UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with 28 identified Facebook User IDs that is stored at premises controlled by Facebook, Inc.

Case No. 18-M-120 (DEJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

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

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

The search is related to violations of: Title 18, United States Code, Section 2339B(a)(1).

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

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

Applicant's signature

FBI Special Agent Tori Gaskill
Printed Name and Title

Sworn to before me and signed in my presence:

Date: Aug. 9, 2018

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones, U.S. Magistrate Judge
Printed Name and Title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH 28 IDENTIFIED FACEBOOK USER IDS THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK, INC.	Case No. 18-M-120 (DEJ)

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Tori R. Gaskill being duly sworn, hereby depose and state the following:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search information associated with Facebook user IDs: 100018358660648, 100015538297029, 100003394781813, 100002111932375, 1202263650, 100006301360001, 708785463, 100003682534004, 100001337974954, 100002115677945, 100004689817817, 100004739910411, 100003449454063, 100002880451310, 100000330381596, 100003893321780, 100003310066527, 100003105302942, 100004455614176, 100002393547312, 100006207193027, 100002721214567, 100011611800178, 100007837176059, 100003229702265, 100004452642186, 100004693445122, and 1756849699 that is stored at premises controlled by Facebook (collectively referred to as the "ACCOUNTS").

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been employed since September 2008. I am currently assigned to the Joint Terrorism Task Force at the Milwaukee Field Office, where I conduct a variety of investigations in the area of

counterterrorism in the performance of my duties. I have investigated and assisted in the investigation of matters involving violations of federal law related to domestic terrorism international terrorism, weapons of mass destruction, the distribution of bomb-making materials, and material support, including in the preparation and service of criminal complaints and search and arrest warrants. I have conferred with colleagues who have received specialized training from the FBI in investigating crimes related to explosives, biological weapons, and weapons of mass destruction.

3. The statements contained in this affidavit are based in part on my personal knowledge, as well as on information provided to me by other law enforcement officers and civilians. This affidavit is being submitted for the limited purpose of securing the requested search warrant, and I have not included each and every fact known to me concerning this investigation.

4. Based on facts set forth in this affidavit, I submit there is probable cause to believe that WAHEBA ISSA DAIS has attempted to provide material support to a foreign terrorist organization in violation of Title 18, United States Code, Section 2339B(a)(1). DAIS is also known by an alias referred to here as "HE." On June 13, 2018, DAIS was charged by criminal complaint with attempting to provide material support or resources to ISIS, in violation of 18 U.S.C. § 2339B(a)(1). I submit there is also probable cause to search the Facebook ACCOUNTS for evidence, fruits, and instrumentalities of this crime.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2339B, relating to attempting to provide material support and resources to an FTO. Elements of the offense are the following: the defendant knowingly attempted to provide material support or resources to a

designated FTO; the defendant knew that the organization was a designated foreign terrorist organization, that the organization had engaged in or was engaging in terrorist activity or terrorism; and one of the five jurisdictional requirements is satisfied.

THE ISLAMIC STATE OF IRAQ AND AL-SHAM

6. On or about October 15, 2004, the United States Secretary of State designated Al-Qaeda in Iraq (AQI), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization (FTO) under Section 219 of the Immigration and Nationality Act and Specifically Designated Global Terrorist under Section 1(b) of Executive Order 13224.

7. On or about May 15, 2015, the Secretary of State amended the designation of AQI as a FTO under Section 219 of the Immigration and Nationality Act and Specifically Designated Global Terrorist 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 FTO listing: The Islamic State of Iraq and al-Sham (ISIS—which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria (ISIS), ad-Dawla al'Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

BACKGROUND OF INVESTIGATION AND FACTS ESTABLISHING PROBABLE CAUSE

8. The FBI Joint Terrorism Task Force has been investigating WAHEBA ISSA DAIS (DAIS) as a suspect involved in the provision of material support to ISIS, in violation of 18 U.S.C. § 2339B. The investigation has revealed that DAIS, through the use of multiple social media accounts that she has hacked and taken over from unwitting victims and private social

media platforms, promotes ISIS ideology, recruits adherents to ISIS, advocates that her followers conduct attacks in the name of ISIS, collects information on how to make explosives and biological weapons and on how to conduct terrorist attacks, and distributes that information to individuals so they can conduct attacks on behalf of ISIS. For instance, DAIS used one of her pro-ISIS Facebook accounts (an account she hacked and took over from an unwitting victim) to direct an individual, whom she believed to be an ISIS supporter planning to conduct an attack in the name of ISIS, to her password-protected social media channel to find instructions on how to make Ricin and then suggested the individual introduce the Ricin to a government post or water reservoirs.

9. According to information provided by the Department of Homeland Security, DAIS was born on or about August 22, 1972, in Jerusalem, Israel, and was allowed to enter the United States without a passport arriving in Chicago, Illinois (via Paris, France), in approximately November 1992 because of her marriage to a U.S. Citizen (her husband filed for divorce in 2003). On DAIS's visa application, she indicated she intended to stay in the United States permanently as a housewife; that she was from Jerusalem; and that she could speak, read, and write in English and Arabic. DAIS is now a Lawful Permanent Resident of the United States and lives in Cudahy, Wisconsin, with five of her children, including three minors.

10. The FBI's investigation indicates that DAIS uses multiple Facebook, Twitter, identified social media, and email accounts that contain pro-ISIS statements and information on how to make biological weapons, explosives, and explosive vests. As explained in more detail below, information provided by Facebook pursuant to 18 U.S.C. § 2702 in approximately January 2018, revealed that a Facebook user with an identified screen name (referred here to as HE) and User Identification number (UID) ending in 1813 appeared to be a Wisconsin-based user posting

detailed instructions on how to make explosive vest bombs in support of ISIS. This Facebook user also appeared to be engaged in detailed question and answer sessions discussing substances used to make bombs. As also discussed more fully below, FBI investigation has determined this user was DAIS. Further investigation has revealed that DAIS has used multiple social media platforms to pledge allegiance to ISIS, promote ISIS's terrorist agenda, communicate with ISIS members overseas, facilitate and encourage recruitment and attack planning for ISIS, and distribute instructions on explosives and biological weapons to self-proclaimed ISIS members and to people she believed to be planning to conduct attacks on behalf of ISIS. The investigation has revealed that DAIS hacks Facebook accounts, taking them over from unwitting victims and changing the profile picture, friends list, and display name. FBI investigation has identified the following Facebook accounts as being used by DAIS to attempt to provide material support to ISIS, distribute information on bomb-making and recipes for Ricin, and facilitate attacks: UID ending in 1813, UID ending in 4063, UID ending in 2942, and UID ending in 6059. As explained below, these four accounts are a small fraction of the accounts the FBI has determined that DAIS has hacked and taken over as her own.

11. Based on the FBI investigation, I believe that DAIS, who has pledged her allegiance to ISIS, is actively promoting ISIS propaganda through social media channels in an attempt to radicalize and recruit ISIS members and to encourage ISIS supporters to conduct terrorist attacks. I further believe that DAIS has helped facilitate planning for attacks in the United States on behalf of ISIS and overseas by providing instructions on how to make explosives, biological weapons, and suicide vests, and providing detailed instruction to people interested in attacks and attack planning. DAIS has also expressed a personal desire to travel overseas in support of ISIS.

DAIS'S HACKING OF VICTIM FACEBOOK ACCOUNTS

12. Open source searches and information provided by Facebook pursuant to 18 U.S.C. § 2702 indicate that DAIS and the individuals who are communicating with DAIS on Facebook are using hacked Facebook accounts as a way to avoid law enforcement detection of their communications. When DAIS takes over a Facebook account, she changes the display name to a variant of HE (written in English and/or Arabic) and changes the profile picture. The profile picture used by DAIS on these hacked Facebook accounts was taken by a professional photographer and is of a young girl wearing a blue dress. The photograph was taken as part of a series documenting Yazidi, a minority population in northern Iraq, fleeing their hometown to escape violence caused by the Islamic State militants. This photograph can be found on the internet.

13. On or about January 11, 2018, an FBI confidential source (Source #1)[1] reported that DAIS is unemployed and has her Islamic husband (which means married by their religion and not law) pay the bills. Source #1 described DAIS as constantly on social media promoting ISIS and using an identified social media application to talk to "shady people" in the Middle East on a regular basis. Source #1 reported that DAIS uses accounts on Twitter and Facebook, but they are always being shut down due to her posting pro-ISIS propaganda. According to Source #1, DAIS also has numerous "throw away" e-mail addresses to create all these accounts. Source #1 stated that DAIS has a YouTube account that she subscribes to and possibly creates videos on how to hack into social media accounts and is able to crack passwords for Facebook accounts. As discussed below, FBI investigation has confirmed that DAIS hacks into Facebook accounts belonging to others, as

[1] Source #1 was opened in approximately January 2018. Some of his/her reporting has been corroborated, he/she has direct access through a sub-source, and he/she is considered reliable. To date, Source #1 has not been paid and is motivated by not wanting to lose his/her ability to obtain a Top Secret clearance for employment due to his/her association with the subject. Source #1 was applying for a position that required a TS clearance.

an operational security measure, and uses those accounts to promote ISIS and to facilitate ISIS recruitment and attack planning.

14. The FBI's investigation has identified multiple Facebook accounts hacked by DAIS. The following list of accounts includes examples of the multiple accounts and is not exhaustive. The information below was provided to the FBI pursuant to legal process, publicly available information, and open source research.

15. Review of account information received pursuant to legal process shows that Facebook account with UID ending in 1813 and display name (HE) was used to pass information on how to build explosives to members of ISIS. FBI investigation has revealed that the account previously belonged to an unrelated female (Victim No. 1) but was hacked and taken over by DAIS in approximately January 2018. According to Facebook, UID ending in 1813 was created in approximately January 2012 by a female in Carabobo, Venezuela. On or about January 4, 2018, the account's display name was changed to HE and the majority of the original friends were removed from the account. The same day, the account quickly began to add a large number of new friends. The account profile picture used was the distinct photo of the young girl in a blue dress that was previously discussed. After the account name was changed, it was frequently accessed from an Internet Protocol (IP) address that resolved to DAIS's residence. It is noted that on or about January 8, 2018, while using UID ending in 1813 to exchange private messages, DAIS provided email address baqyyia22@gmail.com as a means to contact her outside of Facebook. At that time, this email address was associated with DAIS and a phone number that was subscribed to by DAIS. Based on prior investigation and source reporting, I believe DAIS is the user of UID ending in 1813.

16. On or about January 23, 2018, I conducted an open source search of DAIS's alias, HE, and identified UID ending in 4063, which also appears to have been hacked and taken over from a female in Venezuela (Victim No. 2). My review of publicly available information on this account revealed it had the same distinct profile picture as UID 1813. The account was previously used by a female whose profile showed she studied at a University in Carabobo, Venezuela. Review of account information received pursuant to legal process shows this account was created in approximately January 2012, and on or about January 8, 2018, the friends from the original account were removed. On or about January 23, 2018, the account name was changed to a variant of HE and new friends began to be added. After the name of the account was changed, it was accessed frequently from an IP address that resolved to DAIS's residence. Based on prior investigation and source reporting, I believe DAIS is the user of UID ending in 4063.

17. On or about March 2, 2018, an FBI Undercover Employee (UCE) looked up Facebook user name HE and discovered Facebook account with UID ending in 2942 with that name and DAIS's distinct profile picture. The UCE's review of UID ending in 2942 showed the subscriber is from Venezuela (Victim No. 3). The UCE sent DAIS a private message, asking for advice and DAIS provided email address baqyyia22@gmail.com to the UCE as her email address. Open source information indicates that an IP address that has accessed this account resolves to South Milwaukee. Also the same IP address has accessed three email accounts that are known to belong to DAIS. Based on the foregoing, I believe DAIS uses Facebook account UID ending in 2942.

18. On or about April 23, 2018, I conducted an open source search of HE in Arabic and identified Facebook account UID ending in 6059 under the display name of a variant of HE The account had the same distinct profile picture that DAIS is known to use. The profile indicates the subscriber is from Camp Grande, Brazil, and includes pictures of a young male. The rest of the

account is in Arabic. IP address records obtained via Grand Jury subpoena indicate that the IP address used to access the account resolved to 3441 Cudahy Avenue, Cudahy, WI. I believe that this account was previously used by Victim No. 4 and then hacked by DAIS on or about April 12, 2018, when the cover photograph was changed to DAIS' distinct photograph. On or about April 25, 2018, HE posted a link to the audio of Abu Hasan Al-Muhajir's speech. Al-Muhajir is an ISIS official spokesman. His speech was released on May 22, 2018, by the Al-Furqan Foundation. HE described Al-Muhajir' speech as inciting and an inspiring speech that reflected the wisdom of ISIS leadership.

DAIS'S PLEDGES OF SUPPORT TO ISIS

19. DAIS has pledged her allegiance to ISIS on numerous occasions. On or about February 12, 2018, DAIS (using Facebook UID ending in 4063) posted on her Facebook wall, confirming that her posts are her beliefs and that she believes in the doctrine of ISIS: "#Caution. When I publish any statement I completely believe in it. I was and I continue to be on the doctrine of the Islamic State." DAIS (using Facebook UID ending in 4063) posted on her Facebook wall on or about February 10, 2018, a post titled "#Renewal of the pledge of allegiance one more time." DAIS wrote, "I pledge allegiance to Ameer al Mumineen [the commander of the faithful] Ibrahim al-Husaini al-Qarashi, [Abu Bakir al-Baghdadi] to listen and obey in what is desirable and undesirables 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." In response to this post, seventeen of her friends commented pledging their allegiance to ISIS as well.

20. A review of information provided from Facebook pursuant to 18 U.S.C. § 2702, identified a conversation on or about January 7, 2018, between DAIS (using Facebook UID

ending in 1813) and another self-proclaimed ISIS supporter (referred to here as AK) in which they discussed allegiance to ISIS and traveling to join ISIS. DAIS claimed she was born in the United States and was living there. She told AK that she had pledged allegiance to ISIS and was seeking a way to join ISIS in Syria but is forbidden from leaving the country. She further informed AK that an ISIS military trainer in Raqqa, Syria, was trying to assist her in getting to Syria via Turkey. DAIS declared she follows the path and ideology of the Islamic State and that she would not bow for any tyrants. She stated this numerous times throughout the conversation with AK. AK declared that he is a supporter of ISIS as well.

21. In this same conversation, DAIS told AK that she wanted to leave America, but could not and if she tried to leave, she would be arrested for "conspiracy to join." DAIS said that she prayed that Allah would facilitate her exit and that she may "try in a few months." AK told her that they "may end up in Paradise." DAIS told AK that she knew some brothers from Diwan (believed to refer to the ISIS Ministry) and that she had inquired and learned that she can travel to join ISIS without a male escort, which she did not have. DAIS stated she had an ISIS contact in Al-Raqqah who had told her to travel to Turkey and that he would arrange for a male escort to meet her, but then the individual left for Al-Barakah and was "martyred." She said that she had seen videos of him training soldiers online.

22. DAIS has pledged her allegiance to ISIS and has been praised by others for her online support of ISIS via Facebook account UID ending in 1813. For instance, on or about January 5, 2018, a Facebook user (referred to as AA) sent DAIS a private message that stated, "All your postings are in the service for Jihad and the Mujahidin. God bless you." On or about January 14, 2018, DAIS exchanged private messages with the user of Facebook UID ending in 4904 (referred to as AS) about restoring Facebook accounts that had been suspended. DAIS said,

"May God keep you safe" to which AS responded, "and may you stay with us on Facebook forever." DAIS said, "except…May God grant me martyrdom and I leave the Facebook." AS responded by telling DAIS that "we are in jihad to spread this message and the truth. As long as the message is God you will be rewarded... all of us wish for and ask God to grant us martyrdom." On or about January 24, 2018, DAIS (using Facebook UID ending in 4063) posted on her Facebook wall urging people to add #The_Supporters_Campaign to their friends list. The user of another Facebook account (Facebook User No. 7) responded by declaring DAIS a supporter of ISIS and very knowledgeable.

DAIS'S PROMOTION AND RECRUITMENT ACTIVITIES ON BEHALF OF ISIS

23. DAIS has used social media on multiple occasions to promote ISIS and its terrorist agenda and to attempt to recruit others to join ISIS and to commit attacks on behalf of ISIS. On or about January 30, 2018, the UCE conducted an open source search of DAIS's alias, HE, and identified Facebook account UID ending in 4063. Subsequently the UCE sent a friend request to that account and it was accepted that day. The UCE then was able to view the Facebook wall of UID ending in 4063. The UCE noted that DAIS had posted the following in Arabic: "#Attention to the non-#supporters brothers: I accepted your friend requests hoping that Allah will guide at least one of you [to become a supporter]."

24. On or about February 24, 2018, DAIS (using Facebook UID ending in 2942) posted a link to a social media channel entitled, "Khilafah Ray for Supporters Group." I believe Khilafah refers to the Caliphate, also known as ISIS. The UCE visited the channel on February 26, 2018, and noted that the page had multiple voice messages posted by DAIS's social media account @ISWarrior and they consisted of Jihadi songs and speeches by ISIS leaders. One of the

messages encouraged ISIS supporters who cannot travel to ISIS-controlled areas to conduct terrorist attacks in the countries where they reside. If military targets are not in their reach, then attacks directed at civilians are even more desirable by ISIS.

25. On or about January 23, 2018, DAIS (using Facebook UID ending in 4063) posted on Facebook that her social media channel, "The Caliphate's Ray," had been removed. She then posted links to two social media channels. A Facebook user (referred to here as II) posted that it suits DAIS well to be the press manager for ISIS. II continued to praise DAIS for her perseverance, efforts, and exemplary support of ISIS.

26. A review of information provided from Facebook on or about February 6, 2018, pursuant to 18 U.S.C. § 2702, identified a Facebook user (referred to here as OG) who was planning a potential ISIS attack and had been communicating with DAIS (using Facebook account with UID ending in 4063) about the attack. On or about January 26, 2018, OG asked DAIS if she knew about Sharia. DAIS responded by stating that OG should ask the question and DAIS would send it to an expert for an answer. OG stated that he would be traveling to France. He then said it would be better to die than rot in prison. He asked how he can take revenge for ISIS. He suggested running a car through people or shooting at people. He then asked how he would be judged by God after killing many people. DAIS responded that she will send him an answer later. On or about January 27, 2018, DAIS sent a link to a Facebook profile (referred to here as SM) and told OG to talk to this individual, that he will be beneficial to OG.

27. On or about January 28, 2018, OG and SM exchanged private Facebook messages. OG said he was a 25-year-old Algerian who had previously discussed plans with HE (using a short form for DAIS's alias) to travel to France. He said he wanted to plan an operation in support of ISIS so DAIS suggested he talk to SM. SM then sent OG the following pledge to ISIS: "Renewal

of the pledge of allegiance, we are renewing the pledge of allegiance to Sheikh Abu Bakr Al-Bughdadi [sic] to obey him in everything, not to go against his will, not to flee during the fight, not to deny the religion of God and God is our witness." OG requested weapons and brothers to help with his attack. SM reminded OG that the work is individual. On or about January 30, 2018, OG sent DAIS a message saying that DAIS is really knowledgeable.

DAIS'S DISTRIBUTION OF EXPLOSIVES & BIOLOGICAL WEAPONS INFORMATION

28. DAIS has distributed information pertaining to explosives and biological weapons on Facebook and other social media platforms in the form of videos and conversations about bomb-making and biological weapons materials. In particular, DAIS has used Facebook UID ending in 1813 to distribute information on how to build explosives and biological weapons so that people who want to commit violent acts in the name of ISIS will use this information to commit acts of violence. DAIS promotes violent acts in the name of ISIS on her Facebook pages to her Facebook friends who are self-proclaimed ISIS members and supporters. For instance, one friend of account ending in UID 1813 (Facebook User No. 8) has instructions for creating explosives and Ricin on his page and photographs that include the ISIS flag. On or about January 16, 2018, another friend of this account (Facebook User No. 9) engaged in a private message conversation with DAIS (using Facebook UID ending in 1813) in which he said he had been with ISIS for years and told her about specific battles and described the battlefield in detail. As described above, in a private message conversation with DAIS (using Facebook UID 1813), AK declared that he is a supporter of ISIS as well.

29. DAIS has posted numerous videos about explosives on Facebook. On or about January 8, 2018, DAIS posted a video on her Facebook page with UID ending in 1813. The video is a presentation from "Sawt al-Jihad" (translated as "The Voice of Jihad") and titled, "Explosive

Belt/Vest." The video purports to provide step-by-step instructions on how to make an explosive belt and then demonstrates the effect of the bomb when it explodes. Audio in the background plays a chant in support of Jihad. On or about January 11, 2018, DAIS posted a video on the Facebook page for UID ending in 1813. The video is titled, "The Practical Training in the Making of Ammonium Nitrate." The video purports to provide step-by-step instructions on how to make Ammonium Nitrate. On or about January 11, 2018, DAIS posted a video on the Facebook page for UID ending in 1813. The video is titled, "The Practical Training in the Making of TNT."[2] The video purports to provide step-by-step instructions on how to make TNT. Audio in the background plays a chant in support of jihad.

30. DAIS continually seeks to collect information on the best explosives and biological weapons techniques in order to pass this information on to would-be ISIS attackers. On or about January 8, 2018, DAIS used Facebook UID ending in 1813 to communicate with a Facebook user (referred to here as AO) about explosive vests. AO told DAIS that ISIS made a safer and more reliable explosive belt. AO explained that they do not use electronic detonators because they are dangerous and may explode prematurely and suggested a grenade with a fuse. DAIS asked if he had any videos or written instructions that he could share with her. AO then began to discuss plans to kill Jews overseas. At that point, DAIS suggested that AO not discuss such topics on Facebook because they are probably being monitored.

31. On or about January 9, 2018, DAIS (using Facebook UID ending in 1813) had a detailed conversation with AK about substances used to create bombs. On or about January 9, 2018, DAIS posted on her Facebook wall that Nitric Acid[3] can be found in gold stores but that a

---

[2] I know that TNT is Trinitrotoluene, a chemical compound that is a high explosive.
[3] I know that Nitric Acid is a strong acid chemical compound that carries oxygen atoms. It can be used to oxidize or provide oxygen to other chemicals utilized in explosives.

clearance is required to purchase it. DAIS recommended producing it because it is difficult to purchase. She then asked where it can be purchased in the Arab Peninsula. She proceeded to ask for the names of commercial fertilizers that would not trigger suspicion when asked about. She posted within the comments that she had heard that nitric acid is used to melt gold so she wanted to know if it could be purchased from gold stores and if that would raise suspicion. DAIS then asked that someone try to purchase nitric acid from a pharmacy after someone suggested it could be purchased that way. DAIS also recommended researching where to get instant fertilizer in Western countries. She then asked if there are nitrates in Potassium Nitrate. AK responded that Ammonium Nitrate[4] needs to be extracted from fertilizer because it is sold in large quantities to land owners. He recommended that this would make a good security cover. If asked questions, AK suggested that DAIS say she does not understand chemicals but is merely a farmer.

32. DAIS has attempted to provide material support to ISIS by providing detailed instructions on how to make Ricin to an individual seeking to commit an attack in the name of ISIS.

33. In particular, on or about March 2, 2018, the UCE sent a private message to DAIS (using Facebook UID ending in 2942) requesting her permission to discuss a sensitive and important topic that the UCE needed her opinion on. DAIS thanked the UCE for his/her confidence and trust. She encouraged the UCE to share his question. The UCE told DAIS that he/she had anticipated completing his/her master degree in a year, but could no longer stand living in the land of the infidel. The UCE stated he/she constantly clashed with colleagues and felt that government spies were everywhere. DAIS responded saying, "I am reading your words and unfortunately, you are causing your own demise by clashing with them. We live in a time where

[4] I know that Ammonium Nitrate is a chemical compound that is a strong oxidizer often used in explosives.

you do not know when you are going to be stabbed in the back. And I don't think the Islamic State would want its supporters be thrown in infidels' prisons. We cannot be of benefit to them like that." DAIS asked if the UCE knew why the September 11th attacks were successful and then answered it was due to their total secrecy. DAIS instructed the UCE to plan and not leak information. DAIS further stated, "[T]hey do not need any evidence. Just a tip and a suspicion. If someone says that this belongs to a terrorist group, they will come to your house, handcuff you and take you."

34. DAIS instructed the UCE to stay away from others, not discuss this idea with others, and secure the UCE's social media account. DAIS also told the UCE that he/she must act like an ordinary person. She also advised the UCE to not act interested in these topics and if someone asked about it, the UCE should tell them these topics do not interest him/her. DAIS emphasized that total secrecy is the most important thing and that the UCE must take time in planning, choosing a target, and studying it well from all aspects, even if it takes months.

35. DAIS told the UCE it is hard to join the [Islamic] State because they do not have much land under their control and instead it is better to execute an attack where you are. DAIS suggested potential targets for attacks, such as street festivals and celebrations in the summer, or churches. DAIS also advised that it should be something that would devastate and kill more than one person. Further, she said, "Learn how to make bombs and explosive belts as a preparation process. They've been talking about this for months." After the UCE said he/she has no experience making weapons or explosives, DAIS said, "No problem, making bombs is easy, and you can also start with poisons. I have a [social media] Channel you may benefit from." She further said, "I advise you to use poisons first" and then she again recommended her channel as a place to find an encyclopedia of poisons. DAIS told the UCE to let her know if the UCE needed

help. She said the easiest poison to make is Ricin, which she claimed is very effective and lethal to the touch. DAIS then sent a link to the social media channel and said, "Lessons in making explosives and everything related to Lone Wolves, may Allah make us beneficial." DAIS then asked, "Remember Boston Marathon bombing?" The UCE responded affirmatively, and DAIS said, "It was very easy to make. All it needs is a pressure cooker, shrapnel and explosives. Join my channel and research." The UCE asked if there were any poison recipes DAIS could send to the UCE, and DAIS responded, "Yes. I will send you the poison of Ricin for it is easier, more effective, and cannot be traced, even if the person dies, it cannot be found in the body. All you need is just two items." DAIS then said, "Castor seeds and Acetone." The UCE and DAIS then exchanged email addresses.

36. On or about May 2, 2018, the UCE and DAIS exchanged private messages via Facebook. The UCE asked DAIS about her social media channel titled, "Shu'a' Al-Khilafah for lone wolves." I believe Al-Khilafah refers to the Caliphate, aka ISIS. DAIS responded by providing a new link to a social media channel and stating that the link is not publicly available to members but rather just to the administrators. The UCE's review of the channel revealed that it is directed to "lone wolves" making poisons, explosives, weapons, and silencers. I believe that "lone wolves" refers to individuals who are inspired by one or more terrorist groups to commit attacks acting on their own. The channel has 89 members, four photos, 10 videos, 445 files and one shared link. The translated titles of the 92 documents the UCE pulled down all relate to explosives, guns, attack planning, and target selection.

37. On or about May 3, 2018, the UCE sent a private message to DAIS via Facebook account UID ending in 2186. The UCE asked if the account was the account of a variant of HE to which DAIS responded in the affirmative. The UCE said that he/she had downloaded the Ricin file

from DAIS's social media channel. DAIS said, "Good. May Allah make you successful. It's easy to make but remember to be cautious." DAIS continued to provide the UCE with advice such as wearing multiple gloves and covering the surface of the work table "because it's lethal to the touch." In discussing potential targets, DAIS suggests a government post or placing it in water reservoirs. During the conversation, DAIS told the UCE that she resides in the United States. The UCE asked DAIS if it was easy to travel to the Unites States and suggested there might be more targets in the United States. DAIS agreed and said there are many opportunities in the United States. DAIS offered that they could work together. Ricin is a biological toxin made from the castor bean.

38. A review of information provided from Facebook on or about May 11, 2018, pursuant to 18 U.S.C. § 2702, identified a conversation between DAIS (using Facebook UID ending in 2942) and a Facebook user (referred to here as EAR). EAR told DAIS, "I am in need of a way to build explosives by using agricultural fertilizer." DAIS replied, "Participate in my channel about explosives" and then provided a link to her channel titled "The Ray of the Khilafa- Explosives: Lone Wolves." The summary included with the link described the channel as providing "[l]essons in manufacturing of explosives and everything regarding Lone Wolves." EAR said that he would like to "build a bomb that can uproot a whole house. I am confused on which one to pick, and don't know how to formulate in grams of explosives and how to make it powerful." DAIS advised EAR that he needed to "start with a small amount, meaning don't make the whole thing at once. You have to experiment with small quantities and then make it bigger." EAR thanked DAIS for her advice.

PROBABLE CAUSE FOR EACH OF THE SUBJECT ACCOUNTS

39. As described above, FBI investigation has identified the following Facebook accounts as being used by DAIS to attempt to provide material support to ISIS, distribute information on bomb-making and recipes for Ricin, and facilitate attacks: UID ending in 1813, UID ending in 4063, UID ending in 2942, and UID ending in 6059. As discussed below, the FBI has identified an additional 22 accounts that DAIS is believed to have hacked and taken over as her own and 2 accounts that she is believed to have subscribed to herself. Based on the information detailed below and on the results of the FBI's investigation into DAIS material support activities, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2339B will be found in each of the subject ACCOUNTS.

40. As described below, at least 17 of the ACCOUNTS have used DAIS's distinct profile picture and 26 of the ACCOUNTS have used her alias, HE. At least eight of the ACCOUNTS have been used to communicate with or accept friend requests from the UCE. The FBI has forensically linked at least ten of the ACCOUNTS to DAIS. Moreover, at least ten of the ACCOUNTS have been accessed from an IP address that resolves to DAIS's residence or to South Milwaukee, where the residence is located, and at least three of the ACCOUNTS have been accessed primarily through a Virtual Private Network (VPN) that hides the location of the user. FBI physical surveillance has confirmed that DAIS spends most of her time at her residence, where she is believed to conduct her material support activities online.

41. The probable cause for each of the ACCOUNTS is detailed below:

a. 100018358660648: In or around July 2017, Facebook responded to a Grand Jury subpoena requesting any accounts linked to cellular telephone number (414) 346-6212, a number known to be used by DAIS. The results revealed Facebook account UID 0648 with user name

"Mothana Abu Omar" (believed to be a made up name). I do not believe this account was hacked as it was linked to DAIS's phone number.

b. 100015538297029: According to information provided by Facebook pursuant to 18 U.S.C. § 2703(d) on or about September 22, 2017, Facebook account with UID ending in 7029 was created in February 2017 with DAIS's known screen name of HE and registered to e-mail account Hendsalah905@yahoo.com, an email address DAIS is known to have used. I assess the account was not hacked as it was tied to DAIS's e-mail account.

c. 100003394781813: As described above, on or about January 16, 2018, information provided by Facebook pursuant to 18 U.S.C. § 2702 revealed that a Facebook user with the screen name HE and UID ending in 1813 appeared to be a Wisconsin-based user posting detailed instructions on how to make explosive vest bombs in support of ISIS. In or about January 2018, the FBI forensically linked several accounts by reviewing cookie data provided by Facebook pursuant to 18 U.S.C. § 2702. In particular, the FBI determined that the following Facebook accounts had been accessed from the same device that had accessed UID 1813: UID 2375, UID 3650, UID 0001, UID 5463, UID 4004, UID 4954, UID 7945, UID 7817, and UID 0411. Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins to UID 1813 resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. As also described above, FBI investigation has revealed that UID 1813 previously belonged to an unrelated female (Victim No. 1) but was hacked and taken over by DAIS in approximately January 2018. I assess DAIS hacked this account in approximately January 2018, and therefore the requested search is from January 1, 2018, to the present.

d. 100002111932375: In or about January 2018, the FBI determined that Facebook UID 2375 was in the name of HE and was being accessed from the same device that had

accessed Facebook UID 1813 (described above). Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. After reviewing the IP login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

e. 1202263650: In or about January 2018, the FBI determined that Facebook UID 3650 was in the name of HE and was being accessed from the same device that had accessed UID 1813. Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. After reviewing the IP login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

f. 100006301360001: In or about January 2018, the FBI determined that Facebook UID 0001 was in the name of HE and was being accessed from the same device that had accessed UID 1813. Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. After reviewing the IP login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

g. 708785463: In or about January 2018, the FBI determined that Facebook UID 5463 was in the name of HE and was being accessed from the same device that had accessed UID 1813. Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. After reviewing IP login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

h. 100003682534004: In or about January 2018, the FBI determined that Facebook UID 4004 was in the name of HE and was being accessed from the same device that had accessed UID 1813. A Grand Jury Subpoena revealed the name of the account to be HE, but also showed that the account was accessed exclusively through a VPN preventing detection of location. After review of the IP login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

i. 100001337974954: In or about January 2018, the FBI determined that Facebook UID 4954 was in the name of HE and was being accessed from the same device that had accessed UID 1813 Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. After a review of IP login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

j. 100002115677945: In or about January 2018, the FBI determined that Facebook UID 7945 was in the name of HE and was being accessed from the same device that had accessed UID 1813. A Grand Jury Subpoena revealed the name of the account to be HE, but also that the account was accessed exclusively through a VPN preventing detection of location. After a review of IP login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

k. 100004689817817: In or about January 2018, the FBI determined that Facebook UID 7817 was in the name of HE and was being accessed from the same device that had accessed UID 1813. Additionally, a Grand Jury Subpoena revealed the account had been accessed from IP addresses that resolved to South Milwaukee, the general location of DAIS's

residence. After a review of IP login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

l. 100004739910411: In or about January 2018, the FBI determined that Facebook UID 0411 was in the name of HE and was being accessed from the same device that had accessed UID 1813. Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins for this account resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. After a review of the IP address login history, I assess DAIS hacked the account in approximately December 2017, and therefore the requested search is from December 1, 2017, to the present.

m. 100003449454063: On or about January 23, 2018, the FBI conducted an open source search of DAIS's alias, HE, and identified Facebook UID ending in 4063. The account had the same distinct profile picture known to be used by DAIS. Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. As discussed above, on or about February 7, 2018, information provided by Facebook pursuant to 18 U.S.C. § 2702, identified a Facebook user (referred to here as OG) who was planning a potential ISIS attack and had been communicating with DAIS (using Facebook UID 4063) about the attack.. In addition, Facebook UID 4063 was previously used by a female (Victim No. 2) whose profile stated she had studied at a University in Carabobo, Venezuela. I assess DAIS hacked the account in approximately January 2018, and therefore the requested search is from January 1, 2018, to the present.

n. 100002880451310: On or about January 30, 2018, the FBI conducted an open source search of HE (written in English) and identified Facebook UID ending in 1310. The account had the same distinct profile picture as other accounts used by DAIS. After a review of

the IP address login history, I assess DAIS hacked the account in or about January 2018, and therefore the requested search is from January 1, 2018, to the present.

o. 100000330381596: On or about February 5, 2018, the FBI conducted an open source search of HE (written in Arabic) and identified Facebook UID ending in 1596. The account had the same distinct profile picture used by DAIS's other hacked accounts. Additionally, a Grand Jury Subpoena revealed the account had been accessed from IP addresses that resolved to South Milwaukee, the general location of DAIS's residence. After a review of the IP address login history, I assess DAIS hacked the account in approximately December 2017, therefore the requested search is from December 1, 2017, to the present.

p. 100003893321780: On or about February 6, 2018, the FBI conducted an open source search of HE (written in Arabic) and identified Facebook UID 1780. The account had the same distinct profile picture used by DAIS's other hacked accounts. Additionally, a Grand Jury Subpoena revealed the account was accessed primarily through a VPN preventing location detection. The profile indicates the original user was a female (Victim No. 3) from Caxabobo, Venezuela. I assess the account was hacked by DAIS on or about February 1, 2018, when the cover photograph was changed to DAIS's distinct photo and the language changed to Arabic, and therefore the requested search is from February 1, 2018, to the present.

q. 100003310066527: On or about February 15, 2018, the UCE searched for HE's new Facebook account and found UID 6527. Facebook UID 6527 had the same name (HE) and distinct profile picture used by DAIS. The UCE sent a friend request to HE's account and she accepted the request. The UCE asked HE for additional social media accounts that DAIS may have to help stay connected. On or about February 20, 2018, HE provided the UCE with a link to her social media channel named "Khilafah Ray, Public Channel." Previous investigation had

determined this was a site for ISIS propaganda, links to their publications and official statement, and a number of very graphic pictures depicting dead ISIS fighters, dead Kurdish and regime soldiers, beheadings, ISIS battlefronts and pictures of news articles related to ISIS attacks in Europe and elsewhere. In addition, Facebook UID 6527 appeared to have been hacked and taken over by DAIS from a presumed non-U.S. person, as a screenshot taken by the UCE indicates that the original owner (Victim No. 4) studied at DeuCalleqero. On or about February 15, 2018, the UCE noticed DAIS's Facebook friends were advertising UID 6527 as HE's new account. Accordingly, I assess that the account was hacked and taken over by DAIS in or about February 2018, and therefore the requested search is from February 1, 2018, to the present.

r. 100003105302942: On or about March 2, 2018, the UCE searched for HE's new Facebook account and found UID 2942. The account had the same name (HE) and distinct profile picture used by DAIS. The UCE sent a friend request to HE's account and she accepted the request. On or about February 24, 2018, DAIS posted a link to a social media channel entitled, "Khilafah Ray for Supporters Group." The OCE visited the channel on February 26, 2018, and noted that the page had multiple voice messages posted by DAIS's social media account @ISWarrior and they consisted of Jihadi songs and speeches by ISIS leaders. One of the messages encouraged ISIS supporters who cannot travel to ISIS-controlled areas to conduct terrorist attacks in the countries where they reside. I assess this to be another hacked account of a presumed non-U.S. person, as the account states the previous user is from Venezuela therefore the requested search is from February 1, 2018, to the present.

s. 100004455614176: On or about March 18, 2018, the FBI searched using the hashtag "#HE" since DAIS frequently signed her wall posts with "#HE" in Arabic. I searched within Facebook for "#HE" and found a wall post tied to Facebook UID 4176 written in Arabic.

The account had the same distinct profile picture used by DAIS. The FBI notes the last publicly-available post was in approximately July 2017. I assess that the account was hacked and taken over by DAIS in or about July 2017, and therefore the requested search is from July 1, 2017, to the present.

t. 100002393547312: On or about March 23, 2018, the UCE searched for HE's new Facebook account and found UID 7312. The account had the same name (HE) and distinct profile picture used by DAIS. The UCE sent a friend request to UID 7312, and she accepted the request. The UCE then sent a private message, welcoming DAIS back. I assess that the account was hacked and taken over by DAIS in or about March 2018, based on the fact that the account still had pictures from the previous user before that time, and therefore the requested search is from March 1, 2018, to the present.

u. 100006207193027: On or about April 3, 2018, the UCE searched for DAIS's new Facebook account and found UID 3027. The account had the same name (HE) and distinct profile picture used by DAIS. The UCE sent a friend request to UID 3027, and the account user accepted the request. The UCE sent a private message to DAIS reminding her to send an email with instruction on how to make the meal (reference to Ricin poison). The UCE also noted that, on or about April 1, 2018, DAIS had posted on the Facebook page for UID 3027 the following message: "This account has been seized from a Nasraniyah (derogatory word for Christian) Lebanese infidel female. I did not unfriend all of her friends, perhaps they will be guided [to the truth]." Based on the above, I assess that this account was hacked and taken over by DAIS in or about April 2018, and therefore the requested search is from April 1, 2018, to the present.

v. 100002721214567: On or about March 20, 2018, the UCE searched for Facebook accounts with the name HE and found UID 4567. The account had the same name and distinct

profile picture used by DAIS. The UCE sent a friend request to UID 4567, and the account user accepted the request. The UCE then sent a private message and engaged the user in a conversation inquiring as to why she had not yet responded to his/her email. The user (believed to be DAIS) stated that she had sent the email right before deleting everything from her mobile phone. I assess that the account was hacked and taken over by DAIS in or about March 2018 based on the change of the profile picture of the account to the distinct profile picture from her other hacked Facebook accounts, and therefore the requested search is from March 1, 2018, to the present.

w. 100011611800178: On or about April 8, 2018, the FBI searched the alias HE and identified Facebook UID 0178. The account had the same distinct profile picture used by DAIS. I assess that the account was hacked and taken over by DAIS in or about April 2018, which is when the new profile picture was changed, and therefore the requested search is from April 1, 2018, to the present.

x. 100007837176059: On or about April 11, 2018, the UCE searched for Facebook accounts in the name of HE and found UID 6059. The account had the same name (HE) and distinct profile picture used by DAIS. The UCE sent a friend request to UID 6059, and the account user accepted the request. As stated above, on or about April 22, 2018, DAIS posted a link to a speech by Abu Hasan Al-Muhajir (Al-Muhajir) to the wall of Facebook UID 6059. According to open sources, AL-Muhajir is an ISIS official spokesman and his speech had been released on or about April 22, 2018, by the ISIS's media arm, the AL-Furqan Foundation. DAIS described the speech as inciting and inspiring, and reflected the true wisdom of ISIS leadership. Based on when the profile picture was changed from the original user to DAIS's distinct profile

picture, I assess that the account was hacked and taken over by DAIS in or about April 2018, and therefore the requested search is from April 1, 2018, to the present.

y. 100003229702265: On or about April 16, 2018, the FBI conducted an open source search of variations of HE and identified Facebook UID 2265. The account had the same name and same distinct profile picture used by DAIS. On or about April 11, 2018, the UCE sent a friend request to UID 2265, and the account user accepted the request. Based on when the profile picture was changed from the original user to DAIS's distinct profile picture, I assess DAIS hacked the account in or about April 2018, and therefore the requested search is from April 1, 2018, to the present.

z. 100004452642186: On or about May 3, 2018, the UCE searched for Facebook accounts with the name HE and found UID 2186. The UCE had noted another friend had advertised HE's Facebook account by announcing "Peace and Allah's mercy and blessings upon you: Your sister HE is tired of being suspended, she is one of the biggest supporters of the Islamic State. Please honor her by adding and supporting her here, and may Allah reward you with goodness." The account had the same distinct profile picture used by DAIS. The UCE sent a friend request to UID 2186, and the account user accepted the request. Based on when the profile picture was changed from the original user to DAIS's distinct profile picture, I assess that the account was hacked and taken over by DAIS in or about May 2018, and therefore the requested search is from May 1, 2018, to the present.

aa. 100004693445122: On or about May 11, 2018, pursuant to 18 U.S.C. § 2702, the FBI received the contents of Facebook account UID 5122. The account name was HE, DAIS's alias, and it had the same distinct profile picture. On or about April 17, 2018, an individual (AM) asked DAIS if they can be friends. DAIS responded saying "Listen, I am a member of ISIS.

Getting to know others will subject me to be slaughtered." When asked where she is from, DAIS stated, "I am in ISIS. The lands of ISIS." AM said he was from Egypt. The two discussed possible ways to enter Syria, where DAIS said she was located. DAIS told AM he would have to be smuggled in and pay a sum to the "Awakenings" or he would be imprisoned. He would also have to register as a fighter with ISIS. AM responded, "That is my wish; to be a jihadist." Additionally, a Grand Jury Subpoena revealed that some of the IP addresses for log-ins resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. Based on when the profile picture was changed from the original user to DAIS's distinct profile picture, I assess DAIS hacked the account in approximately April 2018, and therefore the requested search is from April 1, 2018, to the present.

bb. 1756849699: On or about June 5, 2018, the UCE searched for Facebook accounts with the name HE and found UID 9699. The account had the same distinct profile picture used by DAIS. The UCE sent a friend request to UID 9699, and the account user accepted the request. On June 5, 2018, the UCE noted that HE posted a video promoting her social media channels called "Al-Khilafah Ray." HE said her channels covered the following topics: publications, public channel, A'maq (the FBI notes this is a pro-ISIS news agency), Lone Wolves, Audio (voice messages). I assess that the account was hacked and taken over by DAIS in or about June 2018, and therefore the requested search is from June 1, 2018, to the present.

INFORMATION ABOUT FACEBOOK

42. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news,

photographs, videos, and other information with other Facebook users, and sometimes with the general public.

43. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

44. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

45. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

46. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

47. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos associated with a user's account will include all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

48. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages

through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

49. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

50. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

51. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

52. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

53. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

54. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which

are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

55. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

56. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

57. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and/or administrator, as well as a PDF of the current status of the group profile page.

58. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

59. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

60. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

61. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

62. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information

(including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

63. Based on the forgoing, I request that the Court issue the proposed search warrant.

64. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Eastern District of Wisconsin has jurisdiction over the offense being investigated." 18 U.S.C. § 2339(b).

65. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

1. This warrant applies the full member list for the Facebook UIDs: 100018358660648, 100015538297029, 100003394781813, 100002111932375, 1202263650, 100006301360001, 708785463, 100003682534004, 100001337974954, 100002115677945, 100004689817817, 100004739910411, 100003449454063, 100002880451310, 100000330381596, 100003893321780, 100003310066527, 100003105302942, 100004455614176, 100002393547312, 100006207193027, 100002721214567, 100011611800178, 100007837176059, 100003229702265, 100004452642186, 100004693445122, and 1756849699, as well as available information on the group's administrator(s) stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook, Inc.:

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A, **and consistent with the date ranges listed in the attached chart**:

(a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which

the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(l) All information about the user's access and use of Facebook Marketplace;

(m) The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);

(n) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(o) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Date Ranges for Search of User IDs:

Facebook User ID	Date Range of Search
100018358660648	March 1, 2017, to present
100015538297029	January 1, 2018, to present
100003394781813	December 1, 2017, to present
100002111932375	December 1, 2017, to present
1202263650	December 1, 2017, to present
100006301360001	December 1, 2017, to present
708785463	December 1, 2017, to present
100003682534004	December 1, 2017, to present
100001337974954	December 1, 2017, to present
100002115677945	December 1, 2017, to present
100004689817817	December 1, 2017, to present
100004739910411	December 1, 2017, to present
100003449454063	January 1, 2018, to present
100002880451310	January 1, 2018, to present
100000330381596	December 1, 2017, to present
100003893321780	February 1, 2018, to present
100003310066527	February 1, 2018, to present
100003105302942	March 1, 2018, to present
100004455614176	July 1, 2017, to present
100002393547312	March 1, 2018, to present
100006207193027	April 1, 2018, to present
100002721214567	March 1, 2018, to present
100011611800178	April 1, 2018, to present
100007837176059	April 1, 2018, to present
100003229702265	April 1, 2018, to present
100004452642186	May 1, 2018, to present
100004693445122	April 1, 2018, to present
1756849699	June 1, 2018, to present

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2339(b) involving DAIS since March 1, 2017, including, for each user ID identified on Attachment A, information pertaining to the following matters:

a. Any information in any form that is related to terrorism or a threat the national security of the United States;

b. Evidence of loyalties to a foreign power;

c. Weapons, ammunition, tactical equipment, tactical or camouflage clothing, explosives, explosives devices, explosive precursor chemicals, incendiaries; incendiary devices, incendiary chemicals or precursor chemicals and any other hazardous devices or substances deemed relevant to the investigation;

d. Flags, banners, patches, specifically designed clothing that depicts the symbol of a terrorist groups or terrorist movements;

e. Forms of identification, journals, and diaries;

f. Travel documents and indicia of travel overseas and domestically, including airline tickets, passports, visas, hotel records, and travel itineraries;

g. Calendars, time schedules, address books, and contact list information;

h. Financial information to include all financial institution records, checks, credit or debit cards, automated teller machine cards, public benefit program cards, account information, other financial records, financial instruments and moneys;

i. Money orders, wire transfers, cashier's check receipts, bank statements, passbooks, checkbooks, and check registers pertaining to travel overseas, the Islamic State of Iraq and al-Sham (ISIS), terrorist or military-like activities, or violent acts;

j. Cellular telephones, smart telephones, computers, electronic data storage devices or media, associated electronic accessories;

k. Any information that could be determined to passwords, personal identification numbers (PINs), or other information necessary to encrypt or decrypt information;

l. Evidence of geographical location of the user of the identified account at times relevant to the investigation; Global Positioning System (GPS) information and mapping history from any account;

m. Secure storage facilities for financial instruments, passports, visas, and identification documents, including safe deposit boxes;

n. Persons associated with ISIS or involved in terrorist or military-like activities or violent acts overseas or in the United States, including their identities and location and contact information;

o. Organizations whose purpose, primary or ancillary, is raising, collecting, organizing, distributing, or facilitating funds, goods, personnel, or services for training and fighting overseas or in the United States and *not* in conjunction with the U.S. armed forces;

p. Instructions, in any form, relating to explosives, biological weapons, terrorist attacks, or the hacking and other unauthorized use of computers and email and social media accounts; and

q. Hacking or the unauthorized use of any computer or email or social media account.

r. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

s. Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

t. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and

u. The identity of the person(s) who communicated with the user ID about matters relating to providing material support to terrorist organizations, including records that help reveal their whereabouts.