

UNITED STATES DISTRICT COURT

for the  
Southern District of California

**SEALED**

s/ T. Ferris

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Cellular telephone utilizing number  
(606) 922-0727

ORDERED UNSEALED on 08/03/2021 s/ TrishaF

Case No. 20MJ3390

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-3, incorporated herein by reference.

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

See Attachment B-3, 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
18 USC sec. 844(f)	Fire to damage federal property

The application is based on these facts:

See Attached Affidavit of NCIS Special Agent Albert Porter, 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.

Albert Porter

Applicant's signature

Special Agent Albert Porter 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: 08/14/2020

Allison H. Goddard

Judge's signature

City and state: San Diego, California

HON. ALLISON H. GODDARD, U.S. Magistrate Judge

Printed name and title

Print

Save As...

Attach

Reset

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS**

I, Albert Porter, being duly sworn, declare and state:

**INTRODUCTION**

1. This affidavit is submitted in support of applications to search the following premise, vehicle, and cellular telephone (collectively, “**Subject Properties**”), and person:

(a) Snyder Hall, Building 3380, Room S1241B, Naval Base San Diego (“**Subject Residence**”);

(b) A 2011 Dodge RAM 1500, dark gray in color, bearing California license 61328Z1 and registered to Ryan Sawyer MAYS (“**Subject Vehicle**”);

(c) A cellular telephone bearing number (606) 922-0727 and utilized by Ryan Sawyer MAYS (“**Subject Telephone**”); and

(d) Ryan Sawyer MAYS, DOB May, 29, 2001 (“**Target Subject**”);

as more fully described in Attachments A-1, A-2, A-3, A-4, respectively, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. Sections 81, Arson within special maritime and territorial jurisdiction, and 844(f), Use of fire to damage federal property (the “**Target Offenses**”), as more fully described in Attachments B-1 (**Subject Residence**), B-2 (**Subject Vehicle**), B-3 (**Subject Telephone**), and B-4 (**Target Subject**). The search of the **Target Subject** would include the seizure of evidence in the form deoxyribonucleic acid (DNA).

2. Based on the information outlined below, probable cause exists that evidence, fruits, and instrumentalities of violations of federal criminals laws may be found on, at, or in the **Subject Properties** and **Target Subject**.

3. The **Subject Properties** and **Target Subject** are all presently located in the Southern District of California.

//

//

## EXPERIENCE AND TRAINING

4. I am a Special Agent with the Naval Criminal Investigative Service (NCIS), San Diego, California. I have been assigned to NCIS in this capacity since March of 2009. I am currently assigned to NCIS Resident Agency San Diego, CA. My duties as an NCIS Special Agent include, but are not limited to, counterintelligence investigation and criminal investigations regarding crimes committed by or against Navy or Marine Corps installations, aircraft, or vessels, investigating crimes involving Department of the Navy or Marine Corps military personnel or civilian employees. Prior to becoming an NCIS Special Agent, I was a Federal Air Marshal from 2002 to 2009, Criminal Intelligence for the Federal Bureau of Prisons from 1995-2002, and a San Diego County Correctional Deputy Sheriff from 1993-1995. I served in the United States Navy as a SEAL (Sea Air Land) from 1983 through 1990, where as an Instructor at Basic Underwater Demolition School (BUDS), I obtained Sailor of the Year and Shore Sailor of the Year Runner-up. I obtained a Bachelor's of Science in Vocational Studies, from Southern Illinois University, at Carbondale in 1991 and a Master in Forensic Sciences National University in 2001.

5. My formalized training includes successful completion of the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC), located in Glynco, Georgia. The CITP course includes intensive training on subjects such as interviewing, firearms, digital forensics, and tactical training, as well as extensive legal courses. I have also successfully completed the NCIS Special Agent Basic Training Program (SABTP), which is a 12-week course with curriculum specifically tailored to the unique challenges faced by NCIS. Such training included military law, death investigations, crime scene processing, intelligence, and narcotics investigation. I have apprehended military members. I have served Command Authorization's for Search and Seizure to search persons, vehicles, barrack's room, berthing areas, digital devices, medical records and the like. I have served search warrants for off base related searches. In my training and experience, it is commonly known that people use their cellular phone

1 to research, store images, data, and text messages relating to elements of the crime. I have  
2 successfully worked criminal cases regarding, but not limited to: arson, domestic violence,  
3 communication of a threat, death, fraud, narcotics, prostitution, sexual assaults, as well as  
4 counterintelligence related investigations.

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

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

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

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

#### 24 BACKGROUND ON DEOXYRIBONUCLEIC ACID

25 10. I know DNA is short for deoxyribonucleic acid. DNA molecules are  
26 contained with human cells and hold the genetic coding that makes each of us individually  
27 distinctive. DNA technology is capable of distinguishing between human beings to an  
28 extent that typically the probability of a random person having the same profile as the

1 questioned profile is many times more that the population of the planet. Such evidence  
2 is commonly introduced in evidence in United States District Courts, Military Courts,  
3 California Superior Courts, and other state courts and has successfully withstood attack  
4 on foundational and *Kelly-Frye* grounds. The DNA evidence I am seeking can be used to  
5 exclude suspects from the crime as well as identify the perpetrator.

6 11. CODIS is the acronym for the Combined DNA Index System and is the  
7 generic term used to describe the Federal Bureau of Investigation (FBI)'s program support  
8 for criminal justice DNA databases as well as the software used to run these databases.  
9 The National DNA Index System or NDIS is considered one part of CODIS, the national  
10 level, containing DNA profiles contributed by federal, state, and local participating  
11 laboratories.

12 12. I submit that the requested saliva and buccal cell samples are necessary for  
13 analysis as well as evidentiary purposes. Such samples may also be used for analysis using  
14 more traditional scientific techniques. Samples taken from the suspect as described in  
15 **Attachment A-4** will be compared against the DNA profile found on the surfaces touched  
16 during the arson, a dismantled fire hose coupling and wye valve which was removed, and  
17 other items of interest recovered or identified during the course of the investigation. In  
18 removing the saliva and buccal cell samples from the **Target Subject**, investigators will  
19 use the least intrusive means possible by swabbing the interior of the mouth of the subject  
20 with a cotton swab.

#### 21 PROBABLE CAUSE

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

23 13. On July 12, 2020, at approximately 9:30 a.m., the NCIS Resident Agency  
24 office in San Diego, CA, became aware of a fire via multiple sources aboard the USS  
25 Bonhomme Richard (LHD-6) (hereinafter referred to as "BHR"). Commissioned in 1998,  
26 the BHR is a member of the Wasp-class, the US Navy's large-deck multipurpose  
27 amphibious assault ship. A total of eight Wasp-class ships were built. All eight ships were  
28 in active service prior to the fire onboard the BHR. Wasp-class LHDs embark, transport,

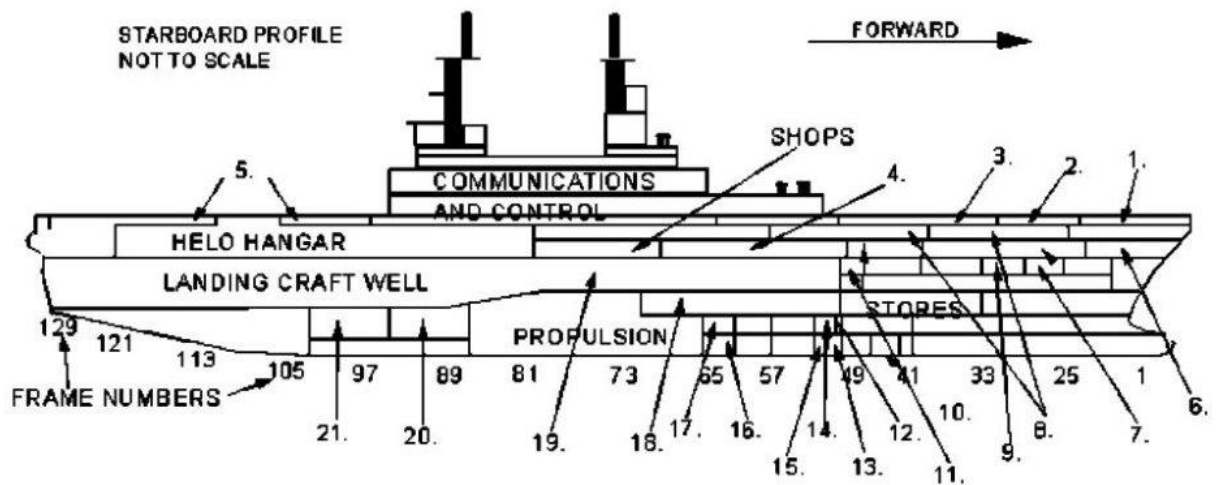
1 deploy, command and fully support all elements of a marine expeditionary unit (MEU) of  
2 2,000 marines, inserting forces ashore via helicopters, landing craft and amphibious  
3 vehicles. In addition to the 2,000 plus marines it can transport, the BHR has a crew of  
4 approximately 1,000 sailors.



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

20 15. Despite efforts to quickly extinguish the fire, the BHR burned for  
21 approximately five days. The fire damaged 470 spaces out of 1400. It has been reported  
22 that 71 individuals were injured during the firefighting efforts. On July 16, 2020, the BHR  
23 was deemed safe for temporary entry and Special Agents from NCIS and the Bureau of  
24 Alcohol, Tobacco, Firearms, and Explosives (ATF) made entry into the Lower V area in  
25 order assess the scene and determine if ATF's Nation Response Team (NRT) should be  
26 activated or if the scope of work could be handled with local resources. Subsequent to the  
27 assessment, ATF NRT was activated. On July 18, 2020, the NRT began to evaluate the  
28

1 damage in an effort to obtain the cause and origin of the fire aboard the BHR. The NRT  
2 processed the scene in the Lower V of the ship for several days.



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

### 12 *Arson Determination and Identification of Target Subject*

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

18 17. An ATF CFI employed a systematic approach and considered relevant data  
19 while conducting the origin and cause investigation. The systematic approach was based-  
20 on the scientific method, an organizational and analytical process suitable for fire scene  
21 investigations, which is also used in the physical sciences.

22 18. In order to determine the origin and cause of the fire, an ATF CFI had to  
23 ascertain where the fire started (origin) and the circumstances that brought about the fire  
24 (cause).

25 19. An ATF CFI examined the exterior of the BHR first and moved from areas  
26 of lesser damage to greater damage being mindful that the ship burned for several days.  
27 The fire damage observed on the exterior of the ship was consistent with a fire that  
28 originated inside and migrated out. The ATF CFI examined the interior of the BHR second

1 and determined the fire originated in the Lower V based-on fire damage observed,  
2 knowledge of fire dynamics and witness statements.

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

6 21. An ATF CFI considered competent ignition sources throughout the Lower V,  
7 e.g. electrical, mechanical, smoking, spontaneous heating and open flame as the cause of  
8 the fire. Ignition hypotheses were developed, tested and disproven, with the exception of  
9 open flame to available combustibles. Among other things, the progression and migration  
10 of the fire, coupled with the time in which a witness observed the **Target Subject** enter  
11 the Lower V (as discussed in detail below) and the report of smoke led the ATF CFI to  
12 classify the fire as incendiary<sup>1</sup>. The ATF CFI classified the fire as incendiary based on fire  
13 damage observed, his knowledge of fire dynamics, arc mapping results and information  
14 collected through witness statements. The ATF CFI subjected his origin and cause opinion  
15 to a technical review with other CFIs before rendering his final conclusion.

16 *Additional Evidence of Arson*

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

24 23. The next day, on July 21, 2020, upon returning to the scene, members of the  
25 ATF observed the plastic bottle was missing and the flagging tape with the same knot and  
26 loop used to mark the plastic bottle discarded on the floor. ATF immediately surveyed all

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

1 members of the NRT and other law enforcement individuals who were processing the  
2 Lower V. None of these officials removed the bottle from the flagging tape or the scene.  
3 Records checks by NCIS revealed that during the timeframe the plastic bottle with the  
4 small amount of liquid went missing, the **Target Subject's** duty section had been onboard  
5 the BHR providing him access to the ship and Lower V.

6 24. Investigators had recovered the other bottles and cans. The second plastic  
7 bottle had a melted cap attached and contained a small amount of liquid. A third plastic  
8 bottle had no cap, was twisted at its approximate center and contained a small amount of  
9 liquid. A fourth plastic bottle had a partially melted cap with a hole in the center attached  
10 and contained a small amount of liquid. Both of the aluminum cans were open; one  
11 contained a small amount of liquid. All of the aforementioned liquid samples were  
12 submitted to the ATF Forensic Science Laboratory for analysis. One liquid sample, which  
13 was associated with the second bottle, tested positive for a heavy petroleum distillate.  
14 Examples of heavy petroleum distillates include diesel, kerosene and jet fuel.

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

21 26. On July 22, 2020, Lieutenant Commander Felix Perez, the Damage Control  
22 Assistant (DCA), conducted a walk-through of the Upper and Lower V compartments  
23 with NCIS and ATF agents. Perez's duties as the DCA entail knowledge of, and  
24 responsibility for, all fire-fighting equipment and personnel aboard the BHR. Perez stated  
25 there were four fire-fighting stations within the Upper and Lower V areas. Perez noted  
26 three of the four fire-fighting stations were not in their normal configuration. One station  
27 located on the port side of the Upper V did not have any hoses connected to the fire-  
28 fighting station. Perez stated regardless of maintenance status, there should have been

1 hoses on the racks with at least one hose connected to the fire station per normal  
2 configuration. The fire station on the starboard side of the Upper V had one hose that was  
3 discovered cut during initial firefighting efforts and the second hose ran down the side of  
4 the BHR and appeared to be connected to diving equipment.

5       27. On July 22, 2020, Perez and the agents also inspected the fire station located  
6 at the bottom of the ramp in the Lower V. Perez noted while there were two hoses present  
7 on the racks, but not connected to the brass wye valve, he described the fire station as  
8 inoperable. Perez indicated the normal configuration would have a brass wye valve, which  
9 converts one stream of water from the fire main to two. The two valves could support two  
10 hoses, but in the ready position, one of the valves would have one hose connected to the  
11 one side of the wye valve with the other open in order to allow sailors to easily observe  
12 leaks from a faulty valve above. Perez noted there were no hoses or couplings connected  
13 to the fire station and a brass coupling to the wye valve laid on the deck directly below the  
14 fire station. Perez again emphasized that the station was not in its normal configuration.  
15 Perez also noted a fourth fire station in the Lower V which was located near the aft  
16 conflagration station was found in the normal configuration. Perez recalled an incident  
17 approximately four (4) months earlier at another location of the ship where a fire hose was  
18 found cut on the fire nozzle end with the fire nozzle missing.

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

27 //

28 //

*Additional Evidence **Target Subject** Committed the Arson*

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

30. On July 20, 2020, U.S. Sailor Seaman Kenji Velasco reported on July 12, 2002, at approximately 0805, while standing watch near the Lower V, he observed a “light-skin male” wearing clean coveralls, a facemask, carrying a silver/metal buck with both hands in front of his body descend into the Lower V; however, he did not identify the individual (the **Target Subject**). Velasco also stated that the **Target Subject** “hates” the U.S. Navy and the Fleet. Additionally, on July 21, 2020, Command Master Chief (“CMC”) Jose Hernandez also identified the **Target Subject** as a person who showed disdain towards authority and the U.S. Navy.

31. On July 21, 2020, Velasco was re-interviewed. Velasco stated that he was standing post at the Upper Vehicle Storage (Upper V) prior to the fire. This area is directly above Lower V. Velasco worked onboard the BHR in the Deck Department<sup>2</sup> and has extensive knowledge of the layout of the BHR. Velasco stated that he observed the **Target Subject** enter the “Lower V” area approximately 5 minutes before reports of white smoke. As he passed Velasco, the **Target Subject** carried a metal bucket in his hands by the bucket itself, rather than its handle, in front of his torso and sarcastically stated, “I love Deck.”<sup>3</sup> Velasco did not observe anyone else enter the Lower V area except the **Target Subject** before the fire started. Velasco and Boatswain’s mate Second Class (BM2) Beau

---

<sup>2</sup> A Navy ship’s Deck Department is in charge of a variety of ship functions, including: maintaining the exterior of the ship’s surfaces (e.g. rust removal and painting); anchoring and mooring the ship; manning the rescue and assistance lifeboats; and monitor underway replenishment.

<sup>3</sup> Being an undesignated Sailor (a sailor without a preassigned career specialization, e.g. corpsman or machinist’s mate) assigned to the Deck Department is generally considered a difficult and somewhat undesirable position, especially for someone who previously had aspirations to be a member of the Navy SEAL Teams (see below).

Benson were interacting at Velasco's post when Benson reported seeing white smoke. Benson nor Velasco reported seeing **Target Subject** leave the Lower V. Velasco stayed at his post until relieved by firefighting personnel and Benson departed to report seeing white smoke.

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

33. Initial checks of publically available social media web sites showed an Instagram post (depicted below) associated with the **Target Subject**, made on June 14, 2020, which stated, "I love the smell of napalm in the morning." Initial checks into the



**Target Subject'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, **Target Subject** changed his career goals to becoming a Navy SEAL, via completion of

1 the BUDS. The **Target Subject** started BUDS in approximately October 2019; however,  
2 five days after training began, **Target Subject** exercised his option out of training and  
3 “Dropped on Request,” known as a DOR. The DOR officially ended his pursuit of  
4 becoming a SEAL. After his DOR from the SEAL training program, the **Target Subject**  
5 was reassigned to BHR as an undesignated Seaman. According to Navy leadership, the  
6 morale and behavior of sailors who had aspired to become a SEAL, and then find  
7 themselves serving in a more traditional role on a Navy ship, are frequently very  
8 challenging.

9 34. A review of the **Target Subject**’s screening interview revealed that on July  
10 20, 2020, he participated in Duty Section Six screening interviews. In response to a  
11 question on the questionnaire, which asked how he learned about the fire; the **Target**  
12 **Subject** wrote that he was in the Hangar Bay<sup>4</sup> and saw black smoke. In response to a  
13 question that asked what time he learned of the fire; the **Target Subject** wrote the he  
14 found out at approximately 0830 that morning<sup>5</sup>. Another question asked if he was working  
15 or scheduled to work in the Lower V area the day of the fire; the **Target Subject** replied  
16 “No, I was suppose to clean the mooring [sic] stations.”<sup>6</sup>

17 35. Additionally, of all the individuals screened, the **Target Subject** was the only  
18 person who reported smelling “burning fuel/rubbery smell.” According to an investigating  
19 ATF CFI, the terminology the **Target Subject** used to describe the smell of the fire was  
20 consistent with items and materials that the ATF observed in the Lower V during their  
21 scene examination. In particular, the ATF CFI noted two forklifts had four rubber tires  
22 each. On each forklift, the two tires facing the starboard side of the BHR were burned and  
23 melted to varying degrees. The ATF CFI also indicated he observed ammunition carts that  
24

---

25 <sup>4</sup> Hangar bay is an area for storing/repairing aircraft, and additional equipment or supplies.

26 <sup>5</sup> This response is inconsistent with VELASCO’s observation of him entering the Lower  
27 V area around 0805, five minutes prior to the reports of smoke in the Lower V.

28 <sup>6</sup> A mooring station is an area of the ship used to secure a ship at a berth.

1 had hard-cast rubber wheels, which were also observed burnt to varying degrees.

2       36. The questionnaire also asked how individuals felt when they learned about  
3 the fire; the **Target Subject** reported that he felt a “small amount of adrenaline and  
4 anxiety.” During the screening process, the **Target Subject** reviewed his questionnaire  
5 with a NCIS special agent and stated that he had taken a picture of the fire with his cellular  
6 phone (**Subject Telephone**) after he exited the BHR.

7       37. Velasco also revealed there are conflagration stations<sup>7</sup> in the “Lower V”  
8 where an individual could leave the Lower V without going back up the ramp to the Upper  
9 V. Deck Department personnel are responsible for maintaining conflagration stations in  
10 Lower V. The Lower V contains two conflagration stations, one at the forward bulkhead  
11 and one at the aft bulkhead. Each conflagration station contained escape trunks with  
12 ladders that only go up out the Lower V. The escape trunks from each conflagration station  
13 open to a variety of locations within the ship.

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

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

23       40. On July 31, 2020, a NCIS agent went to the Lower V of the BHR to the aft  
24 conflagration station identified as 4-72-2-C, noted an open access door leading from the  
25 Lower V into the conflagration station and noted an additional door inside the  
26

---

27 <sup>7</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 conflagration station identified as 4-71-2 that was also open. This door led to an access  
2 trunk identified as 4-72-4-T which led to an access hatch in the same location as the one  
3 on the USS Boxer. The NCIS agent could not access the closed hatch as it was blocked by  
4 fire debris from above.

5 41. On July 22, 2020, CMC Hernandez was interviewed by NCIS and ATF  
6 agents and explained that, on July 5, 2020, the **Target Subject** was sleeping in his  
7 assigned berthing during his duty day. Although the **Target Subject** was allowed to have  
8 personnel items in the berthing area, the **Target Subject** was not allowed to be sleeping  
9 aboard or during the duty day. **Target Subject** was awoken by a contractor who was  
10 working near the **Target Subject's** sleeping area identified as rack twenty-seven in  
11 compartment 1-25-0-L. **Target Subject** reacted by verbally confronting the contractor in  
12 an aggressive way, causing the contractor to report the incident to Navy personnel.

13 42. On or about August 12, 2020, Chief Lino Aguilarbarron provided an oral  
14 sworn statement regarding his conversation with the **Target Subject** on an unknown date  
15 after the fire; where in the **Target Subject** told him he had been in the Lower V area the  
16 day before for the purpose of storing big hoses known as Replenishment At Sea (RAS)  
17 hoses. The **Target Subject** stated he did not see anything in the Lower V that would have  
18 ignited the fire by itself, more likely the fire was started by someone.

19 *DNA Collected*

20 43. Investigators swabbed items at the scene and items that were seized as  
21 evidence for DNA. The swabs were sent to the ATF crime laboratory for DNA analysis  
22 but the results are still pending.

23 *Identification of Subject Residence*

24 44. CMC Hernandez reported the **Target Subject's** address as the **Subject**  
25 **Residence** and provided a roster of all BHR sailors residing in Snyder Hall, Naval Base  
26 San Diego, CA. **Target Subject's** registered room is S1241B, the **Subject Residence**.

27 45. Additionally, utilizing 24-hour camera surveillance, NCIS personnel have  
28 observed **Target Subject** entering and exiting the **Subject Residence** multiple times.

1 Since August 06, 2020, NCIS personnel have observed **Target Subject** use a key card to  
2 gain access to **Subject Residence**.

3 *Identification of Subject Vehicle*

4 46. An investigator reviewed the results of a California Department of Motor  
5 Vehicles database query, which indicated the **Subject Vehicle** was registered to **Target**  
6 **Subject**.

7 47. NCIS personnel have observed **Target Subject** access, enter, and drive the  
8 **Subject Vehicle**.

9 *Identification of Subject Telephone*

10 48. **Target Subject** listed his telephone number as (606) 922-0727 (**Subject**  
11 **Telephone**) during his initial screening interview questionnaire.

12 49. CMC Hernandez provided a BHR command recall telephone roster. A review  
13 of the provided BHR's recall telephone roster confirmed that the **Target Subject** listed  
14 his telephone number as (606) 922-0727 (**Subject Telephone**).

15 50. NCIS personnel conducting surveillance observed **Target Subject**, carrying,  
16 walking with, and using a cellular telephone while driving.

17 *Identification of the Target Subject*

18 51. As discussed above, **Target Subject** was identified by eyewitness accounts  
19 of his activity and statements.

20 52. NCIS agents have reviewed **Target Subject's** personnel records, California  
21 Department of Motor Vehicle records and obtained information from command members  
22 of the BHR.

23 **BASIS FOR EVIDENCE SOUGHT IN SEARCH WARRANT**

24 53. Based on my training and experience, consultation with other agents and  
25 officers experienced in arson investigations, and all the facts and opinions set forth above  
26 in this affidavit, I know:

27 a. It is common for individuals who commit arsons to conduct research  
28 using personal computers, telephones, and other wireless devices, and evidence of such

1 search may be found in their residence, vehicles, or in their electronic media, to include  
2 cell phones, computers, and other electronic storage devices.

3           b. It is common for individuals who commit arson to store, dispose or  
4 conceal articles of clothing used during the commission of the crime in their homes,  
5 vehicles or trash receptacles.

6           c. It is common for individuals who have committed arson to research  
7 and collect news articles relating to the arsons, for several purposes, including monitoring  
8 law enforcement's investigation and response to the fire as well as gratification. I also  
9 know that evidence of such research and collection is commonly stored in their homes,  
10 vehicles and their electronic media, to include cell phones, computers, and other electronic  
11 storage devices.

12           d. Motivation for individuals committing arsons can be varied and  
13 complicated – such motivations may, among other things, include money, revenge,  
14 excitement, depression or anger. I also know that evidence of the individual's motivation  
15 to commit an arson may be found in their homes, vehicles, or electronic media, including  
16 cell phones, computers and other electronic storage devices.

17       54. Based on my training and experience, I know individuals typically access  
18 their email accounts or social media accounts through personal computers and smart  
19 phones, which they typically store or keep in their residences and vehicles.

20       55. I believe there is probable cause to believe that the **Subject Telephone** and  
21 other electronic storage devices such as a computer will contain communications like text  
22 messages and/or other electronic messaging in other formats or applications such as  
23 Instagram. Based on my training and experience, and my consultation with fellow agents,  
24 I know that even after an extended period of time, evidence of criminal activity can often  
25 be found on cell phones, computers and other electronic storage devices. Additionally, I  
26 know that it is reasonable to believe that such evidence may remain, even when the user  
27 has deleted the electronic data. For example, it is common for text message content to  
28 remain on wireless phones or a personal computer for an extended period of time, even

1 after an individual has deleted the messages. Even when a user deletes internet search  
2 history, such search history may frequently be found via a forensic examination of the  
3 phone or computer. Furthermore, cell phone users commonly back-up data from their  
4 wireless devices to their computer where such data may remain for an indefinite period of  
5 time and access social media applications such as Instagram via their telephone.

6 56. Based on my training and experience and consultation with individuals  
7 trained in computer forensics, I also believe that there is probable cause to believe that the  
8 **Subject Telephone** will contain historical GPS (Global Positioning System) or Wi-Fi  
9 data, which would be evidence of the location of the **Subject Telephone** on various times  
10 and dates.

11 PROCEDURES FOR ELECTRONICALLY STORED INFORMATION FOR  
12 CELLULAR TELEPHONES

13 57. It is not possible to determine merely by knowing the cellular telephone's  
14 make, model and serial number, the nature and types of services to which the device is  
15 subscribed and the nature of the data stored on the device. Cellular devices today can be  
16 simple cellular telephones and text message devices, can include cameras, can serve as  
17 personal digital assistants and have functions such as calendars and full address books and  
18 can be mini-computers allowing for electronic mail services, web services and  
19 rudimentary word processing. An increasing number of cellular service providers now  
20 allow for their subscribers to access their device over the internet and remotely destroy all  
21 of the data contained on the device. For that reason, the device may only be powered in a  
22 secure environment or, if possible, started in "flight mode" which disables access to the  
23 network. Unlike typical computers, many cellular telephones do not have hard drives or  
24 hard drive equivalents and store information in volatile memory within the device or in  
25 memory cards inserted into the device. Current technology provides some solutions for  
26 acquiring some of the data stored in some cellular telephone models using forensic  
27 hardware and software. Even if some of the stored information on the device may be  
28 acquired forensically, not all of the data subject to seizure may be so acquired. For devices

1 that are not subject to forensic data acquisition or that have potentially relevant data stored  
2 that is not subject to such acquisition, the examiner must inspect the device manually and  
3 record the process and the results using digital photography. This process is time and labor  
4 intensive and may take weeks or longer.

5 58. Following the issuance of this warrant, I will collect the **Subject Telephone**  
6 and subject it to analysis. All forensic analysis of the data contained within the telephones  
7 and their memory cards will employ search protocols directed exclusively to the  
8 identification and extraction of data within the scope of this warrant.

9 59. Based on the foregoing, identifying and extracting data subject to seizure  
10 pursuant to this warrant may require a range of data analysis techniques, including manual  
11 review, and, consequently, may take weeks or months. The personnel conducting the  
12 identification and extraction of data will complete the analysis within one-hundred twenty  
13 (120) days of the date the warrant is signed, absent further application to this Court.

14 60. After extraction of the data, law enforcement personnel will separate out  
15 relevant information as described in Attachment B-2. After the review is completed, non-  
16 relevant information (apparent innocent third party information) will be preserved with an  
17 evidence custodian but not accessed again post-review absent further authorization from  
18 the Court.

### 19 BIOMETRICS

20 61. This warrant further seeks authorization to permit law enforcement agents  
21 executing the warrant to compel the **Target Subject** to unlock the **Subject Telephone**  
22 believed to belong to him and located during the search, using biometric features. The  
23 grounds for this request are as follows:

24 a. I know from my training and experience, as well as from information  
25 found in publicly available materials published by device manufacturers, that most cellular  
26 phones, particularly newer models, offer their users the ability to unlock the device  
27 through biometric features in lieu of a numeric or alphanumeric passcode or password.  
28 These biometric features include fingerprint scanners, facial recognition features and iris

1 recognition features. Some devices offer a combination of these biometric features, and  
2 the user of such devices can select which features they would like to utilize.

3           b. If a device is equipped with a fingerprint scanner, a user may enable  
4 the ability to unlock the device through his or her fingerprints. For example, Apple offers  
5 a feature called “Touch ID,” which allows a user to register up to five fingerprints that can  
6 unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing  
7 the relevant finger to the device’s Touch ID sensor, which is found in the round button  
8 (often referred to as the “home” button) located at the bottom center of the front of the  
9 device. The fingerprint sensors found on devices produced by other manufacturers have  
10 different names but operate similarly to Touch ID.

11           c. If a device is equipped with a facial-recognition feature, a user may  
12 enable the ability to unlock the device through his or her face. For example, the most  
13 current model Apple iPhones include this feature, which allows the user to unlock the  
14 device by holding it in front of his or her face. The device’s front-facing camera then  
15 analyzes and records data based on the user’s facial characteristics. The device can then  
16 be unlocked if the front-facing camera detects a face with characteristics that match those  
17 of the registered face.

18           d. In my training and experience, users of electronic devices often enable  
19 the aforementioned biometric features because they are considered to be a more  
20 convenient way to unlock a device than by entering a numeric or alphanumeric passcode  
21 or password. Moreover, in some instances, biometric features are considered to be a more  
22 secure way to protect a device’s contents. This is particularly true when the users of a  
23 device are engaged in criminal activities and thus have a heightened concern about  
24 securing the contents of a device.

25           e. As discussed in this Affidavit, I have reason to believe that a cellular  
26 phone was being used by the **Target Subject** and there is probable cause the cellular  
27 phone will contain evidence of the Target Offenses. The passcode or password that would  
28 unlock any cellular phone believed to belong to the **Target Subject** subject to search under

1 this warrant currently is not known to law enforcement. Thus, law enforcement personnel  
2 may not otherwise be able to access the data contained within the phone absent the use of  
3 biometric features.

4 f. I also know from my training and experience, as well as from  
5 information found in publicly available materials including those published by device  
6 manufacturers, that biometric features will not unlock a cellular phone in some  
7 circumstances even if such features are enabled. This can occur when a device has been  
8 restarted, inactive, or has not been unlocked for a certain period of time. Thus, in the event  
9 law enforcement personnel encounter a locked cellular phone equipped with biometric  
10 features, the opportunity to unlock the device through a biometric feature may exist for  
11 only a short time.

12 g. Due to the foregoing, if law enforcement personnel encounter the  
13 cellular telephone believed to belong to the **Target Subject** that are subject to seizure  
14 pursuant to this warrant and may be unlocked using one of the aforementioned biometric  
15 features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers  
16 (including thumbs) of the **Target Subject**, present at the time of the search, to the  
17 fingerprint scanner of the phone found; and/or (2) hold the phone found on the **Target**  
18 **Subject's** person, in his backpack or in his vehicle, and believed to belong to the **Target**  
19 **Subject** in front of the face of the **Target Subject** and activate the facial recognition  
20 feature.

21 PROCEDURES FOR ELECTRONICALLY STORED INFORMATION FOR  
22 COMPUTERS AND OTHER ELECTRONIC MEDIA

23 62. With the approval of the Court in signing this warrant, agents executing this  
24 search warrant will employ the following procedures regarding computers, electronic  
25 storage devices, including electronic storage media, found at the **Subject Residence** and  
26 in the **Subject Vehicle**, which may contain data subject to seizure pursuant to this warrant:

27 //

28 //

*Forensic Imaging*

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

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

*Identification and Extraction of Relevant Data*

65. After obtaining a forensic image, the data will be analyzed to identify and extract data subject to seizure pursuant to this warrant. Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment and software. There are thousands of different hardware items and

1 software programs, and different versions of the same programs, that can be commercially  
2 purchased, installed, and custom-configured on a user's computer system. Computers are  
3 easily customized by their users. Even apparently identical computers in an office or home  
4 environment can be different with respect to configuration, including permissions and  
5 access rights, passwords, data storage, and security. It is not unusual for a computer  
6 forensic examiner to have to obtain specialized hardware or software, and train with it, in  
7 order to view and analyze imaged data.

8         66. Analyzing the contents of a computer or other electronic storage device, even  
9 without significant technical challenges, can be very challenging. Searching by keywords,  
10 for example, often yields many thousands of hits, each of which must be reviewed in its  
11 context by the examiner to determine whether the data is within the scope of the warrant.  
12 Merely finding a relevant hit does not end the review process for several reasons. The  
13 computer may have stored metadata and other information about a relevant electronic  
14 record – e.g., who created it, when and how it was created or downloaded or copied, when  
15 it was last accessed, when it was last modified, when it was last printed, and when it was  
16 deleted. Keyword searches may also fail to discover relevant electronic records, depending  
17 on how the records were created, stored, or used. For example, keywords search text, but  
18 many common electronic mail, database, and spreadsheet applications do not store data as  
19 searchable text. Instead, the data is saved in a proprietary non-text format. Documents  
20 printed by the computer, even if the document was never saved to the hard drive, are  
21 recoverable by forensic programs because the printed document is stored as a graphic  
22 image. Graphic images, unlike text, are not subject to keyword searches. Similarly, faxes  
23 sent to the computer are stored as graphic images and not as text. In addition, a particular  
24 relevant piece of data does not exist in a vacuum. To determine who created, modified,  
25 copied, downloaded, transferred, communicated about, deleted, or printed the data  
26 requires a search of other events that occurred on the computer in the time periods  
27 surrounding activity regarding the relevant data. Information about which user had logged  
28 in, whether users share passwords, whether the computer was connected to other

1 computers or networks, and whether the user accessed or used other programs or services  
2 in the time period surrounding events with the relevant data can help determine who was  
3 sitting at the keyboard.

4         67. It is often difficult or impossible to determine the identity of the person using  
5 the computer when incriminating data has been created, modified, accessed, deleted,  
6 printed, copied, uploaded, or downloaded solely by reviewing the incriminating data.  
7 Computers generate substantial information about data and about users that generally is  
8 not visible to users. Computer-generated data, including registry information, computer  
9 logs, user profiles and passwords, web-browsing history, cookies and application and  
10 operating system metadata, often provides evidence of who was using the computer at a  
11 relevant time. In addition, evidence such as electronic mail, chat sessions, photographs  
12 and videos, calendars and address books stored on the computer may identify the user at  
13 a particular, relevant time. The manner in which the user has structured and named files,  
14 run or accessed particular applications, and created or accessed other, non-incriminating  
15 files or documents, may serve to identify a particular user. For example, if an incriminating  
16 document is found on the computer but attribution is an issue, other documents or files  
17 created around that same time may provide circumstantial evidence of the identity of the  
18 user that created the incriminating document.

19         68. Analyzing data has become increasingly time-consuming as the volume of  
20 data stored on a typical computer system and available storage devices has become mind-  
21 boggling. For example, a single megabyte of storage space is roughly equivalent of 500  
22 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is  
23 roughly equivalent of 500,000 double-spaced pages of text. Computer hard drives are  
24 now being sold for personal computers capable of storing up to 2 terabytes (2,000  
25 gigabytes) of data. And, this data may be stored in a variety of formats or encrypted  
26 (several new commercially available operating systems provide for automatic encryption  
27 of data upon shutdown of the computer). The sheer volume of data also has extended the  
28 time that it takes to analyze data. Running keyword searches takes longer and results in

1 more hits that must be individually examined for relevance. And, once reviewed, relevant  
2 data leads to new keywords and new avenues for identifying data subject to seizure  
3 pursuant to the warrant.

4 69. Based on the foregoing, identifying and extracting data subject to seizure  
5 pursuant to this warrant may require a range of data analysis techniques, including hashing  
6 tools to identify data subject to seizure pursuant to this warrant, and to exclude certain  
7 data from analysis, such as known operating system and application files. The  
8 identification and extraction process, accordingly, may take weeks or months. The  
9 personnel conducting the identification and extraction of data will complete the analysis  
10 within one-hundred twenty (120) days of this warrant, absent further application to this  
11 court.

12 70. All forensic analysis of the imaged data will employ search protocols directed  
13 exclusively to the identification and extraction of data within the scope of this warrant.

14 71. After extraction of the data, law enforcement personnel will separate out  
15 relevant information as described in Attachment B-1. After the review is completed, non-  
16 relevant information (apparent innocent third party information) will be preserved with an  
17 evidence custodian but not accessed again post-review absent further authorization from  
18 the Court.

19 *Genuine Risks of Destruction*

20 72. Based upon my experience and training, and the experience and training of  
21 other agents with whom I have communicated, electronically stored data can be  
22 permanently deleted or modified by users possessing basic computer skills. In this case,  
23 only if the subject receives advance warning of the execution of this warrant, will there be  
24 a genuine risk of destruction of evidence.

25 *Prior Attempts to Obtain Data*

26 73. To date, the United States has attempted to obtain data that may also be  
27 contained on **Target Subject's** personal computer(s) by accessing **Target Subject's**  
28 military account(s) and seizing government computers assigned to the BHR. Analysis of

1 the computers and **Target Subject's** military account have not been completed.

2 REQUEST FOR SEALING

3 74. This affidavit outlines an ongoing criminal investigation, the disclosure of  
4 this affidavit and warrant may adversely affect the prosecution and investigation of law  
5 enforcement. Specifically, there is reason to believe that disclosure of the affidavit and  
6 warrant will result in destruction of or tampering with evidence or otherwise seriously  
7 jeopardize the investigation. Even after the search warrants sought are executed on the  
8 **Subject Properties** and **Target Subject**, the breadth of the investigation will not be  
9 known to the **Target Subject** and any associates or co-conspirators involved in the arson.  
10 Disclosure of the information contained in this affidavit may still affect the integrity of  
11 the investigation and result in the destruction of or tampering with evidence.

12 //

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

CONCLUSION

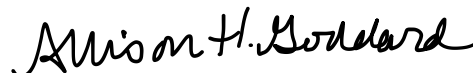
75. Based on the foregoing, I believe there is probable cause to believe items that constitute evidence of violations of federal criminal law, namely, 18 U.S.C. Sections 81 (Arson within special maritime and territorial jurisdiction) and 844(f) (Use of fire to damage federal property), and that evidence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

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



Albert Porter  
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 14th day of August, 2020.



HON. ALLISON H. GODDARD  
United States Magistrate Judge

**ATTACHMENT A-3**

DESCRIPTION OF THE CELLULAR TELEPHONE TO BE SEARCHED

A cellular telephone with the assigned telephone number (606) 922-0727 and utilizing AT&T as its service provider (“**Subject Telephone**”).

**ATTACHEMNT B-3**

**ITEMS SUBJECT TO SEIZURE**

The evidence to be seized from the cellular phone will be electronic records, communications, and data such as emails, text messages, photographs, audio files, videos, and location data, for the period from **June 1, 2020** to and including the day the cellular phone is seized pursuant to this warrant:

a. tending to identify the user of, or persons with control over or access to the **Subject Vehicle** and **Subject Telephone**;

b. tending to identify travel to and from, or presence aboard the USS Bonhomme Richard on July 12, 2020 and July 20, 2020;

c. 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; and

d. tending to identify or explain a motivation to commit arson aboard the USS Bonhomme Richard; and/or

e. 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;

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

The seizure and search of the cellular phone(s) shall follow the procedures outlined in the supporting affidavit. Deleted data, remnant data, slack space, and temporary and permanent files on the cellular phone(s) may be searched or the evidence above.

During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of Ryan Sawyer MAYS onto the fingerprint sensor of the **Subject Telephone**, located pursuant to this warrant, in order to gain access to the contents of any such device. In addition, law enforcement personnel are authorized

1 to hold any cellular phone(s) believed to belong to MAYS, located pursuant to this  
2 warrant, in front of the face of MAYS in order to gain access to the contents of any such  
3 device via facial recognition.