

AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE

*[Handwritten Signature]* 7/18/2022

UNITED STATES DISTRICT COURT

FILED

for the

JUL 18 2022

Western District of Oklahoma

CARMELITA REEDER SHINN, CLERK  
U.S. DIST. COURT, WESTERN DIST. OKLAHOMA  
BY *[Signature]*, DEPUTY

In the Matter of the Search of

323 North 8th Avenue, Fairview, Major County, Oklahoma,  
a black 2012 Porsche Cayenne, bearing Oklahoma tag  
# KMY-732, VIN No. WP1AA2A23CLA10469, and (2) a  
blue 2013 Nissan Titan, bearing Oklahoma tag # HCD-192,  
VIN No. 1N6BA0ECXDN315225

Case No. M-22- 519 -SM

APPLICATION FOR A SEARCH WARRANT

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

See Attachment "A"

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

See Attachment "B" which is incorporated by reference herein.

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:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1752(a)(1)	Enter or Remain in a Restricted Building or Grounds
18 U.S.C. § 1752(a)(2)	Engage in Disorderly or Disruptive Conduct in a Restricted Building or Grounds
18 U.S.C. § 1752(a)(4)	Engage in Act of Physical Violence Against Any Person or Property in a Restricted Building or Grounds
40 U.S.C. § 5104(e)(2)(D)	Engage in Disorderly or Disruptive Conduct in Capitol Grounds or Any of the Capitol Buildings
40 U.S.C. § 5104(e)(2)(F)	Engage in an Act of Physical Violence in the Capitol Grounds or Any of the Capitol Buildings
18 U.S.C. § 1361	Injure or Depredate Any Property of the United States in Excess of \$1,000

The application is based on these facts:

See attached Affidavit of, which is incorporated by reference herein.

- 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.

*[Handwritten Signature: David Otwell]*

Applicant's signature

David Otwell, Task Force Officer, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: July 18, 2022

*[Handwritten Signature: Suzanne Mitchell]*

Judge's signature

SUZANNE MITCHELL, U.S. MAGISTRATE JUDGE

Printed name and title

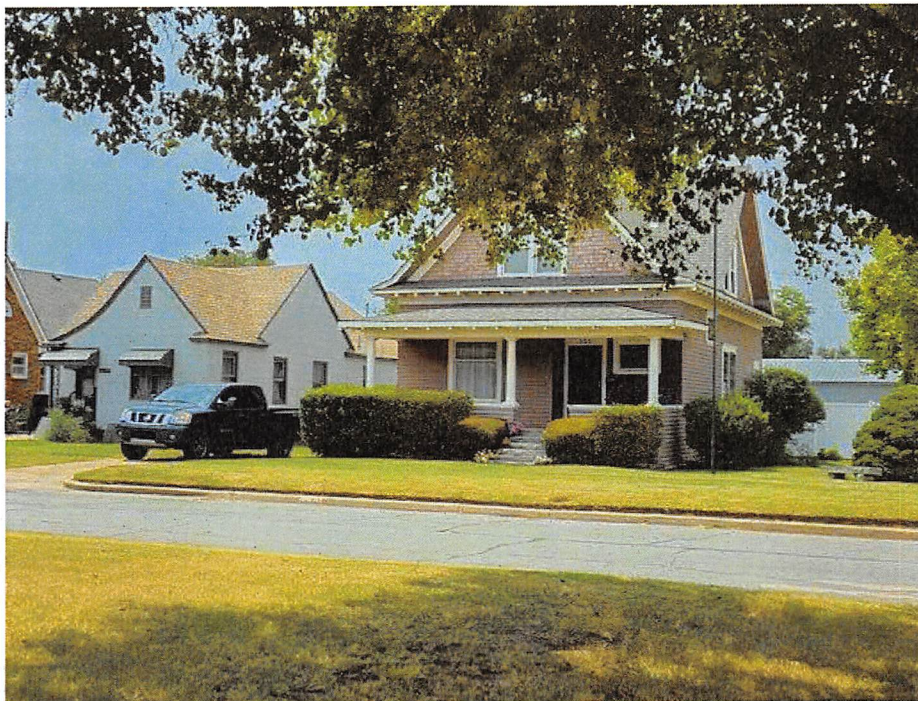
City and state: Oklahoma City, Oklahoma

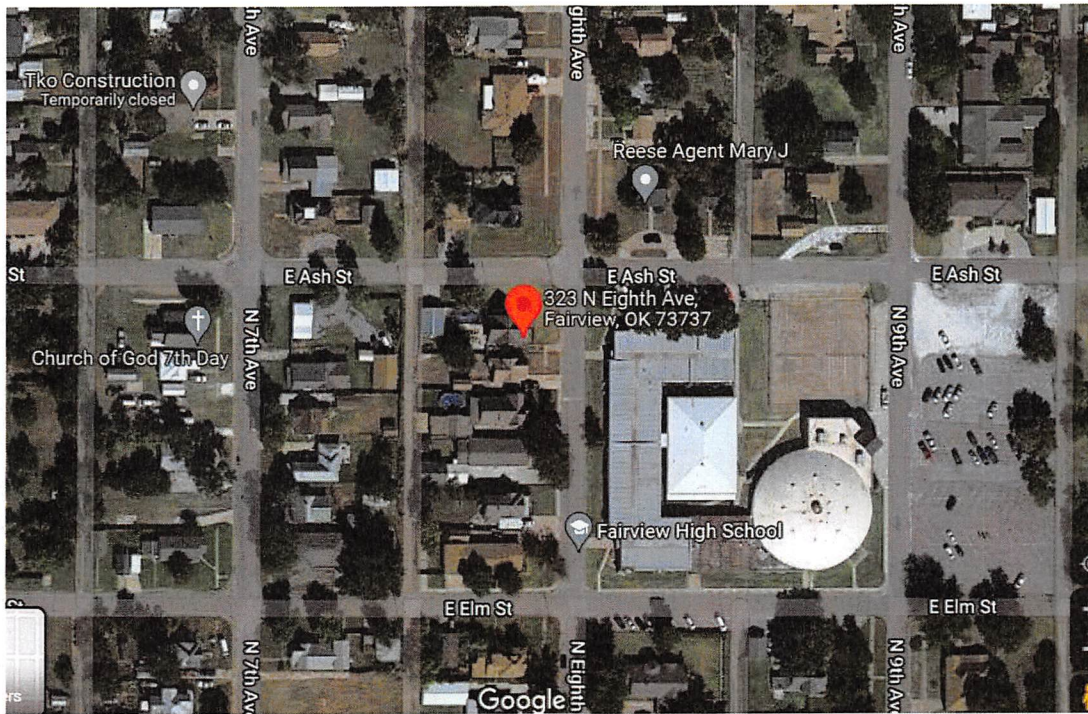
**ATTACHMENT A**

*Property to be searched*

The property to be searched is 323 North 8th Street, Fairview, Major County, Oklahoma (hereinafter "PREMISES"), further described as a two-story single-family residence situated on the southwest corner of East Ash Street and Eighth Avenue, with wood siding painted in a light salmon color on the upper and lower level of the residence, white trim around the windows and doors, black numbers "323" affixed above the front door which faces east, a front door that has a screen door attached with black burglar bars, and the numbers "323" painted in black on the curb in front of the residence. The front of the PREMISES faces east and is across the street from the Fairview High School. The PREMISES has a detached grey metal building with a two-car garage overhead door. The metal building has a cement paved driveway and there is a white plastic privacy fence between the PREMISES and detached garage. Two cars are registered to this address: (1) a black 2012 Porsche Cayenne, bearing Oklahoma tag # KMY-732, VIN No. WP1AA2A23CLA10469, and (2) a blue 2013 Nissan Titan, bearing Oklahoma tag # HCD-192, VIN No. 1N6BA0ECXDN315225.









**ATTACHMENT B**

*Property to be seized*

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 1752(a)(1), 18 U.S.C. § 1752(a)(2), 18 U.S.C. § 1752(a)(4), 40 U.S.C. § 5104(e)(2)(D), 40 U.S.C. § 5104(e)(2)(F), and 18 U.S.C. § 1361 (the “Target Offenses”) that have been committed by DOVA WINEGEART (“the Subject”) and other identified and unidentified persons, as described in the search warrant affidavit; including, but not limited to, any mobile cellular device, including a cellular device that is associated with telephone number \*\*\*-\*\*\*-0028. Cellular devices owned, used, or controlled by WINEGEART may contain:

- a. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- b. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;
- c. Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, *i.e.*, the certification process of the 2020 Presidential Election;
- d. Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, *i.e.*, the certification process of the 2020 Presidential Election;
- e. Evidence relating to a conspiracy to illegally enter and/or occupy the U.S. Capitol Building on or about January 6, 2021;
- f. Evidence concerning the breach and unlawful entry of the United States Capitol, and any conspiracy or plan to do so, on January 6, 2021;
- g. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;

- h. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;
  - i. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;
  - j. Evidence of any conspiracy, planning, or preparation to commit those offenses;
  - k. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
  - l. Evidence concerning materials, devices, or tools that were used to unlawfully enter the U.S. Capitol 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;
  - m. Evidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
  - n. Evidence of the state of mind of the subject and/or other co-conspirators, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and
  - o. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.
2. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:
- a. Any records and/or evidence revealing the Subject's presence at the January 6, 2021, riot;
  - b. Any physical records, such as receipts for travel, which may serve to prove evidence of travel of to or from Washington D.C. from December of 2020 through January of 2021;



- c. The Subject's (and others's) motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
- d. The Subject's (and others's) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021.

3. During the execution of the search of the PREMISES described in Attachment A, or upon arrest, law enforcement personnel are also specifically authorized to obtain from WINEGEART (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 person(s)' 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.

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.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed 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 disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.



UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH  
OF: 323 North 8th Avenue, Fairview,  
Major County, Oklahoma, a black 2012  
Porsche Cayenne, bearing Oklahoma tag  
# KMY-732, VIN No.  
WP1AA2A23CLA10469, and (2) a blue  
2013 Nissan Titan, bearing Oklahoma tag  
# HCD-192, VIN No.  
1N6BA0ECXDN315225,  
UNDER RULE 41

SW No. M-22-519-SM

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41  
FOR A WARRANT TO SEARCH AND SEIZE**

I, David Otwell, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 323 North 8th Street, Fairview, Major County, Oklahoma, a black 2012 Porsche Cayenne, bearing Oklahoma tag # KMY-732, VIN No. WP1AA2A23CLA10469, and a blue 2013 Nissan Titan, bearing Oklahoma tag # HCD-192, VIN No. 1N6BA0ECXDN315225, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Task Force Officer assigned to the Federal Bureau of Investigation (FBI), Joint Terrorism Task Force (JTTF). In my duties as a JTTF-Task Force Officer, I investigate individuals and organizations involved in domestic and international terrorism

and/or the support of it. Currently, I am tasked with investigating criminal activity in and around the Capitol grounds on January 6, 2021. As a JTTF - Task Force Officer I am authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of a violation of Federal criminal laws. Throughout those investigations, I became familiar with how the use of cell phones and social media has become more prevalent throughout the “criminal world.”

3. The facts in this affidavit come from my personal knowledge and 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 my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 1752(a)(1), 18 U.S.C. § 1752(a)(2), 18 U.S.C. § 1752(a)(4), 40 U.S.C. § 5104(e)(2)(D), 40 U.S.C. § 5104(e)(2)(F), and 18 U.S.C. § 1361 (the “Target Offenses”) have been committed by DOVA WINEGEART (“WINEGEART”) and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, WINEGEART, as well as others observed by WINEGEART. There is also probable cause to search the PREMISES, further described in Attachment A, for the things described in Attachment B.



**PROBABLE CAUSE**

***Background – The U.S. Capitol on January 6, 2021***

5. United States 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 (“U.S. Capitol”), located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906, on January 6, 2021.

6. The U.S. Capitol 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 of this area was barricaded and off limits to the public on January 6, 2021.

7. 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.

8. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

9. 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 (“Certification”). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m. EST, 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.

10. 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.

11. At approximately 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 who were there to protect the U.S. Capitol.



12. At approximately 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. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

13. 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.

14. At approximately 2:00 p.m. EST, 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 on the Capitol grounds or in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by USCP 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.

15. Shortly after 2:00 p.m. EST, 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.



16. Shortly thereafter, at approximately 2:20 p.m. EST, 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. 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 were forced to draw their weapons to protect the victims sheltering inside.

17. 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. 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. 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.

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

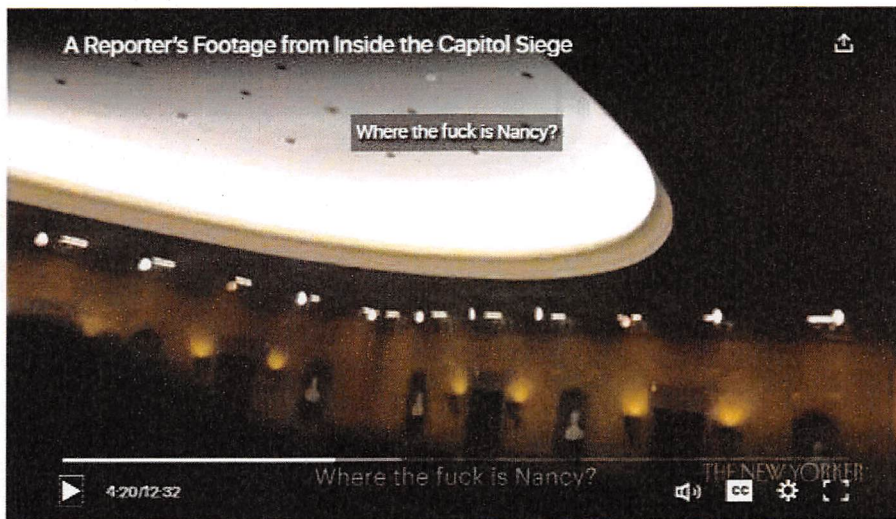
19. At approximately 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

20. At approximately 2:47 p.m. EST, subjects broke into the United States Senate Chamber. Publicly available video 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.

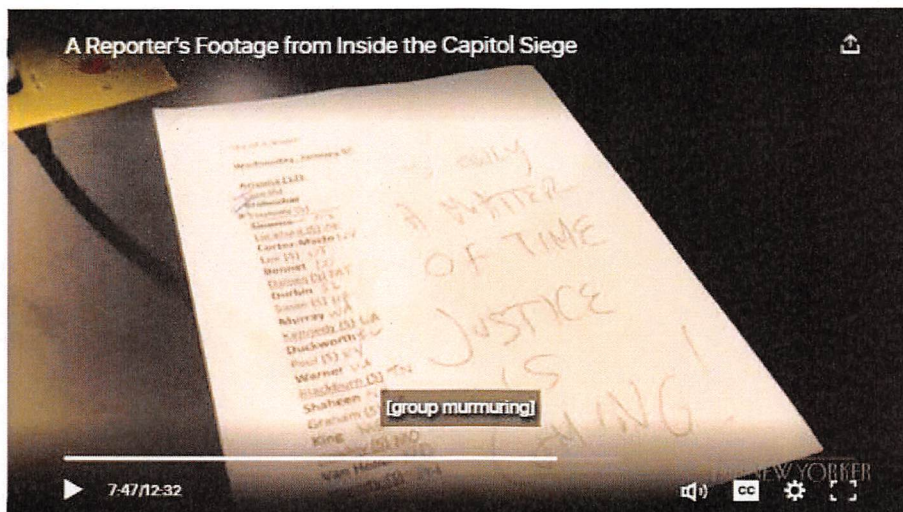




21. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, “Where the fuck is Nancy?” Based upon other comments and the context, law enforcement believes that the “Nancy” being referenced was the Speaker of the House of Representatives, Nancy Pelosi.

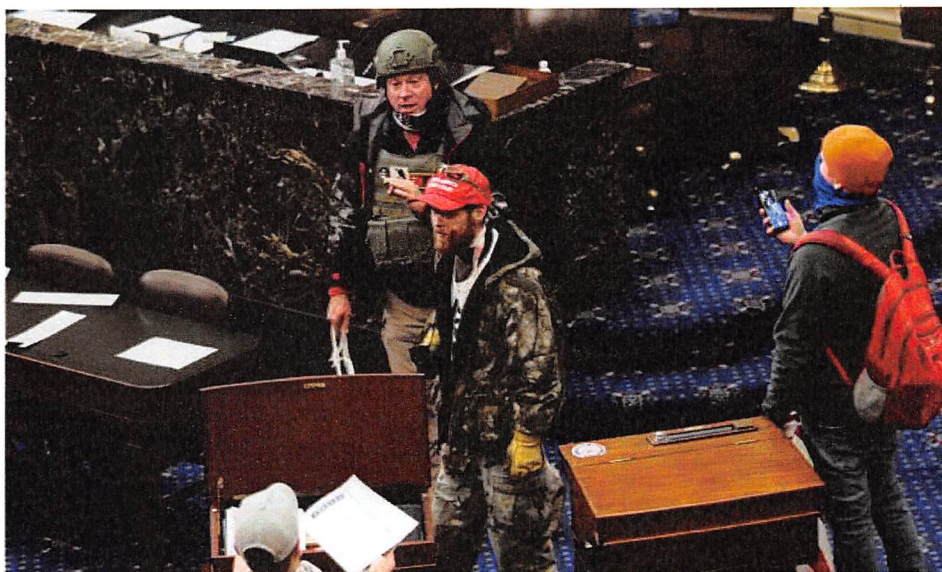


22. One subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated “Is Only A Matter of Time Justice is Coming!”





23. Multiple subjects were observed inside the U.S. Capitol wearing what appears to be, based upon my training and experience, tactical vests and carrying flex cuffs. Based upon my knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals are expected to be taken into custody.



24. At approximately 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

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

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

27. 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. EST 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 Senate resumed work on the Certification at approximately 8:00 p.m. EST 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.

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

29. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3:00 a.m. EST on January 7, 2021.

30. 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.

31. 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 allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

32. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself and damaging and stealing property. 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.

33. Photos below, 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:





<sup>1</sup> <https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/>.

<sup>2</sup> <https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1>.





*Facts Specific To Dova Winegeart*

34. Following the aforementioned events at the U.S. Capitol, the FBI's Washington Field Office (WFO) received information from several tipsters about a subject, Dova Winegeart (WINEGEART), who allegedly entered the U.S. Capitol grounds unlawfully on January 6, 2021.

35. Tipster 1 and Tipster 2, both friends of WINEGEART, separately submitted several photos from January 6, 2021, showing WINEGEART on U.S. Capitol grounds. Photo 1 depicts a woman with blonde hair wearing a long, bright red peacoat with black buttons, a white hat, one black glove, and black rimmed glasses, who appears to be standing on U.S. Capitol grounds next to a man in a blue jacket. In Photo 2, the same blonde-haired woman in the long red peacoat, white hat, and black gloves appears to be swinging a long wooden pole at the window of a door marked as "House of Representatives."

---

<sup>3</sup> <https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e>.



Photo 1



Photo 2

36. Tipsters 1 and 2 also submitted Photo 3, which depicts the same blonde-haired woman in a bright red peacoat with black buttons and black rimmed glasses.

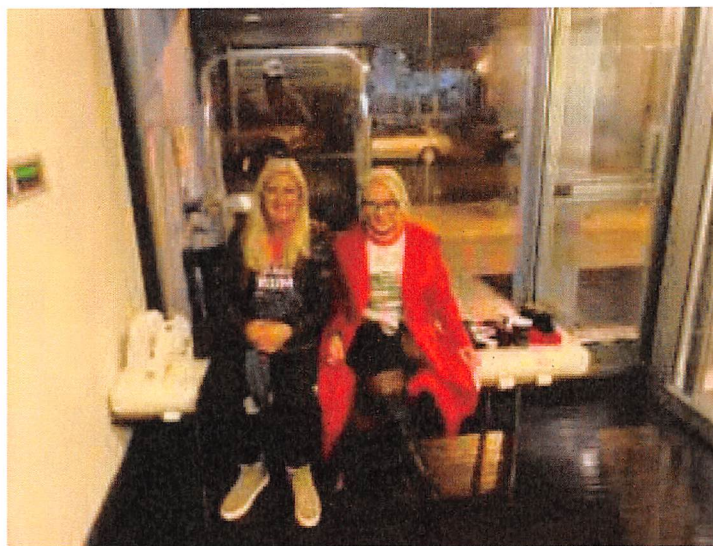


Photo 3

37. Law enforcement interviewed Tipster 1 and Tipster 2 on September 13, 2021. At the interview, both tipsters positively identified WINEGEART as the blonde-haired woman in a bright red peacoat and black rimmed glasses in Photos 1, 2, and 3.



38. Your affiant reviewed U.S. Capitol Police Closed Circuit Television (CCTV) video footage from a camera recording the exterior of the U.S. Capitol building on January 6, 2021 around 2:30 pm EST (House of Representatives door footage), and identified what appears to be the same blonde-haired woman in the long red peacoat, white hat, and black gloves swinging a long wooden pole with what appears to be pointed metal attachments at the window of the House of Representatives door, as depicted in Photos 4 and 5:



Photo 4



Photo 5

39. Your affiant obtained photographs of the window of the door marked as “House of Representatives.” The window has several cracks and holes that appear to be

consistent with damage caused by the pointed metal attachments on the wooden pole that WINEGEART swung several times at the window.



Photo 6

40. Your affiant was provided a quote from the Architect of the Capitol for repair of this glass, which demonstrates that the cost to replace the damaged glass exceeds \$1,000.

41. Your affiant also reviewed Photo 7, which is a photograph submitted by a tipster of a blonde-haired woman in the long red peacoat, white hat, and dark rimmed glasses, consistent with the description of the person that Tipsters 1, 2, and 3 (see below) identified as WINEGEART, in front of the House of Representatives door. The window of the door appears to be damaged.





Photo 7

42. On October 7, 2021, and on October 21, 2021, law enforcement interviewed Witness 3, another of WINEGEART's friends. WINEGEART had sent text messages to Witness 3 on January 7, 2021, including Photo 1 and Photo 3. Witness 3 positively identified WINEGEART in Photos 1 and 3.

43. WINEGEART sent text messages to Witness 3, such as:

- "Had to stay in hotel after storm of capital. It got crazy. I did shit."
- "Some false stories going around. We have tons of video. A lot of pissed of Trump supporters. A few Antifa. Yes we are mad. Yes we want to go inside Capital. It's our building. Not the governments. We are their bosses but get treated like dogs. I'm done with this government. It's fight time non stop now. They asked for it."
- "No I didn't go inside couldn't break open alone. Moved onto balcony with cops after. Pieces of shit."

- "I'll send ya videos when I can."
- "Emergency broadcast system will be sounding off in near future. Then it's go time for real."

44. Witness 3 reviewed the House of Representatives CCTV footage (Photos 4 and 5, above) and positively identified the blonde-haired individual in a red peacoat and white hat walking up to the door of the U.S. Capitol and repeatedly striking the door with a long wooden pole with metal attachments as WINEGEART.

45. On November 3, 2021, law enforcement interviewed WINEGEART and her husband Terry Winegeart at their residence in Fairview, Oklahoma (PREMISES). Terry Winegeart admitted that he and WINEGEART were present at the U.S. Capitol on January 6, 2021. Terry Winegeart reviewed the House of Representatives door footage, and positively identified the person in the red peacoat striking the door with a wooden pole as WINEGEART. WINEGEART also admitted that she was present on the U.S. Capitol grounds on January 6, 2021.

46. During the investigation, your affiant reviewed the aforementioned videos and photos from the Capitol building on January 6, 2021. Additionally, I compared WINEGEART's Oklahoma driver's license photograph with the abovementioned photos and video. Based on your affiant's observations of WINEGEART during the in-person interview and her driver's license photograph, I believe that WINEGEART is the individual in Photos 1-5 and Photo 7.

44. The FBI conducted a database search and confirmed that WINEGEART's cellular telephone number ended in -0028, having service provided by New Cingular Wireless was subscribed to WINEGEART. The phone number ending in -0028 was searched in the Washington's Field Office (WFO's) geofencing database, which covers the inside and outside of the United States Capitol during the approximate time of the riot, showed positive results on January 6, 2021, at 7:57:30 PM UTC. The device type was identified as: Apple Incorporated, Apple iPhone XS Max (A1921) and the IMEI associated with the tower showed ID # 3531101011428522.

45. I know, based on my training and experience, that cell phones are expensive, and people routinely retain their cell phones for many months or years. Apple iPhones also have the ability to backup the stored data to a remote server or computer. It is common for users of iPhones who purchase new iPhones to transfer the settings and data previously stored on their old iPhone to their new iPhone from these backups. Additionally, Apple devices routinely share data between multiple devices such as iPhones, iPad tablets, iMac computers, MacBook laptops, and non-Apple computers.

46. As described in more detail below, there is evidence that WINEGEART had in her possession a digital device while at the U.S. Capitol on January 6, 2021. In addition, based on photos and videos of the offenses that date, numerous persons committing the Target Offenses possessed digital devices that they used to record and post photos and videos of themselves and others committing those offenses. Further, based on the investigation, numerous persons committing the Target Offenses possessed digital devices to communicate with other individuals to plan their attendance at the

gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

47. Moreover, it is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet last updated on April 7, 2021, The Pew Research Center for Internet & Technology estimated that 97% of Americans owned at least one cellular phone, and 85% of Americans own at least one smartphone. *See* Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile/> (last visited July 7, 2022).

48. The property to be searched includes any mobile phone owned, used, and controlled by WINEGEART, including but not limited to a cellular device associated with telephone number \*\*\*-\*\*\*-0028.

49. Investigative efforts conducted by the affiant revealed that the Device identified as owned, used, and controlled by WINEGEART was with her inside the restricted area of the United States Capitol on January 6, 2021.

- a. Witness 3, one of WINEGEART's friends, stated that WINEGEART stated she was at the U.S. Capitol on January 6, 2021, and sent a photograph of herself on Capitol grounds swinging a long wooden pole at the window of a door marked as "House of Representatives."
- b. WINEGEART sent text messages to Witness 3 stating that she would send videos and stated that "[e]veryone was filming[,] We have it from all angles."
- c. Based on the above information, your Affiant believes that the Device will contain incriminating evidence, fruits, instrumentalities, or



contraband related to the suspected offense and that the information described in Attachment B remains stored on the Device(s).

- d. Investigators have reason to believe that the Device is currently located on WINEGEART's person or at 323 North 8th Street, Fairview, Oklahoma because that is the current address of record of WINEGEART, and that is the address where your affiant previously interviewed WINEGEART.

50. A records search revealed two vehicles—a black 2012 Porsche Cayenne, bearing Oklahoma tag KMY-732, VIN# WP1AA2A3CLA10469 and a blue 2013 Nissan Titan, bearing Oklahoma tag HCD-192, VIN# 1N6BA0ECXDN315225—are registered to WINEGEART's husband at the same address as the PREMISES. Additionally, on June 8, 2022, WINEGEART posted a message on her Facebook account noting that she drives a “black on black” vehicle and attached a photograph of the interior of a Porsche Cayenne with black interior.



**TECHNICAL TERMS**

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

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

i. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless 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, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and

video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

- ii. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) 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.
- b. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between

devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- c. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

52. As described above and in Attachment B, this application seeks permission to search for fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, including, but not limited to any mobile phone owned, used, and controlled by WINEGEART, including but not limited to a cellular device associated with telephone number \*\*\*-\*\*\*-0028, 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. 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, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

- a. Individuals who engage in criminal activity, including violations of 18 U.S.C. § 1752(a)(1), 18 U.S.C. § 1752(a)(2), 40 U.S.C. § 5104(e)(2)(D), 40 U.S.C. § 5104(e)(2)(F), and 18 U.S.C. § 1361 (the “Target Offenses”), use digital devices, like the Device(s), to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device(s), documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other “Short Message Service” (“SMS”) messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator’s contact information; (2) keep a record of illegal transactions for future reference; (3) keep an

accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation. During this investigation, your affiant reviewed digital evidence purportedly demonstrating that WINEGEART had or used her cell phone while at Capitol grounds on January 6, 2021.

- 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 smart phone, 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.

53. As further described in Attachment B, 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 device(s) 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, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

- a. Forensic evidence on a digital device can 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.
- b. 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.
- c. 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.

- d. 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.
- e. I know that when an individual uses a digital device to record themselves committing unlawful acts, namely 18 U.S.C. § 1752(a)(1), 18 U.S.C. § 1752(a)(2), 40 U.S.C. § 5104(e)(2)(D), 40 U.S.C. § 5104(e)(2)(F), and 18 U.S.C. § 1361 (the "Target Offenses"), the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the

crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

**METHODS TO BE USED TO SEARCH DIGITAL DEVICES**

54. 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, I know that:

- a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.
- b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed,

encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

- c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.
- d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the

extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for smart phones and other digital devices do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if



certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

- e. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile

application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

- f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

55. 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 B, law enforcement personnel executing this search warrant will employ the following procedures:

- a. Upon securing the PREMISES, or upon arrest, 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 B 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 or upon arrest. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.
- b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents;



“scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

- c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

**BIOMETRIC ACCESS TO DEVICE(S)**

56. This warrant permits law enforcement agents to obtain from the person of WINEGEART (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 Device(s) requiring such biometric access subject to seizure pursuant to this warrant for

which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

57. I know 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.

58. 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.

59. 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.

60. 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.

61. 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.

62. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the Device(s) 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 Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

63. I also know 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. 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.

64. Due to the foregoing, if law enforcement personnel encounter any Device(s) 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 the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to



unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

65. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) 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 Device(s). 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 person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. 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.

66. Law enforcement personnel will commence the execution of this search and seizure warrant upon the PREMISES during daytime hours (between 6:00 a.m. and 10:00 p.m.), as early as practicable.

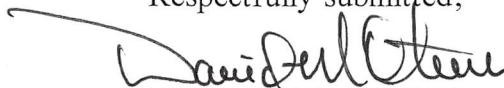
**REQUEST FOR SEALING**

67. I further request that the Court order that all papers in support of this warrant, including the affidavit, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

**CONCLUSION**

68. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,



Task Force Officer David Otwell  
Federal Bureau of Investigation

Subscribed and sworn to before me on July 18<sup>th</sup>, 2022.



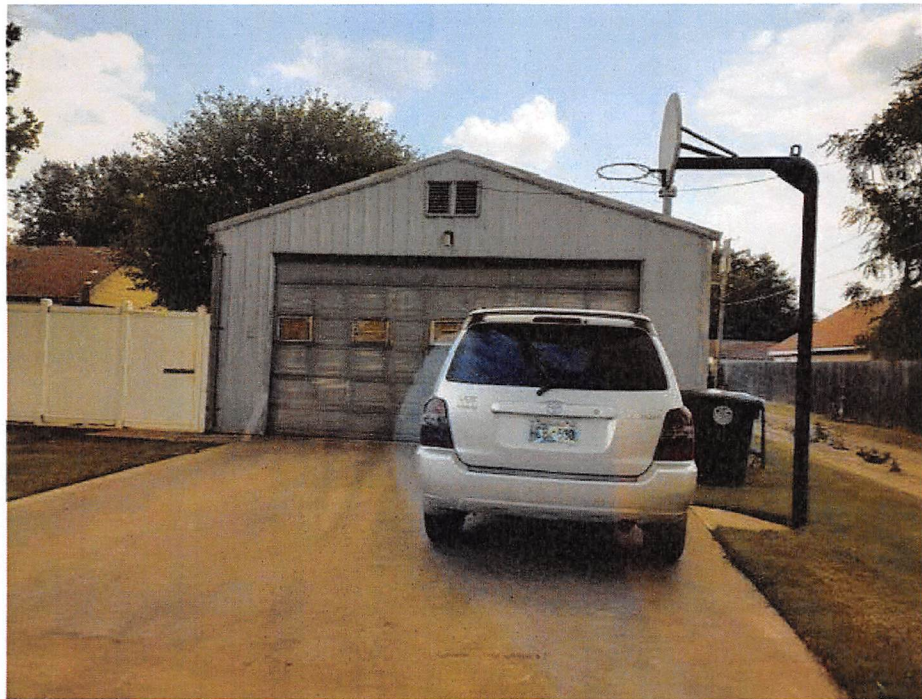
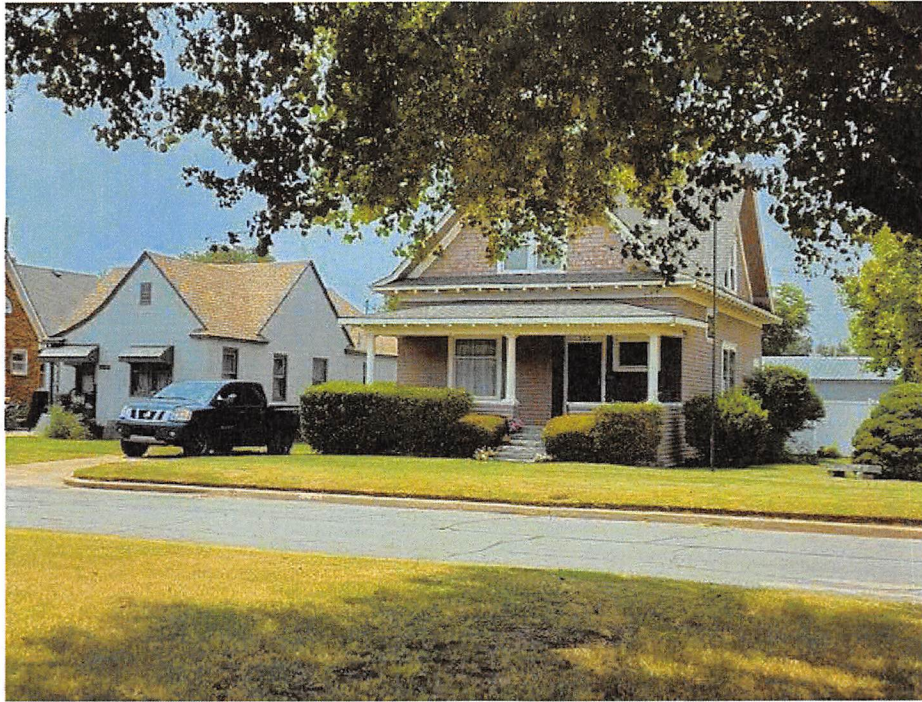
SUZANNE MITCHELL  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

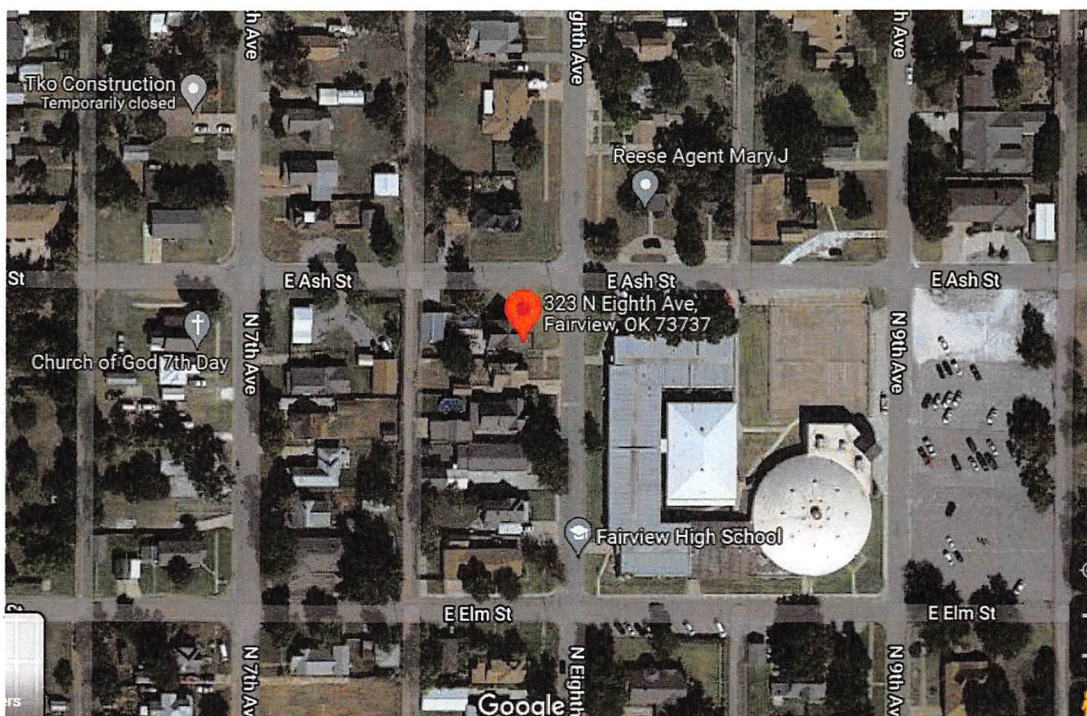
*Property to be searched*

The property to be searched is 323 North 8th Street, Fairview, Major County, Oklahoma (hereinafter "PREMISES"), further described as a two-story single-family residence situated on the southwest corner of East Ash Street and Eighth Avenue, with wood siding painted in a light salmon color on the upper and lower level of the residence, white trim around the windows and doors, black numbers "323" affixed above the front door which faces east, a front door that has a screen door attached with black burglar bars, and the numbers "323" painted in black on the curb in front of the residence. The front of the PREMISES faces east and is across the street from the Fairview High School. The PREMISES has a detached grey metal building with a two-car garage overhead door. The metal building has a cement paved driveway and there is a white plastic privacy fence between the PREMISES and detached garage. Two cars are registered to this address: (1) a black 2012 Porsche Cayenne, bearing Oklahoma tag # KMY-732, VIN No. WP1AA2A23CLA10469, and (2) a blue 2013 Nissan Titan, bearing Oklahoma tag # HCD-192, VIN No. 1N6BA0ECXDN315225.









**ATTACHMENT B**

*Property to be seized*

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 1752(a)(1), 18 U.S.C. § 1752(a)(2), 18 U.S.C. § 1752(a)(4), 40 U.S.C. § 5104(e)(2)(D), 40 U.S.C. § 5104(e)(2)(F), and 18 U.S.C. § 1361 (the “Target Offenses”) that have been committed by DOVA WINEGEART (“the Subject”) and other identified and unidentified persons, as described in the search warrant affidavit; including, but not limited to, any mobile cellular device, including a cellular device that is associated with telephone number \*\*\*-\*\*\*-0028. Cellular devices owned, used, or controlled by WINEGEART may contain:

- a. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- b. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;
- c. Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, *i.e.*, the certification process of the 2020 Presidential Election;
- d. Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, *i.e.*, the certification process of the 2020 Presidential Election;
- e. Evidence relating to a conspiracy to illegally enter and/or occupy the U.S. Capitol Building on or about January 6, 2021;
- f. Evidence concerning the breach and unlawful entry of the United States Capitol, and any conspiracy or plan to do so, on January 6, 2021;
- g. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;

- h. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;
  - i. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;
  - j. Evidence of any conspiracy, planning, or preparation to commit those offenses;
  - k. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
  - l. Evidence concerning materials, devices, or tools that were used to unlawfully enter the U.S. Capitol 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;
  - m. Evidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
  - n. Evidence of the state of mind of the subject and/or other co-conspirators, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and
  - o. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.
2. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:
- a. Any records and/or evidence revealing the Subject's presence at the January 6, 2021, riot;
  - b. Any physical records, such as receipts for travel, which may serve to prove evidence of travel of to or from Washington D.C. from December of 2020 through January of 2021;

- c. The Subject's (and others's) motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
- d. The Subject's (and others's) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021.

3. During the execution of the search of the PREMISES described in Attachment A, or upon arrest, law enforcement personnel are also specifically authorized to obtain from WINEGEART (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 person(s)' 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.

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.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed 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 disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.