UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A RESIDENCE LOCATED AT [redacted] A RECREATIONAL VEHICLE [redacted] PARKED AT [redacted] A BLACK TRAILER [redacted] AND A CELL PHONE CURRENTLY BEING USED BY JEREMY BROWN UNDER RULE 41

Case No. 21-sw-315

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

See Attachment A (incorporated by reference)

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

See Attachment B (incorporated 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 U.S.C. §§ 371 (conspiracy); 231(a)(2) (transport of firearms or explosives for use in civil disorder); 844(a)(2) (transportation of explosives) and 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds).	

The application is based on these facts:

See attached Affidavit (incorporated 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.

Katie M Hill

Applicant's signature

Katie Hill, Special Agent, FBI

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: 09/29/2021

Zia M. Faruqui
2021.09.29 19:35:42 -04'00'

Judge's signature

City and state: Washington, D.C.

Zia M. Faruqui, U.S. Magistrate Judge

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of)
(Briefly describe the property to be searched or identify the person by name and address)) Case No. 21-sw-315
A RESIDENCE LOCATED AT [redacted] A RECREATIONAL VEHICLE [redacted] PARKED AT [redacted] A BLACK TRAILER [redacted] AND A CELL PHONE CURRENTLY BEING USED BY JEREMY BROWN UNDER RULE 41)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Middle District of Florida
(identify the person or describe the property to be searched and give its location):

See Attachment A (incorporated by reference)

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

See Attachment B (incorporated by reference)

YOU ARE COMMANDED to execute this warrant on or before October 13, 2021 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Zia M. Faruqui, U.S. Magistrate Judge .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of .

Date and time issued: 09/29/2021

Zia M. Faruqui
2021.09.29 19:36:09 -04'00'
Judge's signature

City and state: Washington, D.C. Zia M. Faruqui, U.S. Magistrate Judge
Printed name and title

Return

Case No.: 21-sw-315	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

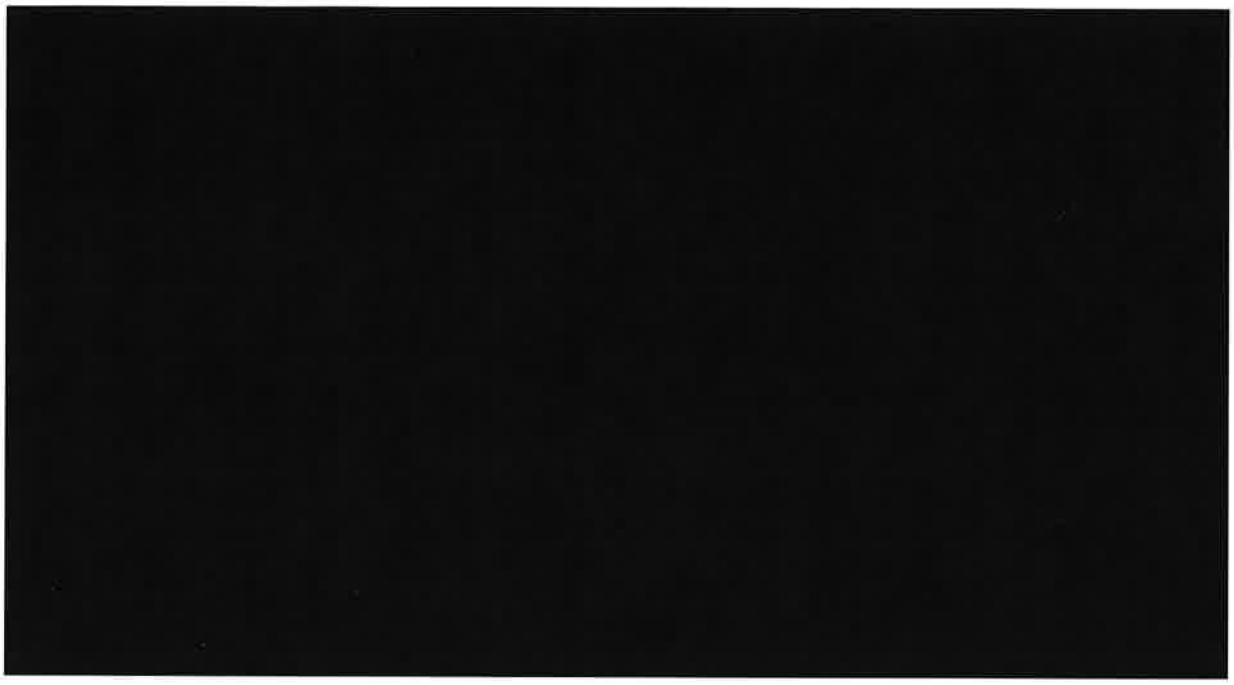
ATTACHEMENT A

PREMISES TO BE SEARCHED

The property and curtilage to be searched is [redacted] located in the Middle District of Florida, further described as a single-story residence located at the corner of [redacted]. The residence is a [redacted]. Next to the front door [redacted] is affixed to the mailbox.

Photograph

Map

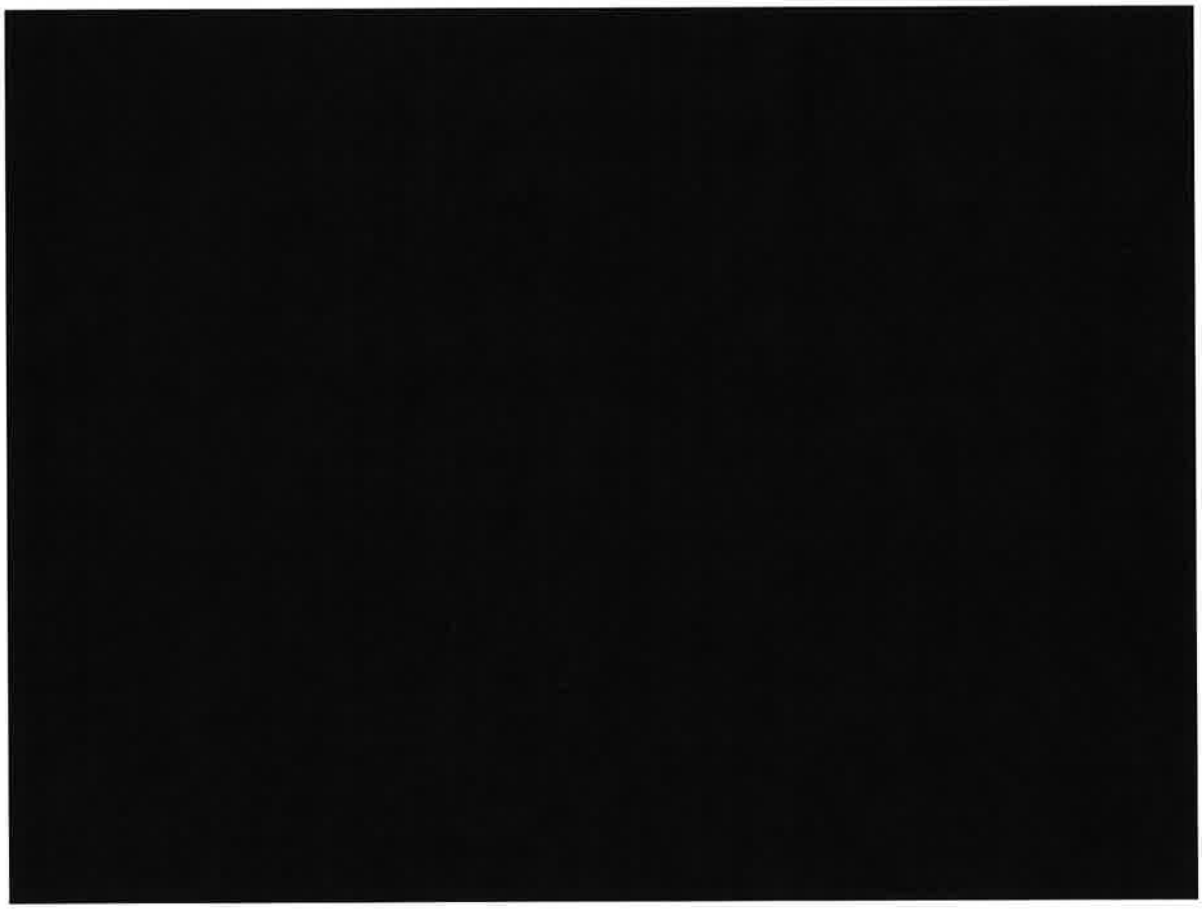


ATTACHEMENT B

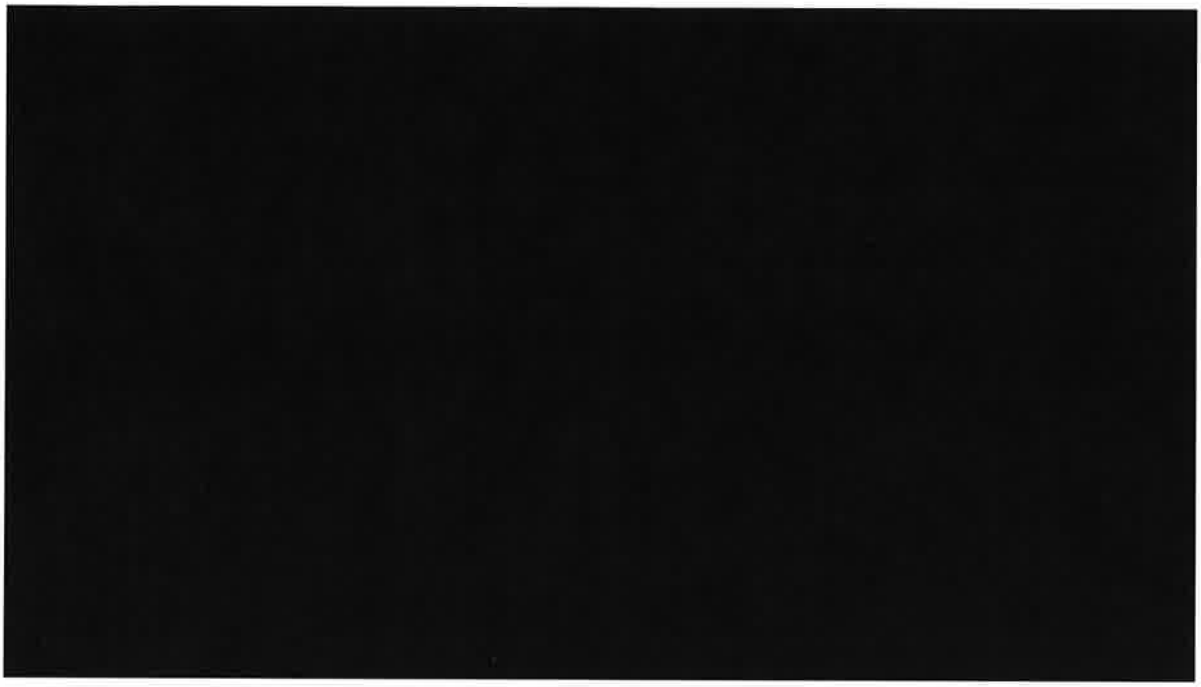
PREMISES TO BE SEARCHED

A recreational vehicle parked at [redacted] located in the Middle District of Florida, registered to [redacted]

Photograph



Map

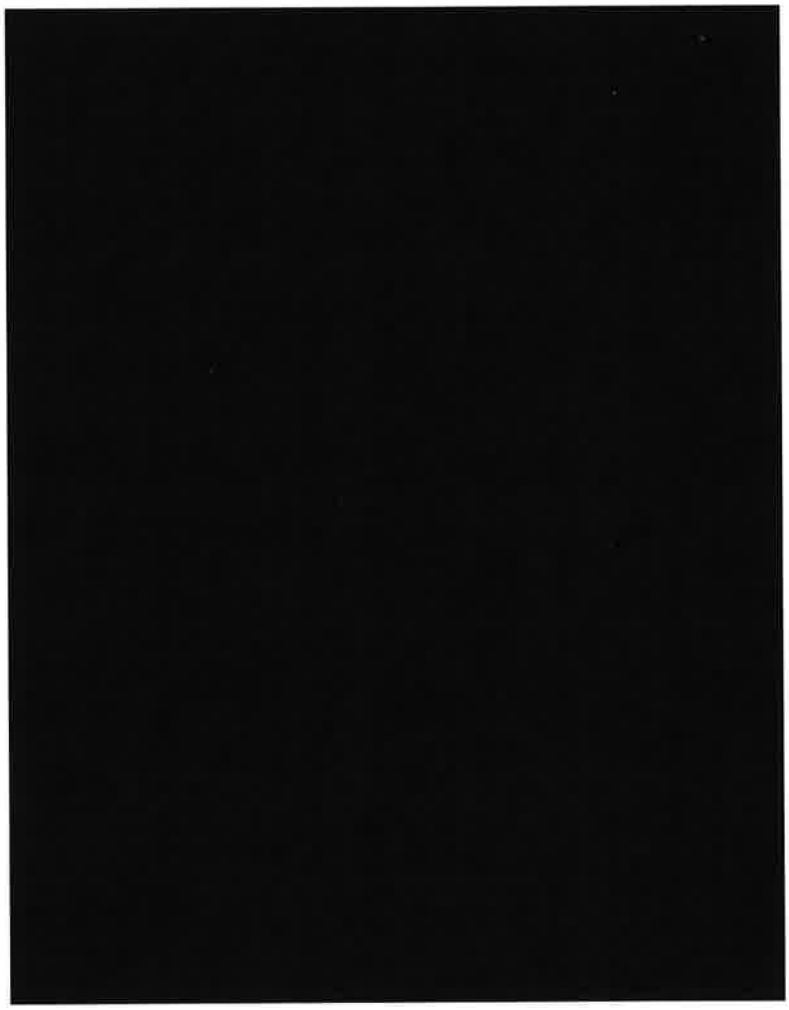


ATTACHEMENT C

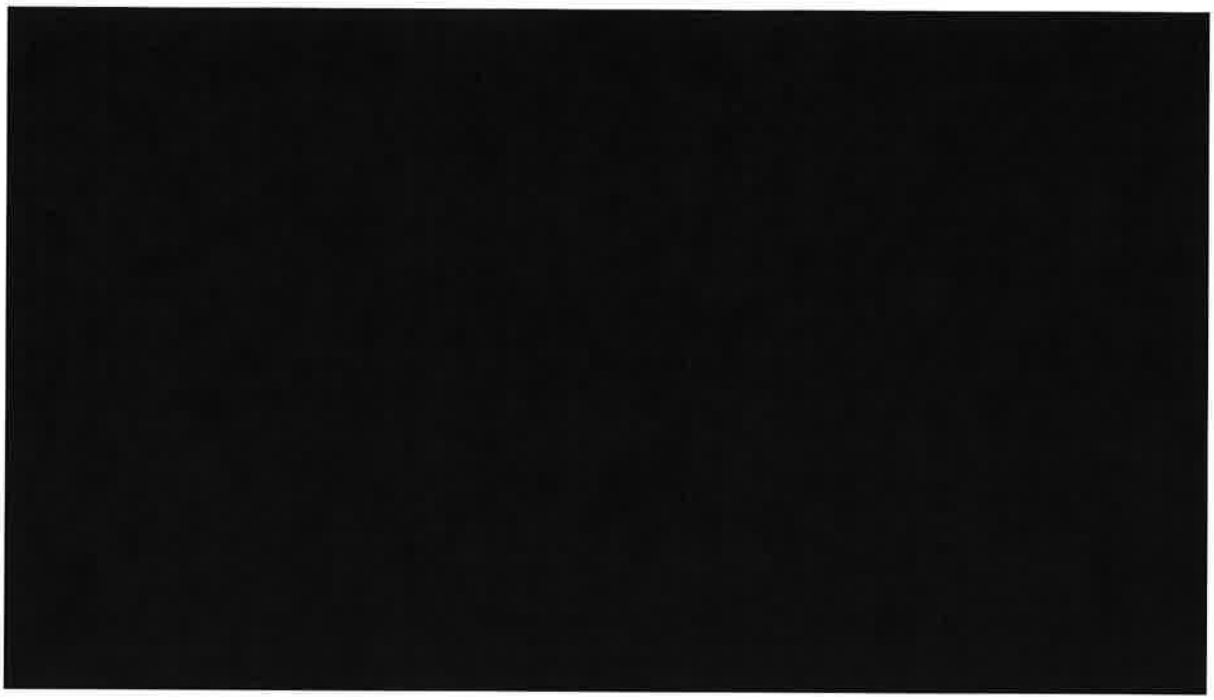
PREMISES TO BE SEARCHED

A black trailer parked at [redacted] located in the Middle District of Florida, registered to [redacted]

Photograph



Map



ATTACHMENT D

Property to be searched

The property to be searched is a cellular phone (the "**TARGET PHONE**") associated with phone number [redacted] which is to be seized from the person of Jeremy Brown (born on [redacted], vicinity of Jeremy Brown, or locations listed in Attachments A, B, and C within the state of Florida.

ATTACHMENT E

Property to be seized

1. All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 USC 371 (conspiracy); 18 USC 231(a)(2) (transport of firearms or explosives for use in civil disorder); 18 USC 844(a)(2) (transportation of explosives) and 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds) (the "Subject Offenses") that have been committed by BROWN and/or other identified and unidentified persons, as described in the affidavit submitted in support of this Warrant, including:

   a. Records and information that constitute evidence of use, control, ownership, or occupancy of the PREMISES and things therein;

   b. Evidence of the Subject Offenses, to include clothing, protective/tactical gear worn during the offenses, as described and depicted in the attached affidavit, and firearms, explosives, precursor materials, other weapons and cases to hold or transport weapons or explosives, and instructions or documents showing an intent to obtain, manufacture, or employ weapons or explosives;

   c. records and information concerning:

      i. the identification of BROWN and other persons, including photographs and videos depicting clothing and other articles and paraphernalia that reflect evidence of having been present at or near the U.S. Capitol Building on or around January 6, 2021;

      ii. the identification of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the SUBJECT

OFFENSES; or (ii) communicated about matters relating to the SUBJECT OFFENSES, including records that help reveal their whereabouts;

iii. the U.S. Capitol Building, including any maps or diagrams of the Building or its internal offices, or presence at, or inside of or on the grounds of, the Building on or around January 6, 2021, including any planning, preparation, or travel;

iv. challenges to or questions about the legitimacy of the 2020 Presidential Election, including awareness of, or any efforts or intent to disrupt, the certification process of the 2020 Presidential Election, or otherwise influence the policy or composition of the United States government by intimidation or coercion;

v. materials, devices, tools, plans, or strategies to enter or assist others in entering the U.S. Capitol Building on or about January 6, 2021, by deceit or by force, including weapons and elements used to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;

vi. communication devices, including closed circuit radios, walkie-talkies, or secure or encrypted "apps," related to the directing of others or direct presence at, inside of, or on the grounds of, the U.S. Capitol Building on or around January 6, 2021;

vii. any conspiracy, planning, or preparation to commit the SUBJECT OFFENSES, or efforts to conceal evidence of the SUBJECT OFFENSES

from law enforcement, or to flee prosecution for the SUBJECT OFFENSES;

viii. the state of mind of BROWN and/or co-conspirators, *e.g.*, intent, absence of mistake, or evidence indicating preparation, planning, knowledge, or experience, including but not limited to tactical training or tactical equipment, related to the SUBJECT OFFENSES;

ix. affiliation or communication with the Oath Keepers, including members thereof.

2. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device(s)":

a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);

e. evidence of the times the Device(s) was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);

g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);

h. records of or information about Internet Protocol addresses used by the Device(s);

i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

4. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

5. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-

ROMs, and other magnetic or optical media.

6. The United States government will conduct a search of the property described in Attachment A-D and determine which information is within the scope of the information to be seized specified above. That information that is within the scope of this warrant may be copied and retained by the United States.

7. Law enforcement personnel will then seal any information from the property searched that does not fall within the scope of this warrant and will not further review the information absent an order of the Court. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.

8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

9. During the execution of the search of the PREMISES described in Attachment A-D, law enforcement personnel are also specifically authorized to obtain from BROWN (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access

subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned persons' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

(a) any of the Device(s) found at the PREMISES,

(b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

10. While attempting to unlock the Device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make

clear that providing any such information is voluntary and that the person is free to refuse the request.

PART II – INFORMATION AND DATA TO BE SEIZED FROM THE DEVICES

The following records and information located on the Devices and related to violations of 18 U.S.C. §§ 371 (conspiracy); and 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds); (the "Subject Offenses") that have been committed by BROWN and/or other identified and unidentified persons, including:

a. The records and information described in Part I, above, in any electronic form;

b. Evidence of who used, owned, or controlled the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, "chat," instant messaging logs, photographs, and correspondence;

c. Evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. Evidence of the lack of such malicious software;

e. Evidence indicating how, when, and where the Devices were accessed or used to determine the chronological context of device access, use, and events relating to crime under investigation and to the Devices user;

f. Evidence indicating the Devices user's state of mind as it relates to the crime under investigation;

g. Evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;

h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Devices;

i. Documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices;

j. Records of or information about Internet Protocol addresses used by the Devices;

k. Records of or information about the Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

l. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF A RESIDENCE LOCATED AT [redacted] A RECREATIONAL VEHICLE [redacted] PARKED AT [redacted] A BLACK TRAILER [redacted] AND A CELL PHONE CURRENTLY BEING USED BY JEREMY BROWN UNDER RULE 41	**SW No. 21-sw-315**

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR A SEARCH WARRANT

Your affiant, Katie Hill, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your affiant is a Special Agent with the Federal Bureau of Investigation ("FBI"), and, as such, am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C). Your affiant joined the FBI as a Special Agent in August 2009. Your affiant is currently assigned to the FBI's Tampa Division Joint Terrorism Task force ("JTTF"). Your affiant's official duties include, but are not limited to, investigating individuals and groups who have committed violations of federal laws, including federal laws related to threats, international terrorism, and domestic terrorism. As a special agent, your affiant has participated in numerous investigations and have executed both arrest and search warrants. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

2. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 USC 371 (conspiracy); 18 USC 231(a)(2) (transport of firearms or explosives for use in civil disorder); 18 USC 844(a)(2) (transportation of explosives) and 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds) (the "Subject Offenses") have been committed by JEREMY BROWN and/or other identified and unidentified persons. In addition, there is probable cause to believe that evidence of these crimes will be found within the Middle District of Florida at the following locations (collectively "the **Premises**"):

- The residence (the "**Residence**" further described in Attachment A) that BROWN currently resides in located at [redacted]
- The recreation vehicle [redacted] (the "**RV**" further described in Attachment B) that is parked at [redacted]
- A black trailer [redacted] (the "**Trailer**" further described in Attachment C) that is parked at [redacted]
- a cell phone associated with the phone number [redacted] (the "**TARGET PHONE**" further described in Attachment D) currently being used by BROWN.

JURISDICTION

3. Although the PREMISES are located outside this district, this Court has jurisdiction under Federal Rule 41(b)(3) because this is an investigation of domestic terrorism as that term is defined in Title 18, U.S.C. Section 2331(5)(b):

> [T]he term "domestic terrorism" means activities that- (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended- (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States.

18 U.S.C. § 2331(5).

PROBABLE CAUSE

Background

4. The US Capitol Police (USCP), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 on January 6, 2021.

The 2020 United States Presidential Election and the Official Proceeding on January 6, 2021

5. The 2020 United States Presidential Election occurred on November 3, 2020.

6. The United States Electoral College is a group required by the Constitution to form every four years for the sole purpose of electing the president and vice president, with each state appointing its own electors in a number equal to the size of that state's Congressional delegation.

7. On December 14, 2020, the presidential electors of the U.S. Electoral College met in the state capital of each state and in the District of Columbia and formalized the result of the 2020 U.S. Presidential Election: Joseph R. Biden Jr. and Kamala D. Harris were declared to have won sufficient votes to be elected the next president and vice president of the United States.

8. On or about December 19, 2020, President Donald J. Trump tweeted, "Statistically impossible to have lost the 2020 Election. Big protest in D.C. on January 6th. Be there, will be wild!"

9. On January 6, 2021, a Joint Session of the United States House of Representatives and the United States Senate ("the Joint Session") convened in the United States Capitol building (the "Capitol" or the "U.S. Capitol") to certify the vote of the Electoral College of the 2020 U.S. Presidential Election (the "Certification").

Criminal Activity Before the Riot

10. Based on my knowledge, training, and experience, I know that participants in the kinds of criminal activities described herein tend to, and often did here, take certain preparatory steps before committing their crimes, including: researching and purchasing materials and supplies such as burner phones, tactical vests and helmets, and weapons including bear spray, pepper spray, asps (police batons), guns and ammunition, and zip tie restraints; mapping and reconnoitering the location of the planned crime and possible entry and escape routes, including checking for surveillance cameras and other potential security surrounding such locations; training in how to use their weapons and other tools and techniques involved in their planned criminal activity; and organizing with other co-conspirators on social media and elsewhere for planned travel and methods of attack.

11. Beginning after the election in November 2020, text and other communications show that some groups of subjects planned and attended military-style training in preparation for opposing the results of the election. Multiple groups that forcibly entered the Capitol appeared to consist of individuals who had coordinated their actions. Some groups at the riot included members who dressed in similar uniforms with the same insignia, and members of some groups

can be heard on video giving and following instructions. Based on my training and experience, and this investigation, these groups' manner of dress, movements, and communication demonstrate that they had prepared together. Furthermore, the movement of these groups within the Capitol demonstrates an intent to, among other things, oppose by force Congress's authority, and to prevent, hinder, or delay the execution of the Joint Session's legal responsibilities.

12. Beginning in December 2020, using social media, text messaging, and messaging applications, subjects planning to participate in the riot sent incendiary messages aimed at recruiting as large a following as possible to go to Washington, D.C. to interfere with the official Congressional proceeding on January 6, 2021. This investigation has shown that many of the subjects of this investigation came from out of state and coordinated using social media, text messaging, and messaging applications on their cell phones.

13. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the U.S. Capitol wearing what appears to be, based upon my training and experience, tactical vests and helmets. The common equipment and paraphernalia that groups inside and outside the Capitol possessed, such as bear spray, eye protection, tactical vests, and helmets, are evidence of some prior agreement among individuals to engage in the conduct described herein.

The Riot at the U.S. Capitol on January 6, 2021

14. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of

open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All this area was barricaded and off limits to the public on January 6, 2021.

15. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

16. On January 6, 2021, the area of the U.S. Capitol grounds was established as a restricted area. This restricted area consisted of both permanent and temporary security barriers as well as posts manned by USCP to include bike racks. The restricted area was bounded to the north of the U.S. Capitol along Constitution Avenue; to the south of the U.S. Capitol along Independence Avenue; to the west of the U.S. Capitol along the eastern side of First Street; and, on the east side of the U.S. Capitol, between the East Front and the grassy areas located between the Plaza and First Street. Within the grassy area, a designated area for media was restricted by bike racks. This bounded area is hereinafter referred to as the "Restricted Grounds." People could lawfully be on the Capitol grounds outside of the Restricted Grounds including on the East Front, east of the bike racks along the Capitol Plaza, including all of the grassy areas on the East Front.

17. Within the West Front of the Restricted Grounds were additional temporary barriers due to preparations and ongoing construction for the Presidential Inauguration including perforated green plastic sheeting attached to stakes at regular intervals, known as snow fencing, and signage stating "Area Closed by order of the United States Capitol Police Board." The exterior plaza of the U.S. Capitol was also closed to members of the public.

18. A map of the area of the U.S. Capitol showing the Restricted Grounds is below, the red line marks the police line at the edges of the Restricted Grounds:

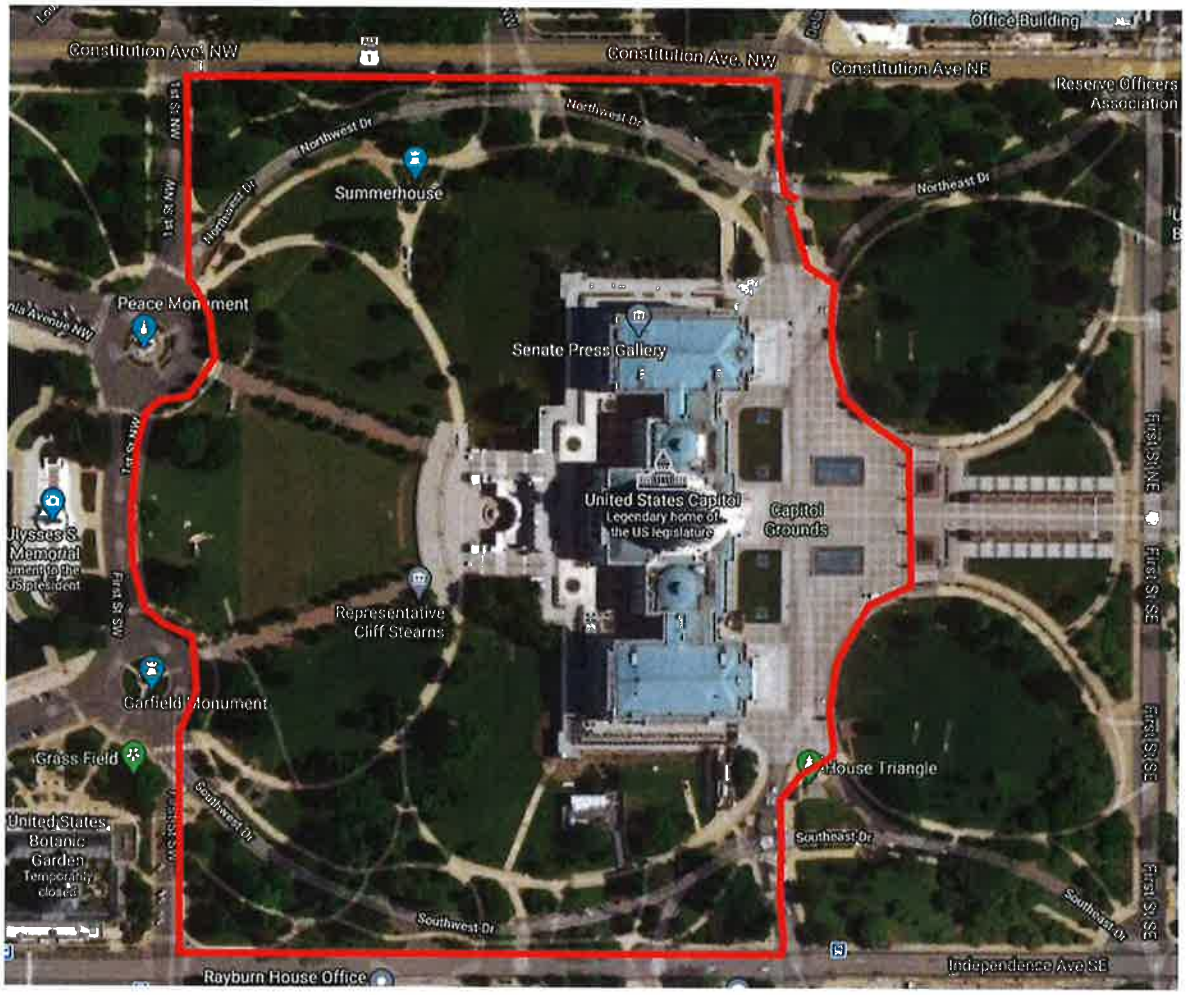


Figure 2: Restricted Grounds around the U.S. Capitol on January 6, 2021.

19. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020. The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m., the House and Senate

adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

20. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and USCP were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

21. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

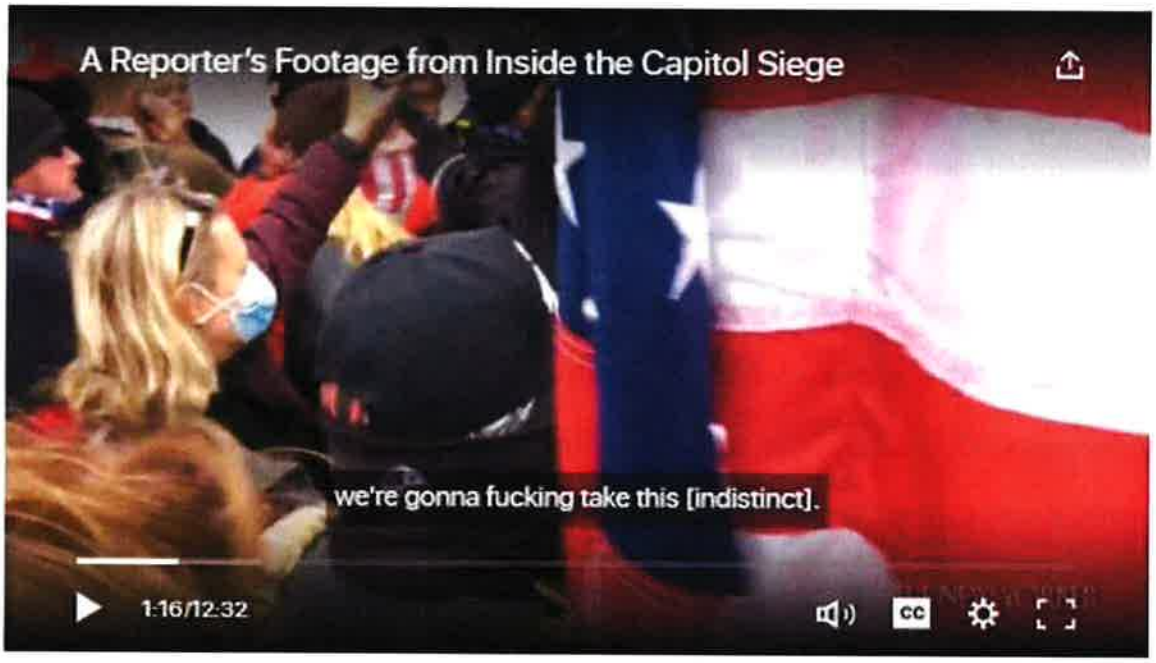
22. At around 1:30 p.m. EST, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby.

23. Media reporting showed a group of individuals outside of the Capitol chanting, "Hang Mike Pence." I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

24. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by U.S. Capitol Police Officers or other authorized security officials. At such time, the

certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

25. Shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown individual saying to a crowd outside the Capitol building, "We're gonna fucking take this," which your affiant believes was a reference to "taking" the U.S. Capitol.



26. Multiple groups that forcibly entered the Capitol appeared to consist of individuals who had practiced and/or coordinated their actions. For example, some groups included members who dressed in similar uniforms with the same insignia, and members of some groups can be heard on video giving and following instructions. Based on my training and experience, and this investigation, these groups' manner of dress, movements, and communication demonstrate that

they had prepared together. In addition, the equipment and paraphernalia that groups inside and outside the Capitol possessed, such as bear spray, eye protection, and helmets, are evidence of some prior agreement among individuals to engage in the conduct described herein. Finally, the movement of these groups within the Capitol demonstrates an intent to, among other things, oppose by force Congress's authority and to prevent, hinder, or delay the execution of the Joint Session's legal responsibilities

27. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As the subjects attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement was forced to draw their weapons to protect the victims sheltering inside.

28. At approximately 2:30 p.m. EST, known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on both the west side and the east side of the building. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured and several were admitted to the hospital.

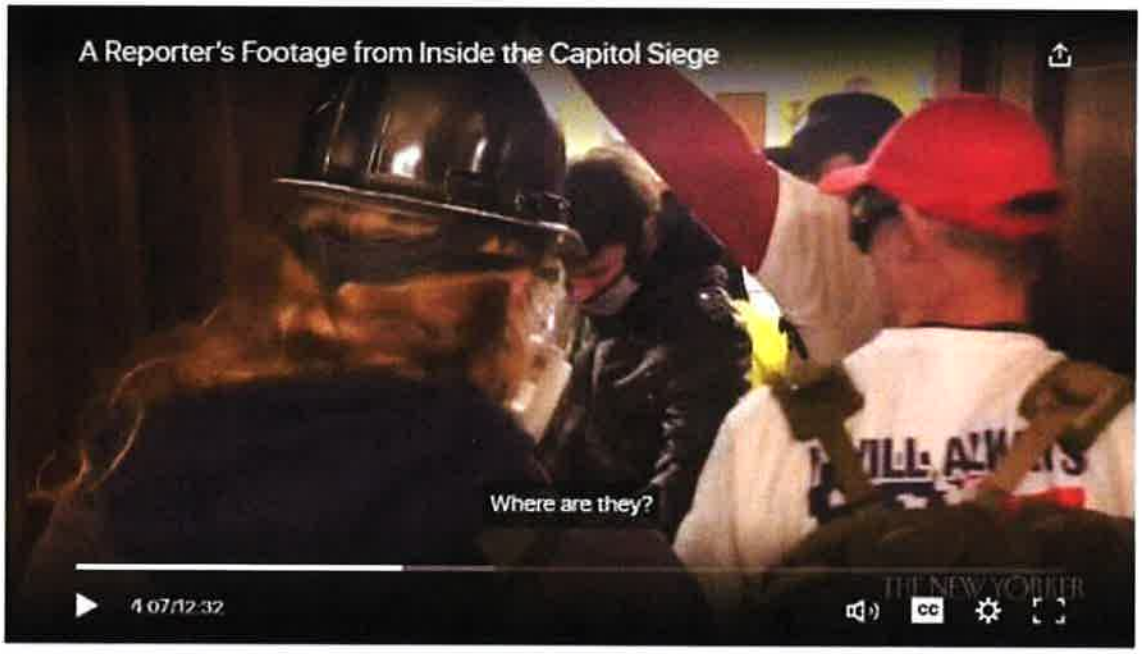
29. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and Tasers. They also took police equipment from overrun police including shields and police batons and used them against law enforcement officers trying to protect the U.S. Capitol and the people who were legitimately inside it. At least one of the subjects carried a handgun with

an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

30. Also, at approximately 2:30 p.m. EST, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

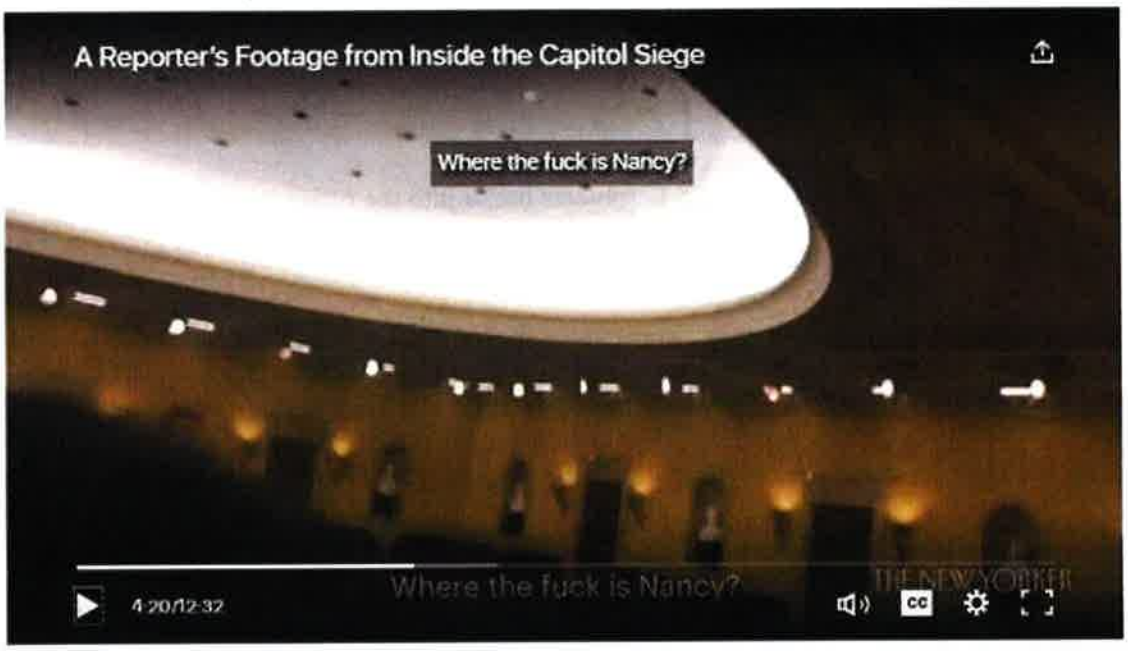
31. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

32. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video on the news media website of The New Yorker shows an individual asking, "Where are they?" as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word "they" is in reference to members of Congress.

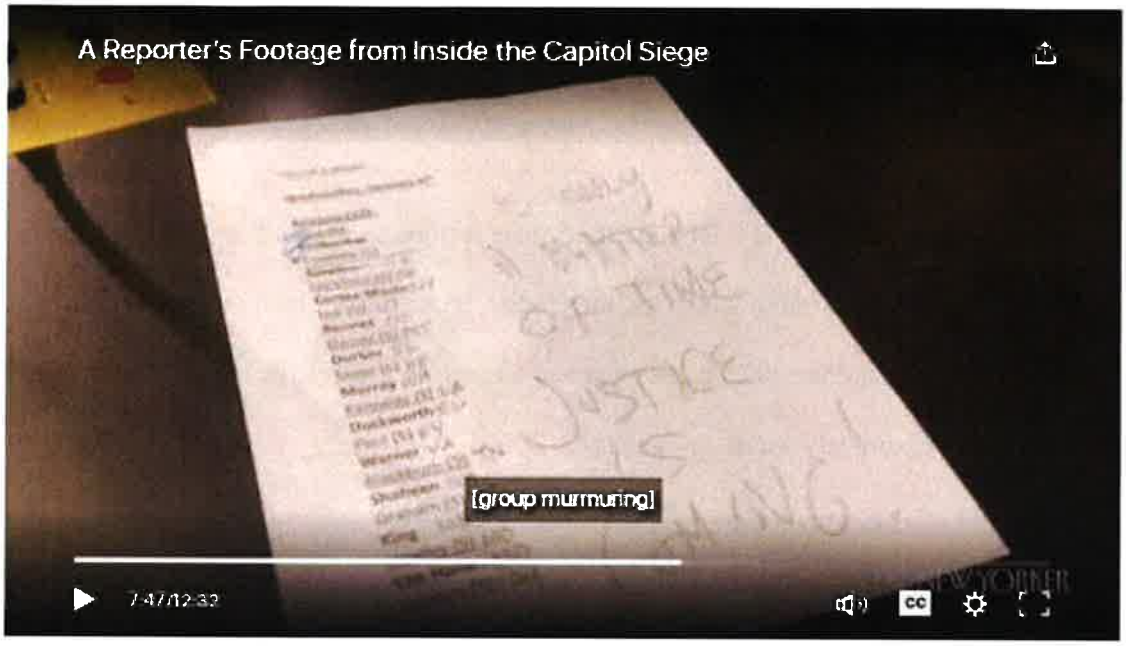


33. After subjects forced entry into the Senate Chamber, the same publicly available video shows that an individual asked, "Where the fuck is Nancy?" Based upon other comments

and the context, law enforcement believes that the "Nancy" being referenced was the Speaker of the House of Representatives, Nancy Pelosi.



34. A subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter on the same video, stated, "Its Only A Matter of Time Justice is Coming."



35. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m.

36. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

37. At around 4:52 p.m. EST, at a staging area for the media set up outside of the U.S. Capitol building on the east side, unknown subjects assaulted members of the media and stole and destroyed equipment owned by various members of the media and media companies.

38. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

39. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at

approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

40. Beginning around 8:00 p.m., the Senate resumed work on the Certification.

41. Beginning around 9:00 p.m., the House resumed work on the Certification.

42. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3 a.m. on January 7, 2021.

Cell Phone Usage at the Riot

43. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there. Subjects also posted comments, pictures, and video before, during, and after breaching the Capitol grounds and the Capitol building.

44. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to coordinate with other participants at the gatherings, to communicate with other individuals about the gatherings, to allow individuals to capture photographs and video footage of the gatherings, and to post on social media and digital forums about the gatherings. Nearly every phone is internet equipped and allows individuals to access the internet, including Google.

45. Many subjects, including those detailed below, seen on news footage in the area of the U.S. Capitol were using a cell phone in some capacity. Based on my participation in this investigation, I know some subjects were recording the events occurring in and around the U.S.

Capitol and others took photos, to include photos and video of themselves after breaking into the U.S. Capitol itself. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

46. Photos available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos.

47. In addition, organized groups within the rioters used social media, text messaging, and messaging applications and other apps on their cell phones to plan and coordinate their activities before, during, and after the riot. As described further below, Oath Keepers and individuals associated with the Oath Keepers engaged in substantial use of internet connected cellular devices during the riots of January 6, 2021.

Criminal Activity After the Riot

48. Following the riot, many subjects posted pictures, video, and texts showing and describing their participation in the riot. These included selfies and videos apparently taken with their personal cell phones. Many of these posts were subsequently deleted. I know from my knowledge, training, and experience that people who commit criminal acts will often delete such information in an attempt to thwart any subsequent criminal investigation. Some subjects subsequently fled their homes and went into hiding.

Facts Specific to This Application

The Oath Keepers Militia

49. Law enforcement and news-media organizations observed that members of an organization known as the Oath Keepers were among the individuals and groups who forcibly entered the Capitol on January 6, 2021. The Oath Keepers are a large but loosely organized collection of individuals, some of whom are associated with militias. Some members of the Oath Keepers believe that the federal government has been coopted by a cabal of elites actively trying to strip American citizens of their rights. Though the Oath Keepers will accept anyone as members, they explicitly focus on recruiting current and former military, law enforcement, and first-responder personnel. The organization's name alludes to the oath sworn by members of the military and police to defend the Constitution "from all enemies, foreign and domestic." The Oath Keepers are led by PERSON ONE.

50. In a widely disseminated video[1] recorded by a photojournalist on January 6, 2021, a "stack" of individuals dressed in matching uniforms consisting of camouflaged-combat attire, to include confirmed Oath Keeper members (further described below), moves up and through a crowd on the east side of the U.S. Capitol. A screenshot of the video is below, with a portion of the "stack" encircled by a red oval:

[1] See https://apnews.com/article/ex-military-cops-us-capitol-riot-a1cb17201dfddc98291edead5badc257/gallery/0ecd1781c66d437f92c61b3f4848a74e

51. Law enforcement reports that a stack or line formation is a tactical formation used by infantryman in the military. One defining feature of this formation is that members keep their hands on the backs or vests of the person in front of them to remain together while entering a room or weaving through a crowd. The purpose of maintaining direct physical contact with one another is to efficiently communicate with one another, especially in crowded or noisy areas.

52. A service called "News2Share" uploaded to YouTube a video of the January 6, 2021, attack at the Capitol. At the approximate 3-minute-and-8-second mark, the video shows eight-to-ten individuals in matching uniforms consisting of camouflaged-combat attire aggressively approaching an entrance to the Capitol.[2] These individuals, who are wearing helmets, reinforced vests, and clothing with Oath Keeper logos and insignia, can be seen moving in an

[2] See https://www.youtube.com/watch?v=b76KfHB0QO8&feature=youtu.be.

organized and practiced fashion and forcing their way to the front of the crowd gathered around a set of doors to the Capitol.

53. A close-up view of the badges on the vest of one of these individuals, seen just under the Oath Keepers emblem on his shirt, displays the Oath Keepers motto, "Not On Our Watch." The badge also says, "I don't believe in anything. I'm just here for the violence."

54. Based on the foregoing observations of the video, and information gained in the course of the investigation, it is reasonable to believe that the organized group of individuals marching to the doors of the Capitol in the video above are members and affiliates of the Oath Keepers. More than a dozen Oath Keepers, including Jessica Watkins, Kelly Meggs, and

approximately eight individuals from Florida (including Defendant Four as referenced below), have been charged for their involvement in the January 6 riots.

Facts Specific to Jeremy Brown

55. On January 25, 2021, FBI WFO received a complaint from Witness 1 who has known JEREMY BROWN for multiple years. Witness 1 provided publicly available photos of BROWN in tactical gear from January 5, 2021, but was unsure about whether BROWN entered the Capitol during the riots. Your affiant has provided one of the photos here:

56. Your affiant was able to identify BROWN'S whereabouts on January 6 by comparing the publicly available photo of Brown (above) from January 5th to photography and video from January 6. Your affiant located a publicly available photo of him on Twitter wearing the same distinctive attire standing just before the steps of the East side steps of the Capitol during the riots of January 6. He was more than 100 feet within the restricted grounds that law enforcement had originally set up to protect Congress and Vice President Pence during the certification of the Electoral College vote. Brown wore full military gear, including a helmet, radio,

a tactical vest, and prominently displayed large surgical trauma shears tucked into a pack sitting on the vest, nearly the exact attire that he wore on the prior day. Your affiant has provided the Twitter photo below:

57. Your affiant reviewed body worn camera footage from January 6, 2021 and was able to identify BROWN by his distinctive attire outside the East doors of the Capitol at approximately 4:27 PM. During this period, Brown remained at least one hundred feet past the barriers that law enforcement had initially set up to protect the Capitol. On the body worn camera video, BROWN carried zip ties attached to his belt, as well as a radio, surgical trauma shears, and tactical gear. Metropolitan Police Officers, in attempting to resecure the Capitol Grounds,

advanced in a line and yelled "Back" in unison. Instead of voluntarily complying with police orders, BROWN only retreated when pushed with police baton sticks. During this encounter, BROWN repeatedly claimed that the officers were, in his opinion, violating the laws and the Constitution of the United States. Your affiant has included a screenshot below:

58. In the course of this investigation, your affiant has also reviewed a statement from Defendant 4 who has pled guilty to Conspiracy to Obstruct an Official Proceeding relating to his conduct and the conduct of other Oath Keepers in breaching the US Capitol on January 6, 2021.

59. According to Defendant 4, Defendant 4 utilized a ride share to travel to BROWN'S house on January 4 in preparation for traveling to Washington D.C. Your affiant has obtained records from the ride share company indicating that Defendant 4 entered an address consistent with BROWN's home address of [redacted] (the "**Residence**").

60. According to Defendant 4, Brown and other individuals associated with the Oath Keepers coordinated their activity via a Signal[3] chat of Florida Oath Keepers. They caravanned in a recreational vehicle (the "**RV**") that was, according to Defendant 4, loaded with a cache of

[3] Signal is an encrypted chat application.

weapons, ammunition, and gas. Defendant 4 followed the **RV** in BROWN'S girlfriend's van. Kelly Meggs, currently indicted for his role in the conspiracy and the leader of the Florida branch of the Oath Keepers, informed Defendant 4 that Brown was a "loose cannon" and had explosives inside the RV. Defendant 4 positively identified Brown in the publicly available Twitter photo referenced above.

61. Your affiant has reviewed the Signal chat referenced by Defendant 4. In the chat, BROWN coordinated travel plans with other Oath Keepers and rendezvous points. On December 23, 2020, he messaged, "We have a RV an Van going. Plenty of Gun Ports left to fill. We can pick you up." On January 1, 2021, BROWN, referring to his RV as "GROUND FORCE ONE" wrote:

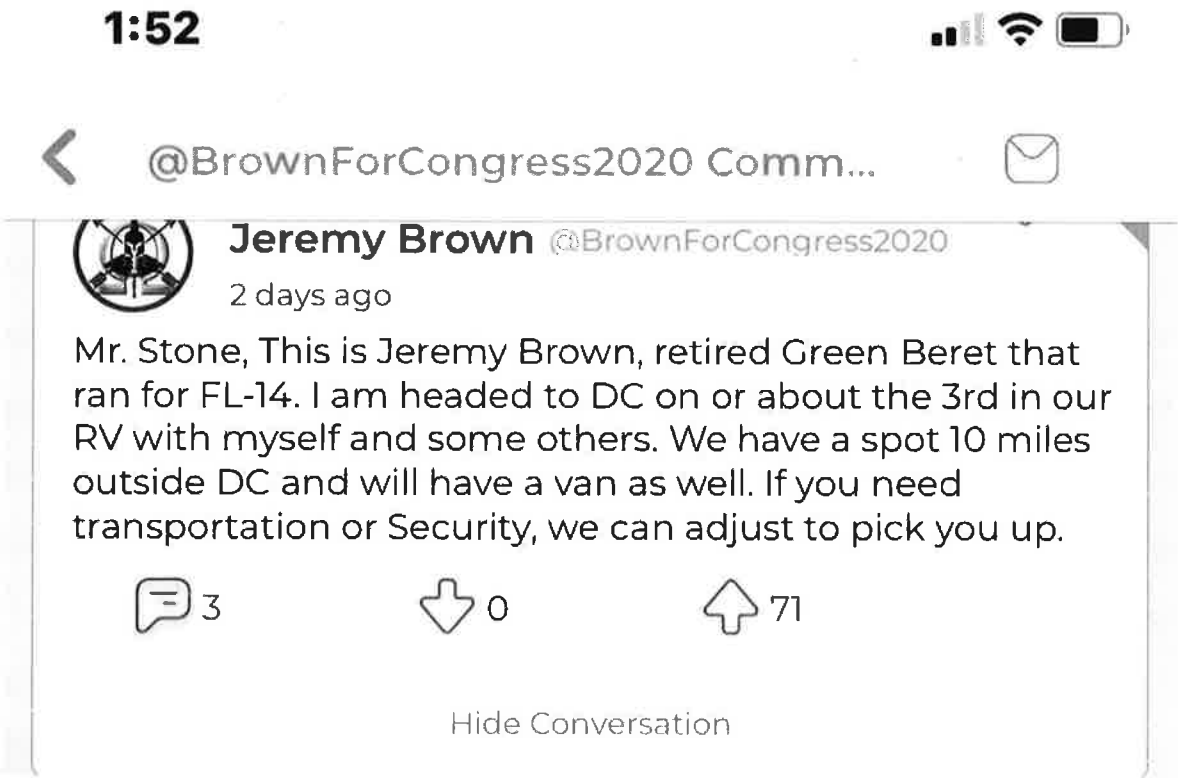
> GROUND FORCE ONE Departure Plan:
> If you can, come to my house anytime Saturday. You can stop by and drop stuff off, or stay the night. This way we can load plan, route plan, and conduct PCIs (Pre Combat Inspections).
> I would LIKE to depart by 0645 on Sunday morning, Jan 3rd. Push through to the NC linkup on the 3rd, RON (Rest Over Night) there, then push to DC on the 4th. This will give us the 4th/5th to set up, conduct route recons, CTR (Close Target Reconnaissance) and any link ups needed with DC elements.
> If you need to be picked up, then we will work that into route plan and will provide exact pickup time by Saturday evening. Please have EVERYTHING ready once we arrive. It will be an ERO (Engine Running Onload).
> IF YOU ARE RIDING WITH ME, dm me with your plan to come here or be picked up. I will send address via the dm.
> I am willing to make adjustments all the way up until we pass your ass headed north, but it is now time to shit or get on someone else's pot. READY? GO!!!

62. Your affiant has also reviewed statements made by BROWN and other Oath Keepers following the riots of January 6, 2021. On that day, BROWN wrote:

> Everything you are watching on the Media and Houses of Congress is a LIE! I was shot in the neck with pepper balls and beating in the forearm with a night stick trying to shield unprotected Civilians from being hit in the head. This was an exercise in the unrestrained addiction to power.

Other indicted Oath Keepers also participated on additional Signal chats with BROWN. On the afternoon of January 7, 2021, Jessica Watkins, who has been indicted on charges of Conspiracy and Obstruction of an Official Proceeding for her actions on January 6, "Proud to go in with you all! I'd say 'I'll follow you into the gates of hell' but we did that already." Law enforcement has been able to retrieve portions, but not all of this chat from the phones of other conspirators. Some messages in the chat appear to have been deleted including those sent by Kelly Meggs, who, like Watkins, has also been indicted for Conspiracy and various charges with other Oath Keepers.

63. Your affiant also has reviewed Parler posts from BROWN'S account (@brownforcongress2020). Based on this review, your affiant was able to confirm that BROWN intended to travel to DC for the January 5 protests in an RV with other individuals:



64. Your affiant also reviewed publicly available video podcasts of BROWN and PERSON ONE. In an interview posted on July 12, 2021,[4] BROWN stated that he was present with other Oath Keepers on January 6. Prior to the riots, he deposited his guns with other Oath Keepers in Virginia and retrieved them after the riots. During the riots, BROWN stated that he was present with other Oath Keepers, including those who have been indicted for actions relating to their breach of the Capitol, and encouraged other Oath Keepers, such as Jessica Watkins, not to enter the Capitol.

65. Your affiant has reviewed a statement given by BROWN to federal agents. Law enforcement agents called BROWN at XXX-XXX-4564 (the "**TARGET PHONE**") on or about January 6 and 7, 2021 and inquired regarding his whereabouts. Agents spoke briefly with BROWN on January 6, 2021 but could not hear him well due to apparent crowd noise. BROWN spoke to agents in more detail on January 7, 2021. He told them that he was present in Washington, D.C. and provided security for VIPs at the "Stop the Steal" rally. He stated that he had no information about anyone who entered the Capitol.

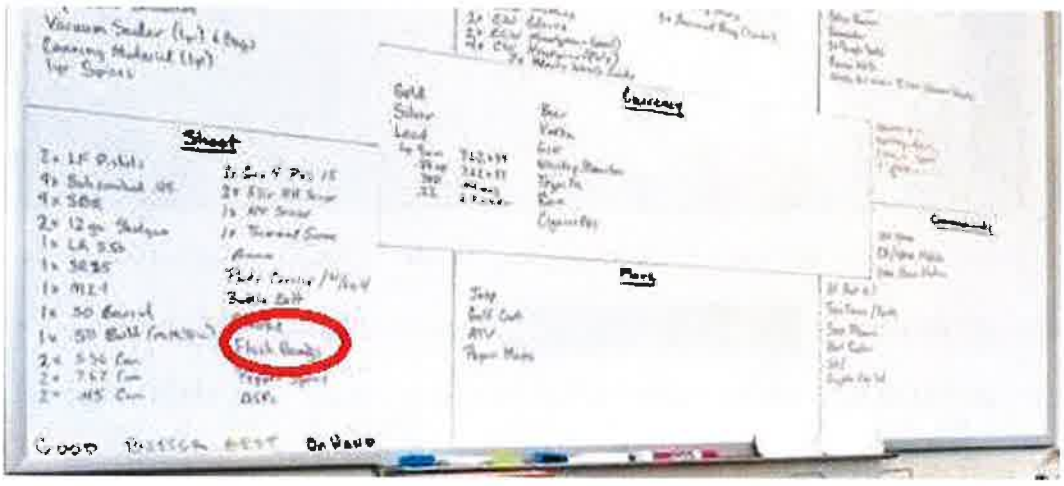
66. According to records obtained through a search warrant which was served on Verizon, on January 6, 2021, in and around the time of the incident, the cellphone associated with the **TARGET PHONE** was identified as having utilized a cell site consistent with providing service to a geographic area that included the interior of the United States Capitol building. Your affiant has not yet identified BROWN inside the Capitol but has identified him within the restricted ground.

67. Your affiant has learned from an individual who has known BROWN for multiple years that he intends to sell his current house located at [redacted]

[4] https://freeworldnews.tv/watch?id=60ecff8474feb85ab1adec2f

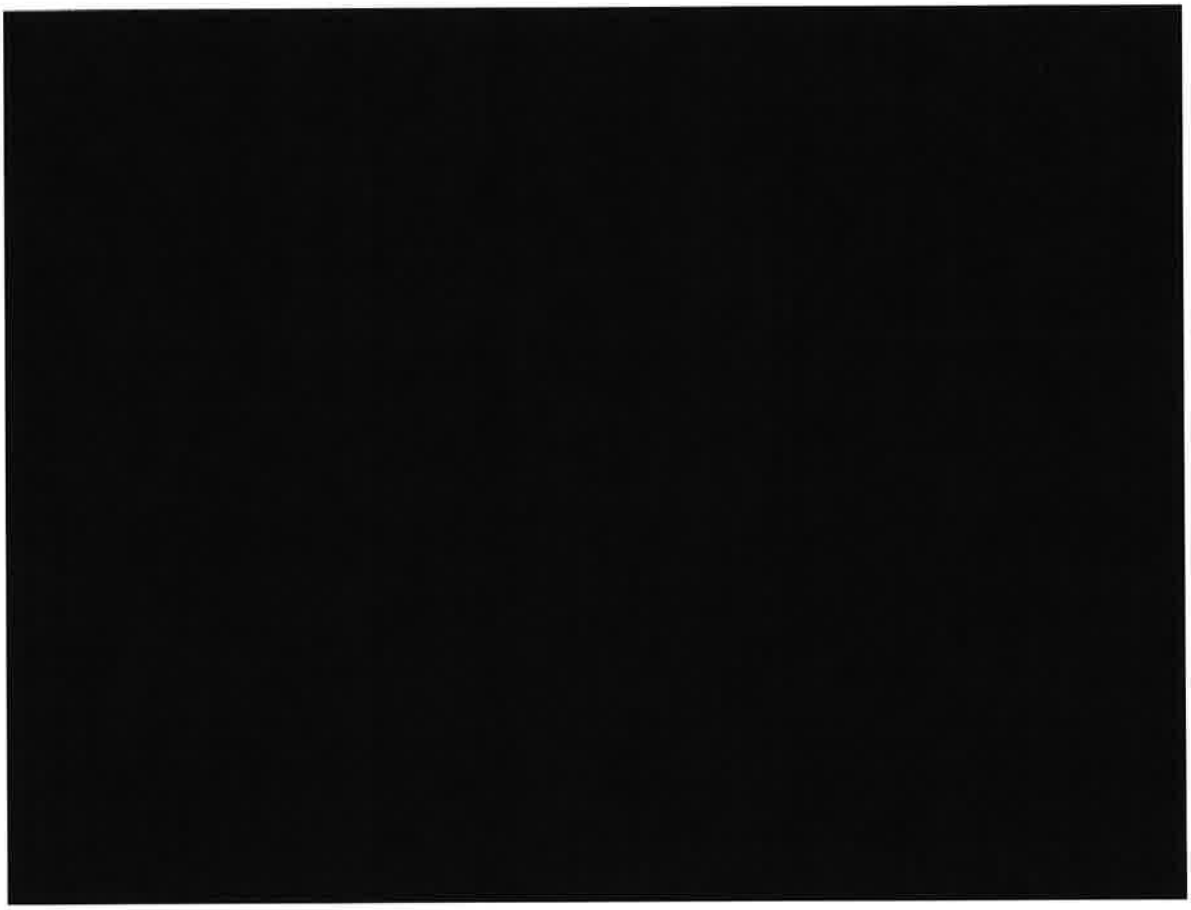
FLORIDA (the "**RESIDENCE**") and vacate by approximately October 2, 2021. According to publicly available information on Zillow, a real estate website, BROWN'S residence is currently for sale. On a photo from what appears to be BROWN'S office, your affiant identified a large white board containing lists of items corresponding to the following column: "Food," "Clothing," "Shelter," "Currency," "Communicate," "Move," and "Shoot." In the "Shoot" column, there are numerous firearms listed and explosive devices such as "flash bangs." "Flash bangs" are prohibited explosive devices under 26 USC 5861, unless registered with the Bureau of Alcohol, Tobacco, and Firearms (ATF). Your affiant has queried information with the ATF. BROWN is not registered to possess explosive devices.

68. At the bottom of the white board, "Good" is written in red marker, "Better" is written in blue marker, "Best" is written in green marker, "On hand" is written in black marker. All items listed under "Shoot," including flash bangs, are written in black marker indicating that they are on hand. Your affiant has included a zoomed in screen shot of the photo below and has circled flash bangs in red:



69. Your affiant has spoken to an individual who has known BROWN for multiple years. This individual did not have any specific knowledge about BROWN possessing or seeking

to possess explosives such as "flash bangs." BROWN is currently living both in the **RV** and in the **RESIDENCE**. The **RV** is the same **RV** he used to travel to Washington, D.C. The **RV** is parked in front of his house. FBI agents observed the RV on September 21, 2021 and photographed it below:



70. Both the **RV** and a black trailer (the "**Trailer**"), which is also parked on the property are registered to [redacted] who according to multiple individuals who have known BROWN for multiple years, is BROWN'S current girlfriend. On her driver's license, [redacted] lists her home address as of [redacted]. BROWN resides with [redacted].

71. A family member of Witness 1 informed Witness 1 that IT was present inside the **RESIDENCE** prior to the house going on the market. The house was full of BROWN'S possessions with multiple boxes and weapons scattered throughout the house. Publicly available photos on Zillow now show an organized home, inconsistent with the description of the house by the family member of Witness 1. Witness 1 stated that BROWN now alternates sleeping in the house and in the RV.

72. Based on my training, experience, general familiarity with the small confines of an RV, the fact that the trailer was purchased approximately one month ago and sits next to the RV and the house within the property line of [redacted] and that it is unlikely that an individual would market a home available for public inspection with guns and explosives inside of the home, it is probable that many of BROWN'S possessions, including electronics, guns, ammunition, and explosives, which constitute potential evidence in the investigation, have been moved to the **RV** or the **TRAILER**.

The Collective Premises

73. On September 21, 2021, law enforcement agents observed the **RESIDENCE** (further described in Attachment A), the **RV** (further described in Attachment B), which is registered to BROWN'S girlfriend, and the **TRAILER** (further described in Attachment C) also registered to BROWN's girlfriend. Public records indicate that [redacted] currently owns the property. BROWN has previously told agents that he resides at the address. BROWN has posted on Facebook that he is actively selling items at the property in preparation for vacating the premises by September 30, 2021. Witness 1 informed your affiant that BROWN is currently sleeping in the RV.

Facts Specific to This Seizure of the TARGET PHONE

74. On or about September 30, 2021, your affiant anticipates arresting BROWN for violations of federal law. Due to officer safety considerations, your affiant and other federal agents anticipate arresting BROWN when he is away from his suspected cache of weapons and explosives that BROWN likely keeps at the **RESIDENCE**, **RV**, or **TRAILER**. In the last week, agents have observed BROWN leave his property. Based on my training and experience, your affiant knows that individuals typically carry their cell phones when they exit their property. Investigators seek this warrant for authority to stop BROWN, search his person for the **TARGET PHONE** (further described in Attachment D), to seize **the TARGET PHONE**, and to search the **TARGET PHONE** for evidence of the offenses under investigation, as described above and in Attachment E.

Cellular Devices

75. There is probable cause to believe that BROWN'S cellular telephone and other electronic devices contain evidence of the criminal conduct under investigation. Because BROWN traveled to Washington, D.C., from Florida, there is also probable cause to believe that BROWN would have used any cellular telephone in his possession to communicate with others during his trip about his activities in Washington, D.C., navigate during travel, conduct searches for food and lodging, and for other purposes that would serve as evidence of his whereabouts and activities at various points during his trip. All of this type of electronically-stored evidence will help investigators prove BROWN'S presence and activities at the U.S. Capitol on January 6, 2021, his intent when traveling to Washington, D.C., and the identities of his coconspirators.

76. It is well-known that virtually all adults in the United States use mobile digital devices like cellular telephones. In a fact sheet from June 12, 2019, The Pew Research Center for

Internet & Technology estimated that 96% of Americans owned at least one cellular phone, and that that same 2019 report estimated that 81% of Americans use at least one smartphone. *See* Mobile Fact Sheet, https://www.pewresearch.org/internet/fact-sheet/mobile. Given cellular telephones' ubiquity, portable size, and ability to store uniquely personal information, your affiant knows that cellular telephone users generally keep his cellular telephone on or near himself.

CELLULAR TELEPHONES AND OTHER ELECTRONIC DEVICES

77. As used herein, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

78. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, your affiant knows the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

i. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

ii. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital

versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

iii. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

iv. A cellular telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephone offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device. Many cellular telephones are minicomputers or "smart phones" with immense storage capacity.

v. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that

antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

79. As described above and in Attachment E, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the **PREMISES**, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; cellular telephones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, your affiant respectfully submits that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment E will be stored in the Devices for at least the following reasons:

a. Individuals who engage in criminal activity, including traveling interstate to commit riots and taking and transmitting photos and videos of themselves while committing rioting activity, use digital devices, like the Devices, to access websites to facilitate illegal activity, obtain directions to places of interest, communicate with co-conspirators online, use social media applications like Facebook, and, among other things, store documents and records relating to their illegal activity. As a result, Devices used for such purposes often contain evidence like logs of online chats with co-conspirators, device location information, email correspondence, text or other "Short Message Service" ("SMS") messages,

internet browsing history, and contact information of co-conspirators, which could include telephone numbers, email addresses, identifiers for instant messaging accounts, and social medial accounts.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

80. As further described in Attachment E, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital devices were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, your

affiant respectfully submits there is probable cause to believe that this forensic electronic evidence and information will be in any of the Devices at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

81. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Therefore, in searching for information, records, or evidence, further described in Attachment E, law enforcement personnel executing this search warrant will employ the following procedures: Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment E and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES.

UNLOCKING CELLULAR TELEPHONES USING BIOMETRIC DATA

82. This warrant permits law enforcement agents to obtain from the person of BROWN (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Devices requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that BROWN'S physical biometric characteristics will unlock the Devices. The grounds for this request are as follows:

83. Your affiant knows from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

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

85. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

86. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

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

88. As discussed in this Affidavit, your affiant has reason to believe that one or more digital devices, the Devices, will be found during the search. The passcode or password that would unlock the Devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

89. Your affiant also knows from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

90. Due to the foregoing, if law enforcement personnel encounter any Devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from BROWN the display of any physical biometric characteristics (such as fingerprint/ thumbprint or facial characteristics) necessary to unlock any Devices, including to (1) press or swipe the fingers

(including thumbs) of the aforementioned person to the fingerprint scanner of the Devices found at the PREMISES; (2) hold the Devices found at the PREMISES in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the Devices found at the PREMISES in front of the face of the aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the Devices in order to search the contents as authorized by this warrant.

91. The proposed warrant does not authorize law enforcement to require that BROWN state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Devices. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned persons to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned persons would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask BROWN for the password to any Devices, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Devices, the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION

92. Based upon the foregoing facts and information, there is probable cause to believe that violations of 18 U.S.C. §§ 371 (conspiracy); and 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds) (the "Subject Offenses") have been committed by BROWN and/or other identified and unidentified persons, and that fruits, evidence, and instrumentalities of those violations will be found at the PREMISES.

Katie M Hill

Katie Hill, Special Agent
Federal Bureau of Investigation

Subscribed and sworn by telephone pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on September 29, 2021.

Zia M. Faruqui
2021.09.29
19:37:14 -04'00'

HON. ZIA M. FARUQUI
United States Magistrate Judge