UNITED STATES DISTRICT COURT

for the

Southern District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Apple, Inc., One Apple Park Way, Cupertino, CA 95014, host of 760-889-3948, Robert.nordicalservices@gmail.com, DSID: 421041178 (**Subject Account**)	)	Case No. 25mj6848

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

See Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Sec. 1366	Destruction of an Energy Facility Conspiracy to Destroy an Energy Facility

The application is based on these facts:

See Attached Affidavit, incorporated herein by reference.

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

Nicholas T. Cutrona
Applicant's signature

Nicholas Cutrona, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: December 9, 2025

Michelle M. Pettit
Judge's signature

City and state: San Diego, California

Hon. Michelle M. Pettit, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID,

760-889-3948,
Apple ID: Robert.nordicalservices@gmail.com,
DSID (Apple Account identifying number): 421041178,
used by Robert Skyler HARRY (the "**Subject Account**"),

that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Service of Warrant

The officer executing the warrant shall permit Apple Inc., as the custodian of the computer files described in Section II below, to locate the files and copy them onto removable electronic storage media and deliver the same to the officer.

II. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International

Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs

associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps to include date and time stamps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

III. Information to be Seized by the Government

All information described above in Section II that constitutes evidence of violations of 18 U.S.C. § 1366 Destruction of an Energy Facility and conspiracy do the same (the "subject offenses"); limited to the period of December 29, 2023, [30 days before the shooting] up to and including February 27, 2024 [30 days after the shooting], and to the seizure of evidence:

a. tending to indicate efforts to destroy an energy facility;

b. tending to identify accounts, facilities, storage devices, and/or services–such as email addresses, IP addresses, and telephone numbers–used to facilitate the destruction of an energy facility;

c. tending to identify co-conspirators, criminal associates, or others involved in destroying an energy facility;

d. tending to identify travel to or presence at the destroyed energy facility;

e. tending to identify the user of, or persons with control over or access to, the Subject Account; and/or

f. tending to place in context, identify the creator or recipient of, or establish the time of creation or receipt of communications, records, or data involved in the activities described above.

All of the above constituting evidence of a violation of the subject offenses.

AFFIDAVIT IN SUPPORT OF

APPLICATION FOR SEARCH WARRANT

I, Nicholas Cutrona, Special Agent, Federal Bureau of Investigation ("FBI"), being duly sworn, hereby state as follows:

A. INTRODUCTION

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with an iCloud account connected to the following Apple ID:

760-889-3948,
Apple ID: Robert.nordicalservices@gmail.com,
DSID (Apple Account identifying number): 421041178,
used by Robert Skyler HARRY (the **Subject Account**),

for items which constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1366, Destruction of an Energy Facility and conspiracy do the same (the "subject offenses"); as more fully described in Attachment B.

2. For the reasons set forth below, I believe there is probable cause for the requested warrants for the **Subject Account**, the contents for which are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Apple Park Way, Cupertino, California 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B, which are attached hereto incorporated herein.

B. TRAINING & EXPERIENCE

3. I am a Special Agent with the FBI and have been so employed since June 2023. I am assigned to the Imperial County Resident Agency of the San Diego Field Office where I investigate federal crimes including, inter alia, fraud, public corruption, kidnappings, bank robberies, extortions, assaults on federal officers, organized crime, drug

offenses, violent crime, and crimes against children. I am an investigative or law enforcement officer within Title 18, United States Code, Section 2510(7), that is, an officer of the United States, empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18 of the United States Code.

4. Prior to becoming a Special Agent, I completed approximately eighteen weeks of training at the FBI Academy in Quantico, Virginia. During the training, I received instruction in a variety of investigative techniques commonly used in support of a wide range of the FBI's investigative priorities. The training included instruction regarding the use of confidential human sources; electronic and physical surveillance techniques, including cellular telephone tracking; law enforcement tactics; search and seizure laws and techniques; interviewing strategies and skills; and a variety of other subjects.

Scope of Search

5. Based upon my training, experience, and consultations with law enforcement officers including officers experienced in investigations relating to the destruction of energy facilities, and all the facts and opinions set forth in this affidavit, I am aware that cellular telephones (including their SIM card(s)) can and often do contain electronic evidence, including, for example, phone logs and contacts, voice and text communications, and data, such as emails, text messages, chats and chat logs from various third-party applications, photographs, audio files, videos, and location data. This information can be stored within disks, memory cards, deleted data, remnant data, slack space, and temporary or permanent files contained on or in the cellular telephone. Additionally, this same information is generally backed up by Apple and maintained in the cloud, called iCloud. Specifically, searches of cellular telephones of individuals suspected of destroying and/or conspiring to destroy energy facilities, and their back-up data stored in Apple's cloud, specifically the **Subject Account**, may yield evidence:

a. tending to indicate efforts to destroy an energy facility;

b. tending to identify accounts, facilities, storage devices, and/or services–such as email addresses, IP addresses, and telephone numbers–used to facilitate the destruction of an energy facility;

c. tending to identify co-conspirators, criminal associates, or others involved in destroying an energy facility;

d. tending to identify travel to or presence at the destroyed energy facility;

e. tending to identify the user of, or persons with control over or access to, the **Subject Account**; and/or

f. tending to place in context, identify the creator or recipient of, or establish the time of creation or receipt of communications, records, or data involved in the activities described above.

6. I am also familiar with Apple products and services because of my experience, training, and conversations with other law enforcement officers.

7. The facts and conclusions set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, my review of documents and records related to this investigation, communications with others who have personal knowledge of the events, details, and circumstances described herein, and information gained through my training, experience, and communications with colleagues. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. Dates and times are approximate.

D. FACTS IN SUPPORT OF PROBABLE CAUSE

Background of 2024 Shooting in Ocotillo Wells, California

8. Since early 2024, the FBI has been investigating a possible shooting of a power substation within the Southern District of California. At approximately 1:13 a.m. on January 28, 2024, approximately $200,000 of damage was caused to the Ocotillo Wells Substation in Ocotillo Wells, California, leaving roughly 250 people without electricity for

eight to twelve hours. The Ocotillo Wells Substation is serviced by the Imperial Irrigation District (IID).

9. Later that day, an IID employee (Employee-1) was alerted that the Ocotillo Wells Substation had lost power and thereafter inspected the Substation. After observing damage to the transformer and fire suppression system, IID personnel contacted a claims investigator in IID's Security, Claims, and Investigations Department (Inspector-1) and the San Diego County Sheriff's Office (SDSO) to file a report. Specifically, IID personnel noticed unnatural holes, resembling bullet holes, in the transformer and fire suppression system, located approximately 10 feet above ground.

10. Employee-1 and a SDSO deputy subsequently followed two all-terrain vehicle (ATV) tracks that were likely ingress and egress routes to and from Split Mountain Road in Borrego Springs, California, located approximately one mile from the Ocotillo Wells Substation. Employee-1 also observed that, prior to the shooting damage, it had recently rained in the area and that the ATV tracks were the only tracks in the area following the shooting and rain.[1]

11. Later that same day, Inspector-1 also inspected the area surrounding the Substation. On the north side of the facility, Inspector-1 found several empty rifle casings and one live 7.62mm-caliber rifle round. This was near a commonly used ATV trail that runs along the Substation's power lines and also where Employee-1 and the SDSO deputy observed fresh ATV tracks. Additionally, Inspector-1 also found an envelope on the ground near the substation; Inspector-I picked up the envelope and placed the rifle casings and live round within the same envelope.

//

//

//

[1] During January each year, this area is commonly used for off-roading sports and activities; visitors also typically park camping trailers for temporary housing. Investigators, however, did not observe temporary housing structures or trailers in the area at the time of the shooting.

Identification of HARRY via Physical Evidence, Verizon Wireless Records, and Records Checks

12. The envelope[2] that Inspector-1 found near the substation was addressed to "Robert Skyler Harry" and featured an address in Valley Center, California. California DMV records confirm that the envelope's address has previously been associated with HARRY, though a more-current address was revealed through Verizon's disclosure of HARRY's subscriber information, discussed *infra*.

13. On June 28, 2024, United States Magistrate Judge Michelle M. Pettit signed an order directing Verizon, pursuant to Title 18, United States Code, Sections 2703(c), (d), to disclose records identifying any wireless telephone call (including the phone numbers and subscriber information of the sending and receiving phones) originating, terminating, or conducted through cell sites providing coverage to the Substation in Imperial County, California, between 12:00 a.m. and 4:00 a.m. on January 28, 2024.

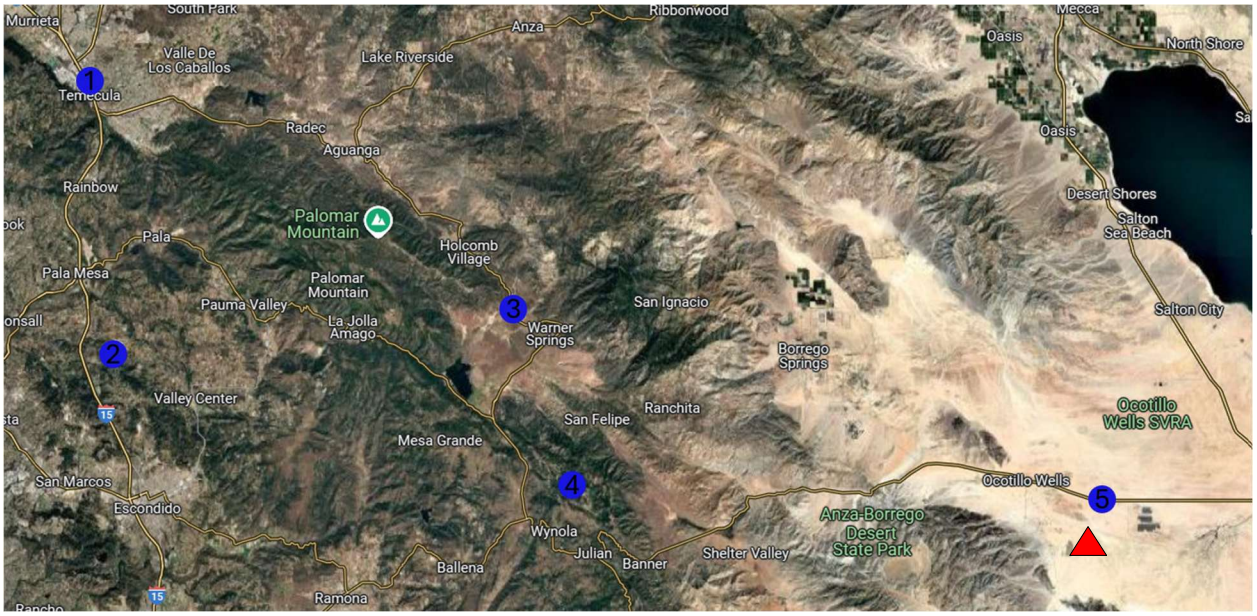
14. On August 12, 2024, in accordance with Judge Pettit's order, Verizon produced records showing several cellular devices making and receiving phone calls between 12:24 a.m. and 3:04 a.m. on January 28, 2024. Specifically, the phone number (760) 889-3948 received a five-minute-long phone call at approximately 3:00 p.m. on January 27, 2024 (*i.e.*, approximately ten hours prior to the shooting) from (760) 755-9892, or the number attributed to JORGENSEN, discussed further in Section C *infra*.

15. On January 28, 2024 (*i.e.*, the day of the shooting), (760) 889-3948 was shown making and receiving several phone calls between 1:02 a.m. and 1:12 a.m. Though impossible to pinpoint exact geographical coordinates, (760) 889-3948 was active that early morning in a designated area between the cell tower and the Substation. According to Verizon's open-source records, (760) 889-3948 is subscribed to HARRY, matching the name of the addressed envelope found at the scene.

---

[2] The envelope has a partial fingerprint linked to Inspector-1. After a fingerprint analysis, HARRY's prints were excluded, as were the prints of his suspected associate, JORGENSEN, discussed in Section C, *infra*.

16. Between 3:00 p.m. on January 27, 2024, and 2:19 a.m. on January 28, 2024, (760) 889-3948 pinged from several cellular towers along highways 15, 76, 79, and 78 from Temecula, California to Borrego Springs, California,[3] outlined in the map and coordinates *infra*. The red triangle in the map below is the approximate location of the Substation.



Plot on Map	Time (PST)	Latitude	Longitude
1	3:00 pm	33.512826	-117.151629
2	7:39 pm	33.260847	-117.122183
3	9:39 pm	33.304702	-116.686489
4	10:49 pm	33.159269	-116.615602
5	2:19 am	33.125328	-116.043408

17. Between December 2024 and April 2025, investigators conducted physical surveillance, records checks, and viewed historical cell site data relating to HARRY and (760) 889-3948, identifying HARRY's residence as 11055 B Mystery Mountain Road,

[3] As discussed in Section C *infra*, during the same time period, (760) 755-9892 also pinged from the cellular tower located in Borrego Springs, or approximately 3.4 miles from the Substation.

Valley Center, California 92082.[4] This address is approximately 77 miles west of the Substation. HARRY's mailing address was changed to the above address on March 20, 2025, including on HARRY's California driver's license.[5] During investigators' physical surveillance of HARRY in April 2025, vehicles registered to HARRY were also observed at this address.

18. Additionally, according to the California Department of Justice Automated Firearms System (CDOJAFS), HARRY has several registered firearms, including a PAP M92 firearm, manufactured to shoot 7.62mm-caliber ammunition, matching the live round located at the Substation's scene. Moreover, according to the California DMV, HARRY owns an off-roading dirt bike and several pickup trucks.

Identification of JORGENSEN via Physical Evidence, T-Mobile Records, and Records Checks

19. On June 24, 2024, United States Magistrate Judge David D. Leshner signed a search and seizure warrant authorizing the search of GPS, Wi-Fi, or Bluetooth-sourced location-history data generated from anonymized mobile devices (e.g., cellphones) within a geographical region surrounding the Substation on January 28, 2024, as well as identifying information for Google accounts associated with the responsive location history data set.[6] The results yielded one reverse location obfuscated identification[7] within the

[4] Prior to this address, HARRY had two prior addresses, both in Valley Center, including: (a) 30726 Roadrunner Ridge, Valley Center, CA 92082; and (b) 12466 Hillpoint Court, Valley Center, CA 92082. However, investigators did not see HARRY or his registered vehicles at either of those addresses during physical surveillance. During agents' investigation, historical cell site data underlined that HARRY remained within Valley Center because (760) 889-3948 continued to ping from cellular towers within Valley Center.

[5] On this date, HARRY's mailing address was changed to the above and backdated for the time period of August 30, 2024 to January 1, 2025.

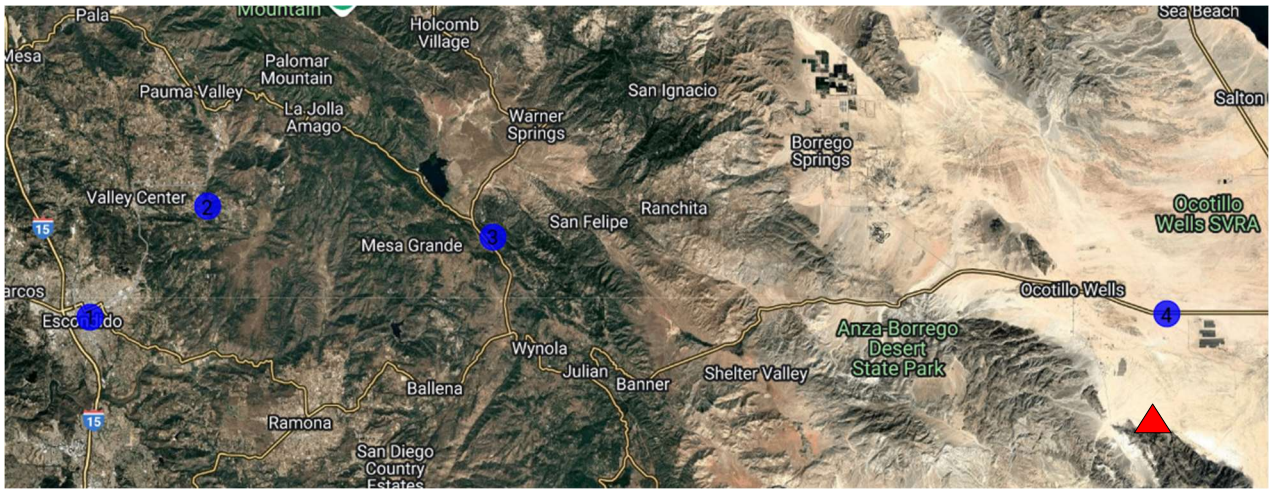
[6] Whether (760) 755-9892 and/or JORGENSEN has a Google account is presently unknown.

[7] Used in geofence search warrants, a reverse location obfuscated identification is an anonymized identifier of devices present in a designated area at a specific time.

temporal and geographical search parameters, identifying the phone number (760) 755-9892 and T-Mobile subscriber, JORGENSEN.

20. On August 30, 2024, United States Magistrate Judge David D. Leshner signed an order directing T-Mobile to provide historical records, data, and information for (760) 755-9892. In accordance with the order, T-Mobile produced results demonstrating that (760) 755-9892 (*i.e.*, associated with JORGENSEN) called (760) 889-3948 (*i.e.*, associated with HARRY) at approximately 3:00 p.m. on January 27, 2024 (*i.e.*, approximately ten hours prior to the shooting) for around five minutes.

21. Between 5:00 p.m. and 8:00 p.m. on January 27, 2024, (760) 755-9892 pinged from several cellular towers along highways S6, 79, and 78 from Escondido, California, to Borrego Springs, California (*i.e.*, approximately 3.4 miles from the Substation),[8] outlined in the map and coordinates *infra*. The red triangle in the map below is the approximate location of the Substation.



Plot on Map	Time (PST)	Latitude	Longitude
1	5:23 pm	33.11296	-117.078548
2	6:43 pm	33.210589	-116.965703

[8] As discussed in Section B *supra*, (760) 889-3948 also pinged from the cellular tower located in Borrego Springs, approximately 3.4 miles from the Substation, during the relevant time period.

3	7:18 pm	33.186835	-116.691752
4	8:00 pm	33.125316	-116.043383

22. (760) 755-9892 continued to ping from the Borrego Springs cellular tower until approximately 8:30 p.m. on January 27, 2024. At approximately 4:00 a.m. on January 28, 2024, (760) 755-9892 attempted to make an outgoing call to its voicemail but was unsuccessful and received a "Call Forwarding on Not Reachable" error message. This indicates that (760) 755-9892 was still in the vicinity of the Borrego Springs cellular tower when the electricity was out following the shooting.

23. Between December 2024 and January 2025, investigators conducted physical surveillance and records checks relating to JORGENSEN, identifying JORGENSEN's residence as 11315 Arirang Lane, Escondido, California 92026. This address is approximately 80 miles west of the Substation. The address above is also JORGENSEN's mailing address as of October 3, 2023, and on JORGENSEN's California driver's license. Multiple vehicles registered to JORGENSEN were observed at this address. California DMV records show that JORGENSEN owns two off-roading vehicles: a Yamaha ATV and a Polaris RZR; a pickup truck; and a trailer capable of towing the off-road vehicles.

24. Additionally, according to records obtained from CDOJAFS, JORGENSEN has several firearms registered in California, with most firearms chambered in .308-Winchester ammunition, though also able to shoot 7.62mm-caliber ammunition as well. On February 22, 2024, or less than one month after January 28, 2024 (*i.e.*, when the shooting at the Substation occurred), JORGENSEN purchased an Aero Precision M5 rifle, chambered with .308 Winchester-brand and 7.62-mm caliber ammunition rounds.

Additional Connections between HARRY and JORGENSEN

25. Moreover, public website searches revealed that HARRY and JORGENSEN are friends[9] on the social media platform, Facebook. Between 2011 and 2014, JORGENSEN posted multiple photos of firearms. A photo posted on October 28, 2011,

[9] Based on my experience, two become Facebook friends once one person sends a friendship request and the other person accepts the request.

captioned "the arsenal", contained two shotguns and two rifles. None of the firearms in the 2011 photo are registered to JORGENSEN in California, suggesting that JORGENSEN has previously possessed unregistered firearms. In a four-month span in 2013, HARRY also posted multiple photos of firearms. A photo posted on June 8, 2013, captioned "Even pregnant woman can shoot an AK!", contained a woman firing an Avtomat-Kalashnikova-style rifle similar in appearance to the PAP M92 firearm registered to HARRY.

Residential Search Warrants for HARRY and JORGENSEN

26. On May 23, 2025, United States Magistrate Judge Valerie E. Torres authorized residential search warrants for: (a) HARRY's residence in Valley Center, California; and (b) JORGENSEN's residence in Escondido, California. Judge Torres also authorized searches for the persons of HARRY and JORGENSEN. On May 28, 2025, law enforcement agents executed residential search warrants on addresses for HARRY and JORGENSEN.

27. After executing the residential search warrant at HARRY's residence in Valley Center, California, agents learned that the day prior (*i.e.*, May 27, 2025), HARRY had surrendered several of his firearms to SDSO due to his ongoing state criminal case.[10] When later contacted by agents, SDSO confirmed that they received a .22-mm-caliber rifle and handguns, none of which appeared modified to shoot 7.62-mm-caliber rounds, as discovered at the Substation scene. Ultimately, following execution of the residential search warrant on May 28, 2025, no firearms were seized at HARRY's residence in Valley Center.

//

//

[10] On April 1, 2025, HARRY is alleged to have threatened a delivery driver and brandished a firearm. As a condition of his pretrial release, HARRY was ordered to surrender his weapons. HARRY did so the day prior to the execution of the residential warrant in his federal investigation. None of the weapons that HARRY surrendered are reportedly capable of shooting 7.62-mm-caliber ammunition. HARRY's state criminal case is ongoing.

28. Agents, however, seized HARRY's cellphone from the floor of his residence, pictured below:

29. Following advisal of his *Miranda* rights, HARRY was interviewed by law enforcement agents. HARRY stated to agents that he did not recall being out near the Ocotillo Wells Substation on January 28, 2024, given that it was so long ago. HARRY also reported his surrendering of firearms to California pretrial services the day prior. HARRY added that he separately possesses firearms in Idaho. HARRY stated his phone number is 760-889-3948 and his e-mail address is Robert.nordicalservices@gmail.com.

30. When shown the above pictured device, HARRY identified the cellphone as his. Following HARRY's interview, HARRY contacted investigating agents requesting that the phone be returned to him.

31. In a separate conversation with HARRY's partner at HARRY's residence, the partner stated to agents that she recalls being in the Ocotillo Wells Substation area during last year's riding season, which includes January 2024. The partner also confirmed the above pictured phone belonged to HARRY.

32. After executing the residential search warrant at JORGENSEN's address in Escondido, law enforcement agents seized one firearm, including an Aero Precision M5 Lower with serial number US342927. Of note, an Aero Precision Atlas R-One Upper with a Vortex Venom Scope was also seized; this, in short, is a firearm's barrel and the additional mechanisms necessary for a firearm to function. A user combines the "upper" and "lower" components, pictured below, to use the firearm. When combined, this firearm could shoot 7.62-mm-caliber ammunition. The "upper" and "lower" components were found adjacent in a bedroom's closet at JORGENSEN's residence.

33. Agents also seized one black PMAG magazine loaded with 7.62 x 51 ammunition (*i.e.*, the exact caliber of ammunition seized from the Substation shooting scene).

//

//

//

//

34. Agents also seized JORGENSEN's cellphone from his person (*i.e.*, Target Device 2), pictured below:

35. Following advisal of his Miranda rights, JORGENSEN was interviewed by law enforcement agents. JORGENSEN acknowledged that he was in the Ocotillo Wells area on January 28, 2024, together with HARRY,[11] but added that he does not know why (760) 755-9892 was in the geofence area near the Substation at that late hour because he would have been sleeping.

36. When shown the phone pictured above, JORGENSEN identified the cellphone as his and separately inputted his passcode into the phone. Following JORGENSEN's interview, JORGENSEN contacted investigating agents requesting the above pictured phone be returned to him.

37. In a separate conversation with JORGENSEN's spouse at JORGENSEN's residence, JORGENSEN's spouse confirmed that JORGENSEN was in the Ocotillo Wells area on January 28, 2024, but that JORGENSEN should have been asleep at that time. JORGENSEN's spouse added that HARRY was also with JORGENSEN on January 28,

[11] Though confirming that he knows HARRY, JORGENSEN caveated that HARRY does not typically go shooting with him and JORGENSEN's spouse.

2024. Both JORGENSEN and his spouse separately confirmed that "everyone" knows where the Ocotillo Wells substation is.

Search of HARRY's Seized Cell Phone

38. On June 27, 2025, United States Magistrate Judge Jill L. Burkhardt authorized the search of HARRY's black iPhone cellular phone. On September 25, 2025, an FBI Computer Forensic Analyst extracted data from HARRY's phone, which was reviewed by an FBI Intelligence Analyst on September 25, 2025. There were several images and videos captured around the January 28 offense date that displayed firearms including rifles that appear to chamber .762 ammunition, images of JORGENSEN shooting a rifle near railroad tracks believed to be in Ocotillo Wells,[12] and screenshots of social media posts about the January 28 substation power outage. When comparing text messages and call detail information between HARRY and JORGENSEN's phone, it is apparent that content is missing from HARRY's cellular extraction. Specifically, JORGENSEN's phone extraction showed a longer text message thread and call detail history between them than the minimal details in HARRY's phone extraction. The missing content is believed to be backed up to HARRY's Apple iCloud.

39. On October 8, 2025, I served a preservation request and a grand jury subpoena to Apple for subscriber information responsive to HARRY's phone number, 760-889-3948, and e-mail address, Robert.nordicalservices@gmail.com. On October 22, 2025, Apple provided a response to that confirmed iCloud data connected to HARRY's phone number, that his e-mail address is his Apple ID, and further providing DSID (Apple Account identifying number) 421041178.

40. Given the above facts and my experience and training, there is probable cause to believe that HARRY was using his cell phone to communicate with JORGENSEN to destroy an energy facility (and conspiracy to do the same) in violation of Title 18, United States Code, Section 1366. Based on my training and experience, it is also not unusual for individuals, such as HARRY or JORGENSEN, to attempt to minimize their involvement

[12] Jorgensen stated to agents that he shot firearms near railroad tracks in Ocotillo Wells.

in criminal activity, which both did during separate conversations with agents following execution of the residential search warrants.

C. BACKGROUND CONCERNING APPLE[13]

41. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

42. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and iCloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via iCloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and

[13] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

43. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address [often ending in @iCloud.com, @me.com, or @mac.com] or an email address associated with a third-party email provider [such as Gmail, Yahoo, or Hotmail]. The Apple ID can be used to access most Apple services

[including iCloud, iMessage, and FaceTime] only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

44. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

45. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

46. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which

is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through iCloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

47. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

48. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what,

why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

49. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the subject offenses. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the subject offenses.

50. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows Investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

51. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

52. Further, I know when a user has an Apple Watch with cellular and an activated cellular plan, the user can stay connected even when away from their iPhone. For all other models of Apple Watch, there are still things the user can do even when the user is away

from their iPhone and not connected to Wi-Fi.[14] When the iPhone is off or out of range, the Apple Watch can use a Wi-Fi network to send and receive data. The watch can also connect to a cellular network if it's a cellular model. If a user set up an Apple Watch for a family member, they can use a cellular or Wi-Fi connection with their watch. A Wi-Fi or cellular connection lets the Apple Watch do the following things, even if your iPhone isn't with you.[15]

53. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators [e.g. encrypted communication platforms]. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

54. I know, based on my training, experience, discussions with other law enforcement officers, and background information related to Apple provided here, that an Apple ID is required to access and use the above captioned features on an Apple product. I know Defendant's cellular telephone was an Apple product based on physical markings including the Apple logo, which is an apple with a bite taken out of the right side, and the HARRY'S cell phone extraction confirming the phone as an Apple device. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience,

---

[14] The information was found on website: https://support.apple.com/guide/watch/useapple-watch-without-its-paired-iphone-apd0443fb403/watchos. According to Apple "Apple Watch has a built-in GPS that allows you to get more accurate distance and speed information during an outdoor workout without your paired iPhone. Apple Watch Series 3, Apple Watch Series 4, and Apple Watch Series 5 also have a built-in barometric altimeter to get more accurate elevation gain/descent information. The always-on altimeter in Apple Watch SE, Apple Watch Series 6, and Apple Watch Series 7 is even more accurate, showing your current elevation in real time."

[15] The referenced information can be found on website: https://support.apple.com/enus/HT205547.

such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

Temporal Scope of the Requested Search

55. I know, based on my training and experience, including my experience within this case, that destroying an energy facility often involves continuing communication that transpires over the days, weeks, and months prior to the destruction event. That activity often continues throughout the life of the overall conspiracy, which is an ongoing series of events, that can often last for months or years.

56. Finally, given the facts of this affidavit, my understanding of how Apple accounts can be used in furtherance of the offenses as described herein, and my awareness that Apple accounts can retain information for extended periods of time, I submit that this Court should authorize a search of the **Subject Account** for the period starting on December 29, 2023, [30 days before the shooting] to February 27, 2024 [30 days after the shooting].

E. INFORMATION TO BE SEARCHED AND ITEMS TO BE SEIZED

57. 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 Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, Investigators or other federal agents and personnel will need to process the data into a format that may be reviewed. Investigators will then need to review the data to locate the items described in Section II of Attachment B. This process takes time. The personnel conducting the examinations into responsive data will **complete the analysis within 90 days** of the date the data is received from Apple, absent further application to this court.

//

//

F. CONCLUSION

58. Based on all of the facts and circumstances described above, there is probable cause to conclude that the **Subject Account** contains evidence of violations of the subject offenses and will contain electronic evidence of those violations, as more fully described in Attachment B.

59. **WHEREFORE**, I request that the court issue a warrant authorizing law enforcement agents and/or other federal and state law enforcement officers to seize and search the items described in Attachment A, and the seizure of items listed in the corresponding Attachment B.

Nicholas T. Cutrona
NICHOLAS CUTRONA
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 9th day of December, 2025.

Michelle M. Pettit
HON. MICHELLE M. PETTIT
United States Magistrate Judge