ATTACHMENT A

Property to be searched

The property to be searched ("the Device") is a black, Samsung Galaxy Ultra 21 in a black phone case, with Model Number SM-G998U and IMEI: 356544763002182, presently in the FBI Evidence Unit, located at 600 Arch Street, Philadelphia, PA, 191106.

ATTACHMENT B

Property to be seized

The items to be seized from the Device are:

Fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1752(a)(1) and (2) (entering and remaining in and disorderly conduct in a restricted building or grounds), and 40 U.S.C. §§ 5104(e)(2)(D) and (G) (disorderly conduct and parading, demonstrating, or picketing in a Capitol Building) (collectively, the "SUBJECT OFFENSES"), committed by Isaiah GIDDINGS ("GIDDINGS") and others on or about January 6, 2021, as described in the search warrant affidavit, including:

a. Records or information concerning unlawful entry into the U.S. Capitol on January 6, 2021;

b. Records or information concerning the riot and/or civil disorder at the U.S. Capitol on January 6, 2021;

c. Records or information relating to 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.

d. Records or information relating to assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the U.S. Capitol on January 6, 2021;

e. Records or information concerning efforts to conceal evidence of the offenses under investigation, or to flee prosecution for the same.

f. Records or information that constitute evidence of GIDDINGS's affiliation with the Proud Boys or communications with members thereof.

g. Records and information—including but not limited to documents, communications, emails, text and social media messages, online postings and chats, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to GIDDINGS's and others'

   i. motive and intent for traveling to Washington, D.C., on or about January 6, 2021;

   ii. plans for travel to and activity in Washington, D.C., on or about January 6, 2021;

   iii. mode of travel, travel expenses, and travel logistics on or about January 6, 2021; and

   iv. activities in and around Washington, D.C. on or about January 6, 2021.

h. evidence of who used, owned, or controlled the Device 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;

i. evidence of software, or the lack thereof, that would allow others to control the Device, 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;

j. evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

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

l. evidence of the times the Device was used;

m. passwords, encryption keys, and other access devices that may be necessary to access the Device;

n. documentation and manuals that may be necessary to access the Device or to conduct a forensic examination of the Device;

o. records of or information about Internet Protocol addresses used by the Device; and

p. records of or information about the Device'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.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF ONE BLACK SAMSUNG GALAXY ULTRA 21, IMEI 356544763002182, IN THE CUSTODY OF THE FBI EVIDENCE UNIT IN PHILADELPHIA, PA	**SW No. 22-MJ-27**

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

I, Malachi Nkosi, 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 a black, Samsung Galaxy Ultra 21 in a black phone case, with Model Number SM-G998U and IMEI: 356544763002182, presently in the FBI Evidence Unit, located at 600 Arch Street, Philadelphia, PA, 19106 ("the Device"), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since August 2020. I am currently assigned to the FBI Philadelphia Division. Since February 2021, I have been assigned to the Joint Terrorism Task Force (JTTF) as a Special Agent. My duties with the JTTF include investigations of domestic terrorism and criminal violations of Title 18 of the U.S. Code, including but not limited to acts of terrorism, threats of violence to public and private entities, and "sovereign citizen" matters.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter. Unless otherwise stated, the information in this Affidavit is either personally known to me, has been provided to me by other individuals, or is based on a review of various documents, records, and reports. Because this Affidavit is submitted for the limited purpose of establishing probable cause to support an application for a search warrant, it does not contain every fact known by me or the United States. The dates listed in this Affidavit should be read as "on or about" dates.

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. § 371 (conspiracy), 18 U.S.C. § 1752(a)(1) and (2) (entering and remaining in and disorderly conduct in a restricted building or grounds), and 40 U.S.C. §§ 5104(e)(2)(D) and (G) (disorderly conduct and parading, demonstrating, or picketing in a Capitol Building) (collectively, the "SUBJECT OFFENSES"), have been committed by Isaiah GIDDINGS (GIDDINGS) and other identified and unidentified persons. On December 8, 2021, a magistrate judge in the District of Columbia signed a criminal complaint charging GIDDINGS with criminal violations of 18 U.S.C. § 1752(a)(1) and (2) and 40 U.S.C. §§ 5104(e)(2)(D) and (G), in connection with his activities in and around the U.S. Capitol on January 6, 2021, in Case No. 21-mj-689 (D.D.C.). There is also probable cause to search the Device, further described in Attachment A, for the things described in Attachment B.

PROBABLE CAUSE

January 6, 2021 Breach of the U.S. Capitol

5. The U.S. Capitol is secured 24 hours a day by U.S. Capitol Police. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by U.S. Capitol Police. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol. On January 6, 2021, the exterior plaza of the U.S. Capitol was also closed to members of the public.

6. On January 6, 2021, a joint session of the U.S. Congress convened at the U.S. Capitol, which is located at First Street, SE, in Washington, D.C. During the joint session, elected members of the U.S. House of Representatives and the U.S. Senate were meeting in separate chambers of the Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which had taken place on November 3, 2020. The joint session began at approximately 1:00 p.m. 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.

7. 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 U.S. Capitol Police were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

8. 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 the U.S.

Capitol Police attempted to maintain order and keep the crowd from entering the Capitol; however, around 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of the U.S. Capitol Police, as others in the crowd encouraged and assisted those acts.

9. Shortly thereafter, at approximately 2:20 p.m., members of the U.S. House of Representatives and U.S. Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. Accordingly, the joint session of the U.S. Congress was effectively suspended until shortly after 8:00 p.m. Vice President Pence remained in the U.S. Capitol from the time he was evacuated from the Senate chamber until the session resumed.

10. During national news coverage of the aforementioned events, video footage, including that 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.

Isaiah GIDDINGS's Participation in the Breach of the U.S. Capitol

11. Isaiah GIDDINGS was born in 1992 and resides in Philadelphia, Pennsylvania.

12. On March 17, 2021, Zachary Rehl, a resident of Philadelphia, Pennsylvania, was arrested on charges related to the January 6, 2021, breach of the U.S. Capitol. Pursuant to legal process, law enforcement searched the contents of a phone belonging to Rehl that was obtained at the time of his arrest.

13. Among the contents of Rehl's phone was a group text message chain (hereinafter, the "Group Text") that included Rehl, Isaiah GIDDINGS (listed in Rehl's contacts as "Issah Pb"),

and three other individuals: Freedom Vy (listed in Rehl's contacts as "Ross Bob (freedom) pb"), Brian Healion (listed as "Tormond PB"), and a fifth individual (hereinafter Person 1).[1] Healion and Vy also reside in the Philadelphia area.

14. Rehl's phone also contained content from Telegram message strings that included GIDDINGS, Healion, and Vy, among others. Rehl's Telegram handle was "Captain Trump." The Telegram handles for GIDDINGS ("Issah PB"), Healion ("Tormond PB"), and Vy ("Freedom Pb") are consistent with the names listed in Rehl's phone contacts. The individuals were all members of a Telegram message group that was created by Rehl (hereinafter "Rehl Telegram Group"), which contained messages from as early as November 19, 2020, to at least February 2, 2021, including messages related to the events of January 6, 2021, at the U.S. Capitol.

Coordinated Travel to Washington, D.C. on January 5, 2021

15. At 2:52 p.m. on January 5, 2021, Person 1 requested emergency contact information and blood types from the other individuals on the Group Text. In response, GIDDINGS provided his blood type and multiple contacts, including a file containing the name, phone number, and

---

[1] Based on the content of the communications in the Group Text and other evidence gathered during this investigation, it appears that "PB" and "Pb" are references to "Proud Boys," and that GIDDINGS, Healion, Vy, Rehl, and Person 1 were known to each other at least in part based on their common membership in the Philadelphia chapter of the Proud Boys, which defines itself as a "pro-Western fraternal organization for men who refuse to apologize for creating the modern world; aka Western Chauvinists." As alleged in the First Superseding Indictment in Rehl's case, Rehl was the president of the Philadelphia chapter of the Proud Boys. This affiliation information is included because it is relevant to context and identification. Person 1 was not physically present in Washington, DC, on January 6.

photograph of a sibling. Healion provided the name, phone number, and address of his fiancé. Healion also wrote, "Not sure the blood type I'm trying to find out," to which Person 1 responded, "Ok brian gotcha." Vy provided his blood type and the name and phone number of a sibling. Rehl also provided his blood type and the name and phone number of his wife.

16. Listed below are the sender, content, and time (converted from UTC to EST) of selected additional messages in the Group Text on January 5, which appear to reflect Rehl, GIDDINGS, Healion, and Vy coordinating their travel from Philadelphia to Washington, D.C. that evening:

Vy:	"Im headed out soon, gotta grab a few things , freshen up and get brian" (3:12pm)
Vy:	"We'll be ready for pickup at 5" (3:12pm)
Vy:	"[providing his home address], Philadelphia pa 19142 (3:13pm)
Person 1:	"Im not going" (3:13pm)
Healion:	"Hey free[2] after we meet what is the plan to have Zach pick us up from your house are we going to his house and heading out from there" (3:46pm)
	***
Rehl:	"Im ready my dudes" (3:53pm)
GIDDINGS:	"I'm at [Person 1's first name]'s I'm ready" (3:53pm)
	***
GIDDINGS:	"I'm jumping in the shower now Zach" (4:22pm)
Rehl:	"Im my way to get issah, had to get the radios from the legion" (5:04pm)
	***
GIDDINGS:	"Ok im ready Pres to come when you get here" (5:04pm)
Rehl:	"Ok" (5:07pm)
Rehl:	"28 mins" (5:25pm)
Rehl:	"I'm here" (5:50pm)
Person 1:	"Hows it going guys" (7:49pm)
GIDDINGS:	"Great so far hour away from DC" (7:51pm)
Person 1:	"OK" (7:59pm)

[2] In writing "Hey free," Healion appears to be addressing Vy, whose first name is "Freedom."

17. According to records obtained from the Darcy Hotel in Washington, D.C., Rehl checked into the hotel on January 5, 2021 with three accompanying guests, who were listed on the hotel records as "Healion, Brian"; "Giddings, Isaiah"; and "Yeng, Joseph."[3]

Conduct on January 6, 2021, and Identification of HEALION, Vy, and Giddings

18. At 9:47 a.m. on January 6, 2021, Person 1 sent two voice messages to the Group Text. The first stated, "Hey y'all have a good day. Dress warm. I love y'all. Be safe. Love y'all." The second stated, "And whatever info I come across today I'll get out to you Zach, get it out to wherever it needs to go. Just let me know where it needs to go."

19. At 10:30 a.m., Healion sent the below photograph to the Rehl Telegram Group, showing two individuals near the Washington Monument that morning.

[3] Your affiant submits that "Yeng, Joseph" is likely an alias for Vy.

20. The FBI reviewed images of Vy and Healion obtained from government databases and identified the individual on the left as Vy and the individual on the right as Healion. The identifications of Vy and Healion are corroborated by, among other things, the fact that the photograph appears to be a "selfie" taken by Healion and was posted from Healion's account, as well as the evidence establishing Healion's and Vy's coordinated activity on January 5 and 6, 2021.

21. During the course of the investigation, law enforcement interviewed a witness (hereinafter W-1) who had a prior association with Healion. W-1 was shown a photo array of more than ten individuals, including Healion. W-1 identified Healion in the photo array as "Brian." Thereafter, W-1 was also shown the above image and confirmed that the person depicted on the right is the person known to W-1 as "Brian."

22. W-1 also had a prior association with Vy. W-1 was shown a photo array of more than ten individuals that included a photograph of Vy. W-1 identified Vy in the photo array as a person known to W-1 as "Free" or "Freedom." Thereafter, W-1 was shown the above image and confirmed that the person depicted on the left is the person known to W-1 as "Freedom."

23. Shortly before 1:00 p.m. on January 6, 2021, a large crowd gathered near the pedestrian entrance to the Capitol grounds on First Street. The entrance, located near the Peace Monument, was secured by a small number of U.S. Capitol Police, who stood behind a waist-high metal barrier. The image below, which is a screen shot from publicly available video, depicts this scene, looking toward the U.S. Capitol from near the Peace Monument.

24. Shortly after the above image was captured on video, two men advanced toward the waist-high metal gate. The crowd followed, and within minutes, the crowd overwhelmed the U.S. Capitol Police officers seen at the top of the steps in the image above, advancing on the Capitol. Near the entrance to the plaza to the west of the Capitol ("West Plaza"), USCP were guarding another set of barricades, along with more permanent fences. Shortly thereafter, rioters again overwhelmed the officers, entering the West Plaza, ultimately reaching the elevated terrace ("Upper West Terrace") where they were able to enter the building as described further above.

25. Immediately below is a photograph recovered from Rehl's phone that depicts Rehl (on the left, wearing goggles, a camouflage hat, and black clothing) and others posing on the Upper West Terrace of the U.S. Capitol during the breach.

26. The FBI identified the individual circled in yellow above as GIDDINGS, based on the similarity of this individual to database photographs of GIDDINGS. W-1 also had a prior association with GIDDINGS and was shown a photo array of more than ten individuals, including GIDDINGS. W-1 identified GIDDINGS in the photo array as "Isaiah." Thereafter, W-1 was also shown the above image and confirmed that the person circled in yellow is the person known to W-1 as "Isaiah."

27. Kneeling in the front right of the image is the person identified above as Healion, although his face is obscured by dark goggles and a black gaiter. Kneeling in the front left of the image is the person identified above as Vy, as evidenced by his facial appearance, clothing, and American flag gaiter.

28. At 7:01 p.m. on January 7, 2021, Rehl posted the below image to the Rehl Telegram Group along with the statement, "Badass pic in DC." The image depicts Rehl, who is in the foreground and appears to be taking the photograph as a "selfie." On the left side of the image, wearing a red hat and an American flag gaiter is the person identified above as Vy. On the right side of the image, wearing a camouflage hat, blue or gray gaiter, gray shirt, and plaid jacket is the person identified above as GIDDINGS. Standing behind GIDDINGS, wearing a red hat, goggles, and black gaiter, is an individual that I believe to be Healion.

29. GIDDINGS, Vy, Rehl, and Healion entered the U.S. Capitol from the west side of the building near the U.S. Senate, and images and video depict them inside the building at various locations. The image immediately below, recovered from Rehl's phone, was sent by text from Healion to Rehl. This photograph depicts from left to right, Healion, Vy, Rehl, and GIDDINGS, all of whose appearance is consistent with other images of these individuals on January 6, 2021, inside the office of U.S. Senator Jeff Merkley (Oregon) during the breach.

30. According to records obtained from the Darcy Hotel in Washington, D.C., Rehl checked out of the Darcy Hotel on January 7, 2021. At 11:04 a.m. on January 7, 2021, Person 1 texted "Yo yo how u guys doing" to the Group Text, which led to the following messages:

Vy:	"Checking out on our way home (11:05am)
Person 1:	"Ok" (11:05pm)
Person 1:	"B safe" (11:05pm)
Person 1:	"All accounted for" (11:05am)
GIDDINGS:	"Yes we have everything and everyone all accounted for all safe a few bruise but we expected that none of our Philly guys had any PB gear the entire event just plain trump supporters from beginning to end thank for the constant check ups and the law enforcement and news updates really really funkin helpful see you when I get back" (11:33am)
Person 1:	"Np bro just doing what can to keep my family safe."

The Device to be Searched

31. On December 10, 2021, GIDDINGS was arrested at 5617 Chew Avenue, Philadelphia, PA 19138, which was determined to be GIDDINGS's residence. Upon his arrest, GIDDINGS requested that he be permitted to bring his cell phone. GIDDINGS's father, who was present, brought the Device to be searched from the residence and handed it to a law enforcement officer participating in the arrest.

32. The Device is a black, Samsung Galaxy Ultra 21 in a black phone case, with Model Number SM-G998U and IMEI: 356544763002182, presently in the FBI Evidence Unit, located at 600 Arch Street, Philadelphia, PA, 191106.

33. Following his arrest, GIDDINGS and the Device were transported to the FBI field office in Philadelphia.

34. In a post-arrest interview, having been advised of his rights, GIDDINGS agreed to speak to law enforcement. During the interview, GIDDINGS admitted that he had travelled to Washington, D.C., and that he entered the U.S. Capitol on January 6, 2021. GIDDINGS admitted to wearing a bullet-proof vest and to carrying a knife and mace into the U.S. Capitol.

35. GIDDINGS further stated that he had a phone with him, and that he used the phone to take photographs and video at the U.S. Capitol on January 6, 2021. That phone, however, was not the Device, which GIDDINGS obtained after that date. Both phones were serviced by AT&T. When asked if he moved information from the first phone to the Device when he obtained the Device, GIDDINGS stated that he did, although he also stated that he deleted information, including photos and video, from the first phone because, as he stated, he did not want to get in trouble.

36. At the conclusion of the interview, GIDDINGS consented to a search of the Device

and signed a consent form. At that time, GIDDINGS stated to law enforcement, "You can look at the contacts and stuff. Contacts is definitely maybe up there if you look at the past contact. Past photos maybe, because this wasn't the phone that I had on January 6th. Like, you can look at the contacts and the photos. I believe they will all still be there." He said that those items "could possibly transfer over to this phone." Asked if he transferred data from the first phone to the Device himself, GIDDINGS said he "did it at AT&T," and he agreed that AT&T transferred data from the first phone to the Device.

37. Subsequent to this interview, GIDDINGS stated to law enforcement that he needed the Device back for the weekend. After law enforcement referenced GIDDINGS's earlier consent to search, GIDDINGS requested to have the Device back. An FBI agent advised GIDDINGS that the FBI would retain possession of the Device and issued GIDDINGS a property receipt. The Device is currently stored at the FBI Evidence Unit, located at 600 Arch Street, Philadelphia, PA, 19106.

38. Based on the information provided by GIDDINGS, a search of the Device is likely to contain evidence of GIDDINGS's presence at the U.S. Capitol on January 6, 2021, and evidence of the Subject Offenses, committed by GIDDINGS and/or others.

39. As exemplified by the Group Text and Rehl Telegram Group, in which GIDDINGS participated, and the photographs from January 6 that Healion sent to Rehl and the Rehl Telegram Group, including GIDDINGS, individuals engaged in criminal conduct, such as the SUBJECT OFFENSES, sometimes use online accounts, to communicate with co-conspirators and criminal associates regarding, among other things, travel and meeting plans. I would expect to find evidence of such communications on any devices belonging to GIDDINGS.

40. Furthermore, information concerning contacts, photographs, group memberships, and patterns of electronic communications with individuals associated with similar social media accounts can provide evidence that is probative of the users' and any co-conspirators' social networks, contacts, travel, banking and other financial facilities, and potential knowledge of or involvement in one or more of the Subject Offenses.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

41. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Device, in whatever form they are found. 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 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 the types of conspiratorial crimes discussed herein 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; and (2) plan coordinated activities.

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.

42. 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. 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.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

43. 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 – whether, for example, desktop computers, mobile devices, or portable storage 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 computers, 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, including tablets, 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.

44. 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. The Device, 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.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

45. Because forensic examiners will be conducting their search of the digital devices in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

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

Respectfully submitted,

s/ Malachi Nkosi
Malachi Nkosi
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on January 6th, 2022.

___/s/ Lynne A. Sitarski_____
HONORABLE LYNNE A. SITARSKI
UNITED STATES MAGISTRATE JUDGE