

UNITED STATES DISTRICT COURT

**SEALED**

unsealed on 8/3/2021, JMR

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)

Case No. 20MJ3733

Google LLC  
1600 Amphitheatre Parkway, Mountain View, CA 94043  
mayssawyer628@gmail.com

**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-2, 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-2, 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.

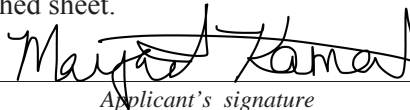
The search is related to a violation of:

Code Section	Offense Description
18, USC sec. 81	Arson within special maritime and territorial jurisdiction; Use of fire to damage
18, USC sec. 844(f)	federal property; False statement
18, USC sec. 1001	

The application is based on these facts:

See Attached Affidavit of Maya Kamat Special Agent NCIS, 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.

  
Applicant's signature

Special Agent Maya Kamat, NCIS  
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: 09/03/2020

  
Judge's signature

City and state: San Diego, California

Hon. William V. Gallo, U.S. Magistrate Judge  
Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS**

I, Maya Kamat, being duly sworn, declare and state:

**INTRODUCTION**

1. This affidavit is submitted in support of applications to search Internet Service Providers (ISPs) – Apple Inc., Google, LLC, and Yahoo! Inc. -- for records and data in and related to the following electronic accounts (collectively, “**Subject Accounts**”):

(a) iCloud account associated with mayssawyer628@yahoo.com (“**Subject Account-1**”);

(b) Google account associated with mayssawyer628@gmail.com (“**Subject Account-2**”);

(c) Yahoo account associated with mayssawyer628@yahoo.com (“**Subject Account-3**”);

(d) Yahoo account associated with maysryan980@yahoo.com (“**Subject Account-4**”); and

(e) Yahoo account associated with ryanmays628@yahoo.com (“**Subject Account- 5**”)

as more fully described in Attachments A-1, A-2, A-3, A-4, A-5 respectively, for items that constitute evidence of violations of 18 U.S.C. Sections 81, Arson within special maritime and territorial jurisdiction; 844(f), Use of fire to damage federal property; and 1001, False Statement (the “**Target Offenses**”), as more fully described in Attachments B-1, B-2, B-3, B-4, and B-5.

2. Based on the information outlined below, probable cause exists that evidence of the Target Offenses will be found by searching the **Subject Accounts**, the contents of which are stored at premises owned, maintained, controlled, or operated by Apple, Google, and Yahoo.

//

//

## EXPERIENCE AND TRAINING

1  
2 3. I am a Special Agent with the Naval Criminal Investigative Service (NCIS),  
3 San Diego, California. I have been assigned to NCIS in this capacity since January of  
4 2019. I am currently assigned to NCIS Resident Agency San Diego, CA. My duties as an  
5 NCIS Special Agent include, but are not limited to, investigating crimes committed by or  
6 against Navy or Marine Corps installations, aircraft, or vessels, investigating crimes  
7 involving Department of the Navy or Marine Corps military personnel or civilian  
8 employees. Prior to becoming an NCIS Special Agent, I obtained a Bachelors of Arts and  
9 Science in Criminal Justice, respectively, from Florida Gulf Coast University, where I  
10 graduated Summa Cum Laude. I worked as an intern for the United States Marshal's  
11 Service.

12 4. My formalized training includes successful completion of the Criminal  
13 Investigator Training Program (CITP) at the Federal Law Enforcement Training Center  
14 (FLETC), located in Glynco, Georgia. The CITP course includes intensive training on  
15 subjects such as interviewing, firearms, digital forensics, and tactical training, as well as  
16 extensive legal courses. I have also successfully completed the NCIS Special Agent Basic  
17 Training Program (SABTP), which is a 12-week course with curriculum specifically  
18 tailored to the unique challenges faced by NCIS. Such training included military law,  
19 death investigations, crime scene processing, intelligence, and narcotics investigations. I  
20 have apprehended military members. I have served Command Authorization's for Search  
21 and Seizure to search persons, vehicles, barrack's room, berthing areas, digital devices,  
22 medical records and the like. I have served search warrants for off base related searches.  
23 In my training and experience, it is commonly known that people use their cellular phone  
24 to research, store images, data, and text messages relating to elements of the crime. I have  
25 successfully worked criminal cases regarding, but not limited to: arson, domestic violence,  
26 communication of a threat, death, fraud, narcotics, prostitution, and sexual assaults.

27 //

28 //

1           5.     In addition to my training, I was a member of the NCIS Major Case Response  
2 Team (MCRT), and have participated in response to a significant amount of active crime  
3 scenes involving military members, many requiring processing of physical evidence in  
4 both sterile and contaminated scenes.

5           6.     I make this affidavit, in part, based on personal knowledge derived from  
6 my participation in this investigation and, in part, based upon information from: (a) oral  
7 and written reports about this investigation which I have reviewed; (b) physical  
8 surveillance conducted by NCIS personnel, which observations have been reported to  
9 me either directly or indirectly; and (c) statements of cooperating individuals.

10          7.     Except as otherwise noted, information set forth in this affidavit has either  
11 been observed or provided to me by law enforcement officers with whom I have spoken,  
12 who were involved in this investigation, or whose reports I have read and reviewed.  
13 Likewise, information resulting from surveillance, except where otherwise indicated,  
14 does not necessarily set forth my own observations but rather has been provided directly  
15 or indirectly by other NCIS personnel who conducted such surveillance.

16          8.     Because this affidavit is being submitted for the limited purpose of seeking  
17 the search warrant specified below, I have not set forth each and every fact learned  
18 during the course of the investigation. Rather, I have set forth only those facts that I  
19 believe are necessary to establish probable cause for the requested warrant.

20                   BACKGROUND ON APPLE, GOOGLE, AND YAHOO

21          9.     Apple Inc. (Apple) designs, develops, and sells consumer electronics,  
22 computer software, and online services. Apple products include the iPhone, iPad, and  
23 Mac personal computer. Apple's online services include iCloud, iMessage, and email.  
24 iCloud allows users to store and backup data from all Apple devices including text  
25 messages, contact lists, photos and videos, application data, emails, Apple wallet, and  
26 documents. As set forth below, I believe there is evidence of criminal activity contained  
27 within Apple associated with **Subject Account-1**.

1           10. Although most people think of Google, LLC, (Google) as specializing in  
2 Internet browsing and search technologies, Google is actually much larger than that. It  
3 provides Internet-related services and products, which also include online advertising  
4 technologies, email and file storage and collaboration, cloud computing, and software  
5 development tools and technologies. Google's services and products collect and store a  
6 vast amount of content and information for a user's account including but not limited to  
7 user account profile information, web browser and search activity data, email and voice  
8 communication data, file storage and collaboration data, and advertisement and analytics  
9 data. As set forth below, I believe there is evidence of criminal activity contained within  
10 Google associated with **Subject Account-2**.

11           11. Yahoo! Inc. (Yahoo), a wholly owned subsidiary of Verizon Communications,  
12 is an Internet company which, among other things, provides electronic communication  
13 services to subscribers. Yahoo's electronic mail service allows subscribers to  
14 communicate with other ISP subscribers through the Internet. Subscribers to Yahoo use  
15 unique screen names and/or email addresses during communications with others. The  
16 screen names and/or email addresses may or may not identify the real name of the person  
17 using a particular screen name or email account. As set for the below, I believe there is  
18 evidence of criminal activity contained with Yahoo associated with **Subject Account-3**,  
19 **Subject Account-4**, and **Subject Account-5**.

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

## PROBABLE CAUSE

*Fire on the USS Bonhomme Richard on July 12, 2020.*

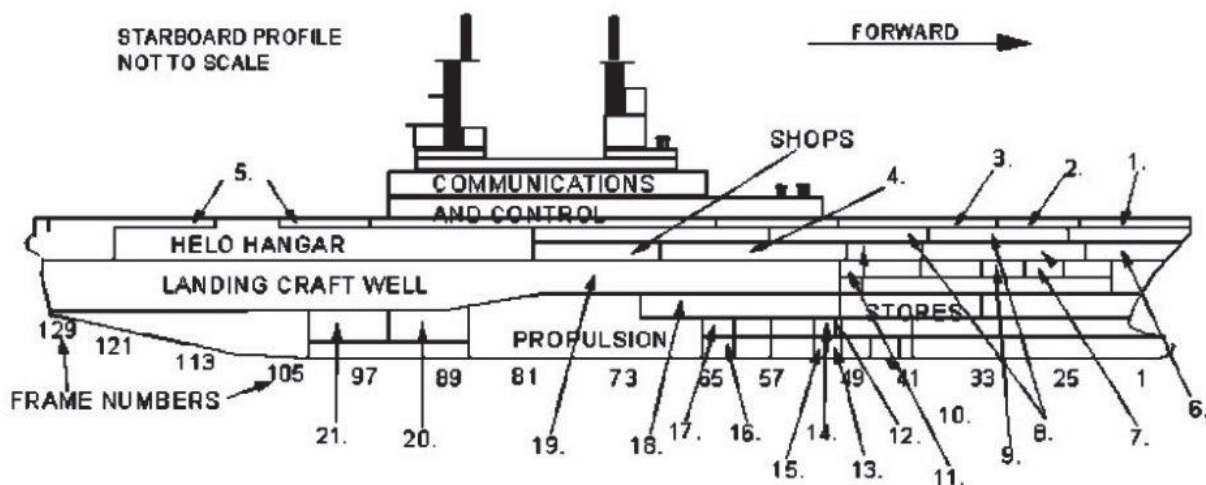
12. On July 12, 2020, at approximately 9:30 a.m., the NCIS Resident Agency office in San Diego, CA, became aware of a fire via multiple sources aboard the USS Bonhomme Richard (LHD-6) (hereinafter referred to as “BHR”). Commissioned in 1998, the BHR is a member of the Wasp-class, the US Navy’s large-deck multipurpose amphibious assault ship. A total of eight Wasp-class ships were built. All eight ships were in active service prior to the fire onboard the BHR. Wasp-class Landing Helicopter Dock (“LHDs”) embark, transport, deploy, command and fully support all elements of a Marine Expeditionary Unit (MEU) of 2,000 marines, inserting forces ashore via helicopters, landing craft and amphibious vehicles. In addition to the 2,000 plus marines it can transport, the BHR has a crew of approximately 1,000 sailors.



13. On July 12, 2020, the BHR was located at pier 2, berthing 6, on Naval Base San Diego, CA. The fire was first reported at approximately 8:10 a.m., based on the observation of smoke. The fire was reportedly located somewhere inside the lower vehicle stowage (“Lower V”). The general location of the Lower V is marked by a red box in the photograph above. The BHR personnel, Naval Base San Diego Fire Department, and numerous civilian fire departments from the surrounding cities responded to fight the fire.



14. Despite efforts to quickly extinguish the fire, the BHR burned for approximately five days. The fire damaged 470 spaces out of 1400. It has been reported



that 71 individuals were injured during the firefighting efforts. On July 16, 2020, the BHR was deemed safe for temporary entry and Special Agents from NCIS and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) made entry into the Lower V area in order to assess the scene and determine if ATF's Nation Response Team (NRT) should be activated or if the scope of work could be handled with local resources. Subsequent to the assessment, ATF NRT was activated. On July 18, 2020, the NRT began to evaluate the damage in an effort to obtain the cause and origin of the fire aboard the BHR. The NRT processed the scene in the Lower V of the ship for several days.

The Lower V. is identified by arrow 18 in the diagram above.

#### *Arson Determination*

15. The ATF Certified Fire Investigator ("CFI") used National Fire Protection Association ("NFPA") 921 – Guide for Fire and Explosive Investigations (2017) (hereinafter referred to as "NFPA 921") during the examination and processing of the fire scene. NFPA 921 establishes guidelines and recommendations used by public and private fire investigators while conducting origin and cause investigations.

16. An ATF CFI employed a systematic approach and considered relevant data while conducting the origin and cause investigation. The systematic approach was based-

1 on the scientific method, an organizational and analytical process suitable for fire scene  
2 investigations, which is also used in the physical sciences.

3 17. In order to determine the origin and cause of the fire, an ATF CFI had to  
4 ascertain where the fire started (origin) and the circumstances that brought about the fire  
5 (cause).

6 18. An ATF CFI examined the exterior of the BHR first and moved from areas  
7 of lesser damage to greater damage being mindful that the ship burned for several days.  
8 The fire damage observed on the exterior of the ship was consistent with a fire that  
9 originated inside and migrated out. The ATF CFI examined the interior of the BHR second  
10 and determined the fire originated in the Lower V based-on fire damage observed,  
11 knowledge of fire dynamics and witness statements.

12 19. An ATF CFI determined the fire originated at or near the starboard elevator  
13 bulkhead in the Lower V, which was based-on the aforementioned observations,  
14 knowledge and witness statements, in addition to arc mapping.

15 20. An ATF CFI considered competent ignition sources throughout the Lower V,  
16 e.g. electrical, mechanical, smoking, spontaneous heating and open flame as the cause of  
17 the fire. Ignition hypotheses were developed, tested and disproven, with the exception of  
18 open flame to available combustibles. Among other things, the progression and migration  
19 of the fire, coupled with the time in which a witness indicated that he believed he had  
20 observed MAYS enter the Lower V (as discussed in detail below) and the report of smoke  
21 led the ATF CFI to classify the fire as incendiary<sup>1</sup>. The ATF CFI classified the fire as  
22 incendiary based on fire damage observed, his knowledge of fire dynamics, arc mapping  
23 results and information collected through witness statements as relayed to him. The ATF  
24 CFI subjected his origin and cause opinion to a technical review with other CFIs before  
25 rendering his final conclusion.

26 //

27 \_\_\_\_\_  
28 <sup>1</sup> According to NFPA 921, the cause of a fire may be classified as accidental, natural,  
incendiary (arson) or undetermined.



*Additional Evidence of Arson*

21. On July 20, 2020, ATF Investigators found a plastic bottle that contained a small amount of liquid closest to the area of origin in the Lower V. Investigators flagged the plastic bottle, which had no cap, with a piece of fluorescent orange flagging tape around the neck of the bottle and placed it on top of a spool of rope. The tape served to alert crime scene technicians to the bottle's presence so that it could be collected and processed for DNA and fingerprints. Investigators left the flagged bottle in place at the scene while they continued to process other items of interest.

22. The next day, on July 21, 2020, upon returning to the scene, members of the ATF observed the plastic bottle was missing and the flagging tape with the same knot and loop used to mark the plastic bottle discarded on the floor. ATF immediately surveyed all members of the NRT and other law enforcement individuals who were processing the Lower V. None of these officials removed the bottle from the flagging tape or the scene. Investigators stopped processing the fire scene and conducted an exhaustive physical search of the Lower V and found three additional bottles and two aluminum cans. Records checks by NCIS revealed that during the timeframe the plastic bottle with the small amount of liquid went missing, MAYS's duty section had been onboard the BHR providing him or his associates access to the ship and Lower V. DNA was found on the discarded flagging tape. Analysis confirmed it was not MAYS's DNA or the DNA of the ATF investigator who found the bottle.

23. Investigators recovered the remaining three bottles and two cans. The second plastic bottle had a melted cap attached and contained a small amount of liquid. A third plastic bottle had no cap, was twisted at its approximate center and contained a small amount of liquid. A fourth plastic bottle had a partially melted cap with a hole in the center attached and contained a small amount of liquid. Both of the aluminum cans were open; one contained a small amount of liquid. All of the aforementioned liquid samples were submitted to the ATF Forensic Science Laboratory for analysis. One liquid sample, which

1 was associated with the second bottle, tested positive for a heavy petroleum distillate.  
2 Examples of heavy petroleum distillates include diesel, kerosene and jet fuel.

3 24. ATF Investigators also found a number of expended CO2 cartridges  
4 throughout the fire debris in the Lower V, some of which were reportedly stored there  
5 prior to the fire. However, investigators found additional CO2 cartridges inside the wash  
6 tub of a washer/dryer combination unit that appeared to have exploded during the fire, as  
7 well as additional cartridges on top of boxes of Purell hand-sanitizer that were inside coils  
8 of metal hose line.

9 25. On July 22, 2020, Lieutenant Commander Felix Perez, the Damage Control  
10 Assistant (DCA), conducted a walk-through of the Upper and Lower V compartments  
11 with NCIS and ATF agents. Perez's duties as the DCA entail knowledge of, and  
12 responsibility for, all fire-fighting equipment and personnel aboard the BHR. Perez stated  
13 there were four fire-fighting stations within the Upper and Lower V areas. Perez noted  
14 three of the four fire-fighting stations were not in their normal configuration. One station  
15 located on the port side of the Upper V did not have any hoses connected to the fire-  
16 fighting station. Perez stated regardless of maintenance status, there should have been  
17 hoses on the racks with at least one hose connected to the fire station per normal  
18 configuration. The fire station on the starboard side of the Upper V had one hose that was  
19 discovered cut during initial firefighting efforts and the second hose ran down the side of  
20 the BHR and appeared to be connected to diving equipment.

21 26. On July 22, 2020, Perez and the agents also inspected the fire station located  
22 at the bottom of the ramp in the Lower V. Perez noted while there were two hoses present  
23 on the racks, but not connected to the brass wye valve, he described the fire station as  
24 inoperable. Perez indicated the normal configuration would have a brass wye valve, which  
25 converts one stream of water from the fire main to two. The two valves could support two  
26 hoses, but in the ready position, one of the valves would have one hose connected to the  
27 one side of the wye valve with the other open in order to allow sailors to easily observe  
28 leaks from a faulty valve above. Perez noted there were no hoses or couplings connected

1 to the fire station and a brass coupling to the wye valve laid on the deck directly below the  
2 fire station. Perez again emphasized that the station was not in its normal configuration.  
3 Perez also noted a fourth fire station in the Lower V which was located near the aft  
4 conflagration station was found in the normal configuration. Perez recalled an incident  
5 approximately four (4) months earlier at another location of the ship where a fire hose was  
6 found cut on the fire nozzle end with the fire nozzle missing.

7 27. Perez further stated he or his damage control staff walked the aforementioned  
8 spaces for inspection on Friday, July 10, 2020 and while it was possible one station could  
9 have been overlooked, it was, in his opinion, nearly impossible for three of the four closest  
10 to and inside the Lower V to have been missed by damage control personnel. Of note, the  
11 fire-station at the bottom of the ramp to the Lower V in particular could have been used  
12 by the first responders who went into the Lower V. Perez opined that three of the four fire  
13 stations aboard the BHR appeared to be have been purposely tampered with and/or  
14 disconnected.

15 *Identification of MAYS*

16 28. Initial witness screenings of approximately 177 service members assigned to  
17 the BHR were conducted between June 19, 2020 and June 20, 2020. The screening  
18 interviews were administered via written questionnaires.

19 29. U.S. Sailor Seaman Kenji Velasco was interviewed several times regarding  
20 the fire onboard BHR. In his first interview, he reported that on July 12, 2020, at  
21 approximately 0805, while standing watch near the Lower V, he observed a “light-skin  
22 male” wearing clean coveralls, a facemask, carrying a silver/metal bucket with both hands  
23 in front of his body descend into the Lower V (MAYS). In this initial interview, however,  
24 Velasco said he did not recognize the individual. When discussing his questionnaire,  
25 Velasco did mention a sailor named MAYS that “hates” the U.S. Navy and the Fleet.

26 30. Velasco was re-interviewed on several subsequent occasions. Velasco stated  
27 that he was standing post at the Upper Vehicle Stowage (Upper V) prior to the fire. This  
28 area is directly above Lower V. Velasco worked onboard the BHR in the Deck Department

1 and has extensive knowledge of the layout of the BHR. Velasco stated that he observed  
2 an individual enter the “Lower V” area approximately 5 minutes before reports of white  
3 smoke. As he passed Velasco, the individual carried a metal bucket in his hands by the  
4 bucket itself, rather than its handle, in front of his torso and sarcastically stated, “I love  
5 Deck.” Velasco did not observe anyone else enter the Lower V area except that individual  
6 before the fire started. Velasco and Boatswain’s Mate Second Class (BM2) Beau Benson  
7 were interacting at Velasco’s post when Benson reported seeing white smoke. Benson nor  
8 Velasco reported seeing an individual leave the Lower V after the fire started. Velasco  
9 stayed at his post until relieved by firefighting personnel and Benson departed to report  
10 seeing white smoke. During an interview on July 21, 2020, Velasco said he was “fairly  
11 sure” and “90% sure” he saw MAYs descend into the Lower V at 0805 on the day of the  
12 fire.

13 31. Velasco further explained that in the hours and days after the fire, it had  
14 dawned on him that the individual who descended to the Lower V at 0805 on the day of  
15 the fire was MAYS’s height and build, had fair hair that could be seen coming out from  
16 his cover, like MAYS, sounded like MAYS, and said, “I love deck,” which is an  
17 expression Velasco knew MAYS to say. Velasco further explained that after the fire on  
18 the BHR he was attending a muster at the base theater, when he asked MAYS if he had  
19 gone to the Lower V before the fire started. According to Velasco, MAYS, replied, “Yes.”

20 32. In late August 2020, investigators followed up with sailors who may  
21 have been in the vicinity of this exchange between Velasco and MAYS. Several sailors  
22 said they did not have a recollection from that day. However, MAYS’s friend, Gonzalez,<sup>2</sup>  
23 said he remembered Velasco asking the question to MAYS and MAYS looking  
24 uncomfortable. Gonzalez did not remember MAYS answering.

25 33. On July 20, 2020, Benson reported he had a conversation with Velasco in the  
26 Naval Base San Diego movie theatre. During this interaction, Velasco told Benson that

---

27 <sup>2</sup> During an interview, described below, MAYS named two close friends, Matthew  
28 Gonzalez and Joshua McGill.

1 while having port side watch on July 12, 2020, Velasco observed an unknown person walk  
2 down the Lower V ramp holding something in his/her hands. Benson was not able to give  
3 a description of the unknown person or the items he was carrying in his/her hands because  
4 Velasco did not provide Benson any identifiers of the unknown person. Benson stated  
5 Velasco told him the unknown person stated "I love deck" as he/she walked by Velasco  
6 and down the ramp.

7       34. On August 29, 2020, Boatswain's Mate Third Class Matthew Betz was  
8 interviewed. Betz recounted a conversation he had with Velasco the day after the fire.  
9 According to Betz, Velasco told him that he saw someone go down to the Lower V the  
10 day of the fire wearing boot camp coveralls and carrying a plastic bucket. Velasco said  
11 the person he saw go down to the Lower V said "Fuck deck" or "I love deck" when he  
12 went down the ramp. Betz indicated he believed the person Velasco described going down  
13 to the Lower V was MAYS because MAYS wore the boot camp coveralls the week prior  
14 to the fire. According to Betz, after Velasco described the person he saw going down to  
15 the Lower V, Betz told Velasco that sounded like MAYS. Betz said a separate Sailor said  
16 MAYS came into the berthing area to tell everyone to get off the ship because the ship  
17 was on fire. Betz said MAYS could have went up the escape truck, went into the deck  
18 berthing area, and take his coveralls off while wearing his cammies underneath the  
19 coveralls. Betz said it is normal for Sailors to wear coveralls over their cammies, because  
20 Sailors were not allowed to wear coveralls around base.

21       35. On July 21, 2020, Command Master Chief (CMC) Jose Hernandez also  
22 identified MAYS as a person who showed disdain towards authority and the U.S. Navy.

23       36. A copy of the roster of sailors on board the BHR on the morning of July 12,  
24 2020 showed that Duty Section Six was on duty to which both Velasco and MAYS were  
25 assigned. It was also determined that MAYS was not certified in ship board firefighting  
26 techniques, also referred to as Damage Control. On July 18, 2020, ATF determined that  
27 the fire originated in the Lower V, the same area where Velasco observed MAYS enter,  
28 but not exit.



37. Initial checks of publically available social media web sites showed an Instagram post (depicted below) associated with MAYS, made on June 14, 2020, which stated, “I love the smell of napalm in the morning.” Initial checks into MAYS’s Navy



background, revealed that he joined the Navy in 2019 with the intent on becoming trained in the Advanced Electronics Computer Fields. At some point, MAYS changed his career goals to becoming a Navy SEAL, via completion of the BUDS. MAYS started BUDS in approximately October 2019; however, five days after training began, MAYS exercised his option out of training and “Dropped on Request,” known as a DOR. The DOR officially ended his pursuit of becoming a SEAL. After his DOR from the SEAL training program, MAYS was reassigned to BHR as an undesignated Seaman. According to Navy leadership, the morale and behavior of sailors who had aspired to become a SEAL, and then find themselves serving in a more traditional role on a Navy ship, are frequently very challenging.

38. A review of MAYS’s screening interview revealed that on July 20, 2020, he participated in Duty Section Six screening interviews. In response to a question on the questionnaire, which asked how he learned about the fire; MAYS wrote that he was in the



1 Hangar Bay<sup>3</sup> and saw black smoke. In response to a question that asked what time he  
2 learned of the fire; MAYS wrote the he found out at approximately 0830 that morning.<sup>4</sup>  
3 Another question asked if he was working or scheduled to work in the Lower V area the  
4 day of the fire; MAYS replied “No, I was suppose to clean the mousing [sic] stations.”<sup>5</sup>

5 39. Additionally, of all the individuals screened, MAYS was the only person who  
6 reported smelling “burning fuel/rubbery smell.” According to an investigating ATF CFI,  
7 the terminology MAYS used to describe the smell of the fire was consistent with items  
8 and materials that the ATF observed in the Lower V during their scene examination. In  
9 particular, the ATF CFI noted two forklifts had four rubber tires each. On each forklift,  
10 the two tires facing the starboard side of the BHR were burned and melted to varying  
11 degrees. The ATF CFI also indicated he observed ammunition carts that had hard-cast  
12 rubber wheels, which were also burnt to varying degrees.

13 40. The questionnaire also asked how individuals felt when they learned about  
14 the fire; MAYS reported that he felt a “small amount of adrenaline and anxiety.” During  
15 the screening process, MAYS reviewed his questionnaire with a NCIS special agent and  
16 stated that he had taken a picture of the fire with his cellular phone after he exited the  
17 BHR.

18 41. Velasco also revealed there are conflagration stations<sup>6</sup> in the “Lower V”  
19 where an individual could leave the Lower V without going back up the ramp to the Upper  
20 V. Deck Department personnel are responsible for maintaining conflagration stations in  
21 Lower V. The Lower V contains two conflagration stations, one at the forward bulkhead

---

22 <sup>3</sup> Hangar bay is an area for storing/repairing aircraft, and additional equipment or supplies.  
23

24 <sup>4</sup> This response is inconsistent with VELASCO’s observation of him entering the Lower  
25 V area around 0805, five minutes prior to the reports of smoke in the Lower V.

26 <sup>5</sup> A mooring station is an area of the ship used to secure a ship at a berth.

27 <sup>6</sup> A conflagration station is a small observation room generally used to stand watch of  
28 the area while out to sea where a sailor can, among other things, initiate firefighting  
operations or escape a space.

1 and one at the aft bulkhead. Each conflagration station contained escape trunks with  
2 ladders that only go up out the Lower V. The escape trunks from each conflagration station  
3 open to a variety of locations within the ship.

4 42. On July 16, 2020, during ATF's initial assessment of the scene, ATF agents  
5 noted that the door leading into the BHR's conflagration station at the aft bulkhead,  
6 identified as 4-72-2-C, was open while the door connected to the forward conflagration  
7 station was closed.

8 43. On July 27, 2020, NCIS agents traversed an access trunk on the USS Boxer  
9 (LHD-4), a ship that is similar in type, specifically within a conflagration station located  
10 at 4-72-2-C. The agents maneuvered from the Lower V to an area between the mess deck  
11 and hanger bay areas through an access trunk identified as 2-74-2-T in approximately 23  
12 seconds.

13 44. On July 31, 2020, a NCIS agent went to the Lower V of the BHR to the aft  
14 conflagration station identified as 4-72-2-C, noted an open access door leading from the  
15 Lower V into the conflagration station and noted an additional door inside the  
16 conflagration station identified as 4-71-2 that was also open. This door led to an access  
17 trunk identified as 4-72-4-T which led to an access hatch in the same location as the one  
18 on the USS Boxer. The NCIS agent could not access the closed hatch as it was blocked by  
19 fire debris from above.

20 45. On July 22, 2020, CMC Hernandez was interviewed by NCIS and ATF  
21 agents and explained that, on July 5, 2020, MAYS was sleeping in his assigned berthing  
22 during his duty day. Although MAYS was allowed to have personnel items in the berthing  
23 area, MAYS was not allowed to be sleeping aboard or during the duty day. MAYS was  
24 awoken by a contractor who was working near MAYS's sleeping area identified as rack  
25 twenty-seven in compartment 1-25-0-L. MAYS reacted by verbally confronting the  
26 contractor in an aggressive way, causing the contractor to report the incident to Navy  
27 personnel.

28 //



1 assist fire fighters, alert at least one sailor in crew berthing to the threat of the fire, and  
2 how he eventually helped fight the fire. When directly asked, MAYS repeatedly denied  
3 having started the fire on the BHR or having been in the Lower V on the day of the fire.  
4 He maintained his innocence as to being the cause of the fire throughout the entire  
5 interview. At one point, after being told that he had been identified as having descended  
6 the ramp to the Lower V, before the fire started, MAYS stated that he was being setup.

7       49. Approximately two hours into the interview, MAYS told investigators for the  
8 first time that a group of sailors in the Deck Department had discussed that an unknown  
9 sailor had seen an individual in coveralls and a mask, carrying a bucket to the Lower V  
10 just before the fire started. Investigators had not previously mentioned during the course  
11 of the interview that the individual had been seen wearing a mask. At one point MAYS  
12 told investigators the witness could not have identified him because, "I had a face mask  
13 on."

14       50. Investigators asked MAYS the different routes to leave the Lower V, to  
15 which MAYS replied a person in the Lower V would be "fucked," implying no way out,  
16 if present during a fire. Initially, MAYS said the only route out of the Lower V was to  
17 walk up the ramp from the Lower V to the Upper V. Eventually, MAYS stated he knew  
18 about the two conflagration stations in the Lower V because he cleaned them in the past.  
19 MAYS also stated he knew one of the conflagration stations terminated at the 01 Level  
20 where the Hanger Bay and Mess Decks were located. MAYS claimed the other  
21 conflagration station terminated in an area where contractors stored their supplies above  
22 the Lower V. Lastly, MAYS admitted he has traversed at least one of the two conflagration  
23 station ladders where he learned to "skate off and hide" from work.

24       51. Investigators asked MAYS about his Instagram post and he seemed to  
25 indicate that it was an homage to Apocalypse Now, the movie he had quoted.

26       52. MAYS initially told investigators he lost most of his worldly possessions in  
27 the fire because he stored them in berthing aboard BHR, with the exception of his  
28 MacBook Pro computer. MAYS indicated he kept the MacBook Pro with him and not

1 aboard BHR because it was too valuable.

2 53. At approximately 6:30 PM, investigators asked MAYS to identify the  
3 location of his computer because NCIS agents did not find it in his residence or vehicle  
4 while serving search warrants. MAYS replied and stated he owned two computers; one  
5 Acer laptop and one MacBook Pro.

6 54. According to MAYS, both computers were at his mother's house in  
7 Kentucky. MAYS stated his mom purchased the MacBook Pro as a gift when he was a  
8 junior or senior in high school. MAYS described the MacBook Pro as the most expensive  
9 gift his mom ever purchased for him besides his truck. MAYS told investigators he  
10 shipped the MacBook Pro to his mom in Kentucky in March or April 2020 because he had  
11 no use for it while in BUD/S in Coronado, California. MAYS told investigators the Acer  
12 had always been in Kentucky at his mom's house. MAYS stated there was no password  
13 for the Acer computer and claimed he did not remember the password for his MacBook  
14 Pro despite having just provided passwords for online accounts.

15 55. At approximately 10:45 PM, MAYS told investigators he took the MacBook  
16 Pro with him to boot camp in Great Lakes, Illinois in July or August 2019. According to  
17 MAYS, he was attending a BUD/S preparatory school in Great Lakes, IL when he posted  
18 the MacBook Pro for sale on "GroupMe." MAYS described GroupMe as social media  
19 platform used by his pre-BUD/S classmates. MAYS stated he sold the MacBook Pro to a  
20 classmate for \$700.00. MAYS stated he could not identify the classmate by name.

21 56. According to MAYS, his mom routinely asked about his MacBook Pro  
22 including after the BHR fire. MAYS told investigators he lied to his mom since selling  
23 the computer in 2019.

24 57. Investigators asked MAYS to go to the BHR with them and show them where  
25 he had been on the ship the morning of the fire. MAYS agreed and walked with them  
26 through the BHR. MAYS stated he was willing to take a polygraph examination and  
27 eventually asked to take one.

28 //





*Execution of Search Warrants*

62. On August 20, 2020, investigators executed federal search warrants, searching MAYS's apartment, vehicle, cell phone, his person, and taking a buccal DNA swab.

63. Investigators found and seized 1 uniform pair of pants (type 3s), 3 pairs of boots, laundry booster, assorted letters sent to MAYS, and photos from MAYS's barracks room. One additional letter was recovered from MAYS's vehicle. Additionally, MAYS's iPhone was seized.

64. Investigators have downloaded MAYS cell phone but the analysis is in its early stages and ongoing. As of this writing, investigators have found no significant inculpatory or exculpatory evidence as relates to MAYS.

65. A partial male DNA profile was recovered from the flagging tape. Analysis revealed it did not belong to MAYS.

*Identification of Subject Accounts*

66. **Subject Account-1, Subject Account-2 and Subject Account-3** were all identified during a manual review of MAYS's iPhone during the execution of the above mentioned search warrant. **Subject Account-4** was identified when MAYS listed it as his email address on his screening questionnaire completed on July 20, 2020. **Subject Account-5** was listed on Navy Federal Credit Union financial records, which were obtained via a Grand Jury subpoena.

BASIS FOR EVIDENCE SOUGHT IN SEARCH WARRANT

67. Based on my training and experience, consultation with other agents and officers experienced in arson investigations, and all the facts and opinions set forth above in this affidavit, I know that individuals involved with arsons often utilize cell phones and computers to access accounts, including accounts maintained by Apple, Google, and Yahoo, in the weeks and months prior to, during, and after an arson event, so the **Subject Accounts** could contain:

a. Communications, photographs, videos, or other data depicting

1 clothing, disguises worn (e.g., masks), tactics, techniques and procedures used to commit  
 2 the arson and materials used during the arson, along with any trophies seized, and also  
 3 items related to an individual's motivation for committing arson;

4           b. Internet and web-search history relating to the arson (e.g., research and  
 5 news articles relating to the arsons to monitor law enforcement's investigation and  
 6 response to the fire as well as gratification);

7           c. Celebratory remarks or veiled remarks after the arson;

8           d. Geo-locational information related to an arson;

9           e. Communications, photographs, videos, or other data depicting  
 10 clothing and gear used during an arson or related to the arson itself; and

11           f. Communications about covering up or hiding their crimes and  
 12 escaping or hiding from law enforcement.

#### 13                   GENUINE RISKS OF DESTRUCTION OF EVIDENCE

14           68. Based upon my experience and training, and the experience and training of  
 15 other agents with whom I have communicated, electronically stored data can be  
 16 permanently deleted or modified by users possessing basic computer skills. In this case,  
 17 only if the user of the **Subject Accounts** or a coconspirator with access to the **Subject**  
 18 **Accounts** receives advance warning of the execution of this warrant, will there be a  
 19 genuine risk of destruction of evidence. If this application and order are placed under seal  
 20 and a preclusion order issues, I do not believe that the **Subject Accounts** user is likely to  
 21 destroy evidence.

#### 22                   PRIOR ATTEMPTS TO OBTAIN THIS EVIDENCE

23           69. To date, the United States has attempted to obtain data contained within the  
 24 **Subject Accounts** by obtaining a search warrant for MAYS's cellular phone. A forensic  
 25 analysis of that data is ongoing and has not been completed. Additionally, the United  
 26 States has attempted to obtain data contained in **Subject Account-4** and **Subject**  
 27 **Account-5** by obtaining an order authorizing disclosure of information under 18 U.S.C.  
 28 section 2703(d). Analysis of those subject accounts have not been completed.

## 1 PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

2 70. Apple, Google, and Yahoo ("ISPs") provide electronic communication  
3 services to their subscribers. The ISPs allow subscribers to exchange electronic  
4 communications with others through the Internet. The ISPs' subscribers access to their  
5 services through the Internet.

6 71. Subscribers to the ISPs' electronic communication services use account  
7 names during their electronic communications. The account names may or may not  
8 identify the real name of the person using a particular screen name. Although the ISPs  
9 requires users to subscribe for a free account, they do not verify the information provided  
10 by the subscriber for their free services.

11 72. At the creation of the ISPs' account and for each subsequent access to the  
12 account, the ISPs log the IP address of the computer accessing the account. An IP address  
13 is a unique address through which a computer connects to the Internet. IP addresses are  
14 leased to businesses and individuals by Internet Service Providers. Obtaining the IP  
15 addresses that have accessed a particular electronic account often identifies the Internet  
16 Service Provider that owns and has leased that address to its customer. Subscriber  
17 information for that customer then can be obtained using appropriate legal process.

18 73. Federal agents and investigative support personnel are trained and  
19 experienced in identifying communications relevant to the crimes under investigation.  
20 The ISPs' personnel are not. It would be inappropriate and impractical for federal agents  
21 to search the ISPs' vast computer network for the relevant accounts and then to analyze  
22 the contents of those accounts on the ISPs' premises. The impact on its business would  
23 be disruptive and severe.

24 74. Therefore, I request authority to seize all content, including electronic mail  
25 and attachments, stored instant messages, stored voice messages, photographs, and any  
26 other content from the subject's the ISPs accounts, as described in **Attachments B-1, B-**  
27 **2, B-3, B-4, and B-5.** In order to accomplish the objective of the search warrant with a  
28 minimum of interference with the ISPs' business activities, to protect the privacy of its

1 subscribers whose accounts are not authorized to be searched, and to effectively pursue  
2 this investigation, the NCIS seeks authorization to allow the ISPs to make digital copies  
3 of the entire contents of the accounts subject to seizure. Those copies will be provided to  
4 me or to an authorized federal agent. The copy will be imaged and the image will then be  
5 analyzed to identify communications and other electronic records subject to seizure  
6 pursuant to **Attachments B-1, B-2, B-3, B-4 and B-5**. Relevant electronic records will be  
7 copied to separate media. The original media will be sealed and maintained to establish  
8 authenticity, if necessary.

9       75. Analyzing the data to be provided by the ISPs may require special technical  
10 skills, equipment, and software. It may also be time-consuming. Searching by keywords,  
11 for example, often yields many thousands of "hits," each of which must be reviewed in its  
12 context by the examiner to determine whether the data is within the scope of the warrant.  
13 Merely finding a relevant "hit" does not end the review process. Keyword searches do not  
14 capture misspelled words, reveal the use of coded language, or account for slang or  
15 typographical errors. Keyword searches are further limited when electronic records are in  
16 or use foreign languages. Certain file formats also do not lend themselves to keyword  
17 searches. Keywords search text. Attachments to electronic mail messages are often in  
18 proprietary formats that do not store data as searchable text. Instead, such data is saved  
19 in a proprietary non-text format. And, as the volume of storage allotted by service  
20 providers increases, the time it takes to properly analyze recovered data increases  
21 dramatically. Internet Service Providers like Google do not always organize the electronic  
22 files they provide chronologically, which makes review even more time consuming and  
23 may also require the examiner to review each page or record for responsive material.

24       76. Based on the foregoing, searching the recovered data for the information  
25 subject to seizure pursuant to this warrant may require a range of data analysis techniques  
26 and may take weeks or even months. Keywords need to be modified continuously based  
27 upon the results obtained and, depending on the organization, format, and language of the  
28 records provided by Google, examiners may need to review each record to determine if it

1 is responsive to **Attachments B-1, B-2, B-3, B-4 and B-5**. The personnel conducting the  
2 examination of the ISPs' records will complete the analysis within **ninety (90) days** of  
3 receipt of the data from the service provider, absent further application to this court.

4 77. Based upon my experience and training, and the experience and training of  
5 other agents with whom I have communicated, it is necessary to review and seize all  
6 electronic communications that identify any users of the **Subject Accounts** and any  
7 electronic communications sent or received in temporal proximity to incriminating  
8 messages that provide context to the incriminating communications.

9 78. All forensic analysis of the imaged data will employ search protocols directed  
10 exclusively to the identification and extraction of data within the scope of this warrant.

11 **PROCEDURES FOR ELECTRONICALLY STORED INFORMATION FOR**  
12 **COMPUTERS AND OTHER ELECTONIC MEDIA**

13 *Forensic Imaging*

14 79. After securing the premises, or if sufficient information is available pre-  
15 search to make the decision, the executing agents will determine the feasibility of  
16 obtaining forensic images of electronic storage devices while onsite. A forensic image is  
17 an exact physical copy of the hard drive or other media. A forensic image captures all the  
18 data on the hard drive or other media without the data being viewed and without changing  
19 the data. Absent unusual circumstances, it is essential that a forensic image be obtained  
20 prior to conducting any search of the data for information subject to seizure pursuant to  
21 this warrant. The feasibility decision will be based upon the number of devices, the nature  
22 of the devices, the volume of data to be imaged, the need for and availability of computer  
23 forensics specialists, the availability of the imaging tools required to suit the number and  
24 nature of devices found, and the security of the search team. The preference is to image  
25 onsite if it can be done in a reasonable amount of time and without jeopardizing the  
26 integrity of the data and the agents' safety. The number and type of computers and other  
27 devices and the number, type, and size of hard drives are of critical importance. It can  
28 take several hours to image a single hard drive - the bigger the drive, the longer it takes.

1 As additional devices and hard drives are added, the length of time that the agents must  
2 remain onsite can become dangerous and impractical.

3 80. If it is not feasible to image the data on-site, computers and other electronic  
4 storage devices, including any necessary peripheral devices, will be transported offsite for  
5 imaging. After verified images have been obtained, the owner of the devices will be  
6 notified and the original devices returned within ninety (90) days of seizure absent further  
7 application to this court.

8 *Identification and Extraction of Relevant Data*

9 81. After obtaining a forensic image, the data will be analyzed to identify and  
10 extract data subject to seizure pursuant to this warrant. Analysis of the data following the  
11 creation of the forensic image can be a highly technical process requiring specific  
12 expertise, equipment and software. There are thousands of different hardware items and  
13 software programs, and different versions of the same programs, that can be commercially  
14 purchased, installed, and custom-configured on a user's computer system. Computers are  
15 easily customized by their users. Even apparently identical computers in an office or home  
16 environment can be different with respect to configuration, including permissions and  
17 access rights, passwords, data storage, and security. It is not unusual for a computer  
18 forensic examiner to have to obtain specialized hardware or software, and train with it, in  
19 order to view and analyze imaged data.

20 82. Analyzing the contents of a computer or other electronic storage device, even  
21 without significant technical challenges, can be very challenging. Searching by keywords,  
22 for example, often yields many thousands of hits, each of which must be reviewed in its  
23 context by the examiner to determine whether the data is within the scope of the warrant.  
24 Merely finding a relevant hit does not end the review process for several reasons. The  
25 computer may have stored metadata and other information about a relevant electronic  
26 record – e.g., who created it, when and how it was created or downloaded or copied, when  
27 it was last accessed, when it was last modified, when it was last printed, and when it was  
28 deleted. Keyword searches may also fail to discover relevant electronic records, depending



1 on how the records were created, stored, or used. For example, keywords search text, but  
2 many common electronic mail, database, and spreadsheet applications do not store data as  
3 searchable text. Instead, the data is saved in a proprietary non-text format. Documents  
4 printed by the computer, even if the document was never saved to the hard drive, are  
5 recoverable by forensic programs because the printed document is stored as a graphic  
6 image. Graphic images, unlike text, are not subject to keyword searches. Similarly, faxes  
7 sent to the computer are stored as graphic images and not as text. In addition, a particular  
8 relevant piece of data does not exist in a vacuum. To determine who created, modified,  
9 copied, downloaded, transferred, communicated about, deleted, or printed the data  
10 requires a search of other events that occurred on the computer in the time periods  
11 surrounding activity regarding the relevant data. Information about which user had logged  
12 in, whether users share passwords, whether the computer was connected to other  
13 computers or networks, and whether the user accessed or used other programs or services  
14 in the time period surrounding events with the relevant data can help determine who was  
15 sitting at the keyboard.

16 83. It is often difficult or impossible to determine the identity of the person using  
17 the computer when incriminating data has been created, modified, accessed, deleted,  
18 printed, copied, uploaded, or downloaded solely by reviewing the incriminating data.  
19 Computers generate substantial information about data and about users that generally is  
20 not visible to users. Computer-generated data, including registry information, computer  
21 logs, user profiles and passwords, web-browsing history, cookies and application and  
22 operating system metadata, often provides evidence of who was using the computer at a  
23 relevant time. In addition, evidence such as electronic mail, chat sessions, photographs  
24 and videos, calendars and address books stored on the computer may identify the user at  
25 a particular, relevant time. The manner in which the user has structured and named files,  
26 run or accessed particular applications, and created or accessed other, non-incriminating  
27 files or documents, may serve to identify a particular user. For example, if an incriminating  
28 document is found on the computer but attribution is an issue, other documents or files

1 created around that same time may provide circumstantial evidence of the identity of the  
2 user that created the incriminating document.

3 84. Analyzing data has become increasingly time-consuming as the volume of  
4 data stored on a typical computer system and available storage devices has become mind-  
5 boggling. For example, a single megabyte of storage space is roughly equivalent of 500  
6 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is  
7 roughly equivalent of 500,000 double-spaced pages of text. Computer hard drives are  
8 now being sold for personal computers capable of storing up to 2 terabytes (2,000  
9 gigabytes) of data. And, this data may be stored in a variety of formats or encrypted  
10 (several new commercially available operating systems provide for automatic encryption  
11 of data upon shutdown of the computer). The sheer volume of data also has extended the  
12 time that it takes to analyze data. Running keyword searches takes longer and results in  
13 more hits that must be individually examined for relevance. And, once reviewed, relevant  
14 data leads to new keywords and new avenues for identifying data subject to seizure  
15 pursuant to the warrant.

16 85. Based on the foregoing, identifying and extracting data subject to seizure  
17 pursuant to this warrant may require a range of data analysis techniques, including hashing  
18 tools to identify data subject to seizure pursuant to this warrant, and to exclude certain  
19 data from analysis, such as known operating system and application files. The  
20 identification and extraction process, accordingly, may take weeks or months. The  
21 personnel conducting the identification and extraction of data will complete the analysis  
22 within one-hundred twenty (120) days of this warrant, absent further application to this  
23 court.

24 86. All forensic analysis of the imaged data will employ search protocols directed  
25 exclusively to the identification and extraction of data within the scope of this warrant.

26 87. After extraction of the data, law enforcement personnel will separate out  
27 relevant information as described in **Attachment B-1, B-2, B-3, B-4, and B-5**. After the  
28 review is completed, non-relevant information (apparent innocent third party information)

1 will be preserved with an evidence custodian but not accessed again post-review absent  
2 further authorization from the Court.

3 REQUEST FOR SEALING AND PRECLUSION OF NOTICE

4 88. At this time, MAYS is not aware of the full extent of the investigation. I  
5 believe that, if MAYS and any potential co-conspirators were to learn NCIS were  
6 investigating them, they would take steps to evade prosecution and would also seek to  
7 destroy evidence.

8 89. Accordingly, I am requesting that this Affidavit, Applications For Search  
9 Warrants, the Search Warrants, and Sealing Motions and Orders related to the **Subject**  
10 **Accounts** be sealed until further order of the Court, and Google be precluded from  
11 notifying the subscriber for a period of six months, that is, no earlier than **March 3, 2021**.  
12 I am requesting a six-month preclusion period because investigators are reviewing a  
13 voluminous amount of evidence in furtherance of the investigation, including digital  
14 records. Further, it can take ISPs four weeks or longer to respond to warrant requests.  
15 Accordingly, I believe that preclusion of notice is necessary for a six-month period to  
16 avoid alerting the target(s) of this investigation to the full nature and scope of the  
17 investigation, which would likely result in the destruction of evidence. MAYS has already  
18 given contradictory statements about the location of his computer, possibly for the purpose  
19 of frustrating the investigation.

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

CONCLUSION

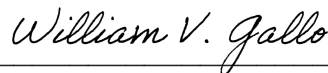
90. Based on the foregoing, I believe there is probable cause to believe items that constitute evidence of violations of federal criminal law, namely, 18 U.S.C. Sections 81 (Arson within special maritime and territorial jurisdiction), 844(f) (Use of fire to damage federal property), 1001 (False statements), and that evidence of said violations as described in **Attachments B-1, B-2, B-3, B-4, and B-5** will be found in/at/on the properties to be searched, as provided in Attachments A-1, A-2, A-3, A-4, A-5.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.



Maya Kamat  
Special Agent  
Naval Criminal Investigative Service

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 03rd day of September, 2020.



HON. WILLIAM V. GALLO  
United States Magistrate Judge

**ATTACHMENT A-2**

**DESCRIPTION OF THE ACCOUNT TO BE SEARCHED**

Information associated with the Google email account “mayssawyer628@gmail.com” (“**Subject Account-2**”) that is stored at premises controlled by Google, a company whose headquarters is located at 1600 Amphitheatre Parkway in Mountain View, CA.

**ATTACHMENT B-2**

**I. Service of Warrant**

The officer executing the warrant shall permit Google, LLC, as 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. Items to be Provided by Google, LCC**

Any and all messages, e-mails, records, files, logs, or information (whether deleted or not) concerning:

A. All records or other information regarding the identification of the account, to include subscriber information, full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

B. Any and all available location data;

C. All photos and/or videos stored by an individual using this account;

D. All messages sent or received by an individual using this account from **June 1, 2020 to August 21, 2020;**

E. All messaging application data stored or backed up by user;

F. The types of service utilized by the user; and

G. All records pertaining to communications between Google, LLC and any person regarding the account, including contacts with support services and records of actions taken.

//

//



### III. Items to be Seized as Evidence

The search of the data supplied by the Google, LLC pursuant to this warrant will be conducted by NCIS as provided in the “Procedures For Electronically Stored Information” of the affidavit submitted in support of this search warrant and will be limited to the seizure of:

- a. Communications, records, and attachments tending to identify the research or viewing of news articles, reports, or other information related to arson or starting fires or covering up crimes, including information related to the July 12, 2020 fire aboard the USS Bonhomme Richard;
- b. Communications, records, and attachments tending to identify or explain a motivation to commit arson aboard the USS Bonhomme Richard;
- c. Photographs or videos depicting coveralls, a bucket, fire, smoke, implements for starting a fire, accelerants, or possible trophies from the arson on the USS Bonhomme Richard;
- d. Location data tending to identify travel to and from, or presence aboard the USS Bonhomme Richard on July 12, 2020 and July 20 to 21, 2020; and
- e. Communications, records, and attachments that provide context to any communications described above, such as electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail tending to identify users of the subject accounts for the **period from June 1, 2020 to August 21, 2020;**

**which are evidence of violations of 18 U.S.C. Sections 81, 844(f), and 1001.**

The seizure and search of the Subject Account shall follow the procedures outlined in the supporting affidavit.