"></div>		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: _____</p> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 45%;"></div> <div style="width: 45%; text-align: center;"> <p>_____</p> <p><i>Executing officer's signature</i></p> <p>_____</p> <p><i>Printed name and title</i></p> </div> </div>		

**ATTACHMENT A-2**

**DESCRIPTION OF PREMISES TO BE SEARCHED**

All electronic devices in the possession of the SUBJECT PERSON, identified as follows:



**Name:** ASHRAF AL SAFOO, a/k/a Abu Al'-Abbas Al-Iraqi, Abu Shanab, Abbusi  
**DOB:** XX-XX-1984  
**Hair:** Black  
**Eyes:** Brown  
**DLN:** A42101384142



**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

Evidence and instrumentalities concerning violation of Title 18, United States Code, Section 2339B, as follows:

1. Items related to the Islamic State of Iraq and the Levant ("ISIL"), the Islamic State of Iraq and Syria ("ISIS"), Abu Bakr al-Baghdadi, jihad, terrorism, martyrdom, bi'a, weapons or physical training, and any individuals or organizations associated with the above.
2. Items related to Khattab Media Foundation.
3. Items related to foreign travel.
4. Computer hardware, software and applications that enable connection of electronic devices to the internet, enable user anonymization, disguise a user's identity, conceal files and file folders, securely delete data, and encrypt communications.
5. Computer hardware, software and applications used to edit text, image, video or sound files.
6. Items related to the commission of acts of violence in the United States or overseas, including justifications for such conduct, the selection of a target or targets, the logistics of such conduct, and any tools or weapons to be used in such conduct.
7. Items related to the purchase or use of cellular phones.

8. Items related to use or acquisition of social media accounts.

9. Items concerning ownership or use of any computer and cell phone recovered, including, but not limited to:

a. evidence of who used, owned, controlled, or copied the computer, cell phone, and related media at time the items to be seized were created, edited, or deleted, such as logs, registry entries, configuration files, email and email contacts, instant messaging logs, saved usernames and passwords, encryption keys, documents, photographs, and correspondence; and

b. evidence of internet use relating to the items to be seized, such as browsing history and cookies, user profiles, Media Access Control (MAC) addresses, connection records, firewall logs, caches, "bookmarked" or "favorite" web pages, search terms entered into a search engine, and records of user-typed web addresses.

10. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints of ASHRAF AL SAFOO onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device found at the **Subject Premises** in order to gain access to the contents of any such device.



### **ADDENDUM TO ATTACHMENT B**

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.