Exhibit 1

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of The premises located at [redacted] CA	)	Case No. 8:21-MJ-00038

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

See Attachment A-1

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

See Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1752	Entering or Remaining in a Restricted Building or Grounds/Disruption of Orderly Conduct of Government Business

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

/s/
Applicant's signature

FBI Special Agent Jessica Salo
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 1/26/2021

/s/ Autumn D. Spaeth
Judge's signature

City and state: Santa Ana, CA

Hon. Autumn D. Spaeth, U.S. Magistrate Judge
Printed name and title

AUSA: Paul C. LeBlanc 213-393-6933

AFFIDAVIT

I, Jessica Salo, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since November 2014. Prior to becoming an agent, I worked as an Intelligence Analyst at the FBI for approximately six years. I am currently assigned to the Orange County Joint Terrorism Task Force, which investigates United States persons who commit violent criminal acts in furtherance of their political or social ideology. I have participated in several investigations involving individuals that committed criminal acts in furtherance of ideological goals, to include Racially Motivated Violent Extremists and Anti-Government/Anti-Authority Extremists. I successfully completed the 21 weeks of New Agent Training at the FBI Academy in Quantico, Virginia in 2015. During that time, I received training in physical surveillance, legal statutes and procedures, terrorism investigations, money laundering techniques, confidential source management, and electronic surveillance techniques.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of search warrants for the SUBJECT PREMISES, SUBJECT VEHICLES, AND PERSONS described below and in Attachments A-1, A-2, A-3, A-4, A-5, and A-6, for the items to be seized described in Attachments B-1 and B-2.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. PREMISES AND PERSONS TO BE SEARCHED

4. The premises, vehicles, and persons to be searched are:

a. [redacted] CA, the residence of Alan Hostetter ("HOSTETTER"), which is described in more detail in Attachment A-1 ("SUBJECT PREMISES 1");

b. A 2020 black Chevy Silverado truck, bearing California license plate number [redacted] and vehicle identification number [redacted], which is registered to HOSTETTER ("SUBJECT VEHICLE 1"). SUBJECT VEHICLE 1 is described in more detail in Attachment A-2;

c. The person of HOSTETTER, who is described in more detail in Attachment A-3;

d. [redacted] CA, the residence of Russell Taylor ("TAYLOR"), which is described in more detail in Attachment A-4 ("SUBJECT PREMISES 2");

e. A 2020 black Cadillac SUV, bearing California license plate number [redacted] and vehicle identification number

[redacted], which is registered to TAYLOR ("SUBJECT VEHICLE 2"). SUBJECT VEHICLE 2 is described in more detail in Attachment A-5; and

f. The person of TAYLOR, who is described in more detail in Attachment A-6.

IV. ITEMS TO BE SEIZED

5. The items to be seized are the evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1752 (Entering or Remaining in a Restricted Building or Grounds/Disruption of Orderly Conduct of Government Business)[1], as described in Attachments B-1 and B-2, which is incorporated herein by reference (the "SUBJECT OFFENSE").

V. SUMMARY OF PROBABLE CAUSE

6. As detailed below, on January 6, 2021, the United States Congress convened at the United States Capitol to count

---

[1] 18 U.S.C. § 1752(c)(1) defines "restricted building or grounds" as any posted, cordoned off, or otherwise restricted area--

(A) of the White House or its grounds, or the Vice President's official residence or its grounds;

(B) of a building or grounds where the President or other person protected by the Secret Service is or will be temporarily visiting; or

(C) of a building or grounds so restricted in conjunction with an event designated as a special event of national significance; and

(2) the term "other person protected by the Secret Service" means any person whom the United States Secret Service is authorized to protect under section 3056 of this title or by Presidential memorandum, when such person has not declined such protection.

18 U.S. Code § 3056(a)(1) includes the Vice President and Vice President-elect. Vice President Pence and Vice President-elect Kamal Harris were present in the Capitol on January 6, 2021.

and certify the Electoral College ballots from the November 2020 U.S. Presidential election. At approximately 2:00 p.m., a crowd of rioters gathered outside of the Capitol Complex – the grounds surrounding the Capitol building. Thereafter the crowd forcefully and unlawfully entered the Capitol grounds and the Capitol building. U.S. Capitol Police ("USCP") officers were overwhelmed as the crowd surged through the Capitol Complex. Many of the rioters travelled from outside of the Washington, D.C. area to join the riot. Many of the rioters posted, on social media platforms, pictures of themselves and others from inside the secure Capitol area.

7. HOSTETTER drove from Orange County, California to Washington, D.C. to participate in the riot. HOSTETTER posted several pictures of himself and others, including next to TAYLOR, illegally inside the Capitol Complex to publicly available social media platforms.

8. Several pictures of TAYLOR and others were located in media outlets and posted on publicly available social media platforms. These photos show TAYLOR illegally inside the secure Capitol complex, often times accompanied by HOSTETTER.

VI. STATEMENT OF PROBABLE CAUSE

A. Background on the January 6, 2011 Capitol Riots

9. Based on my training and experience, conversation with law enforcement personnel, review of Internet maps and news reports, I know the USCP, the FBI, and assisting law enforcement agencies are investigating the riot and related offenses that occurred at the United States Capitol Building, located at 1

First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

10. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

11. 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.

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

13. 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. 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.

14. 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.

15. At around 1:00 p.m., known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

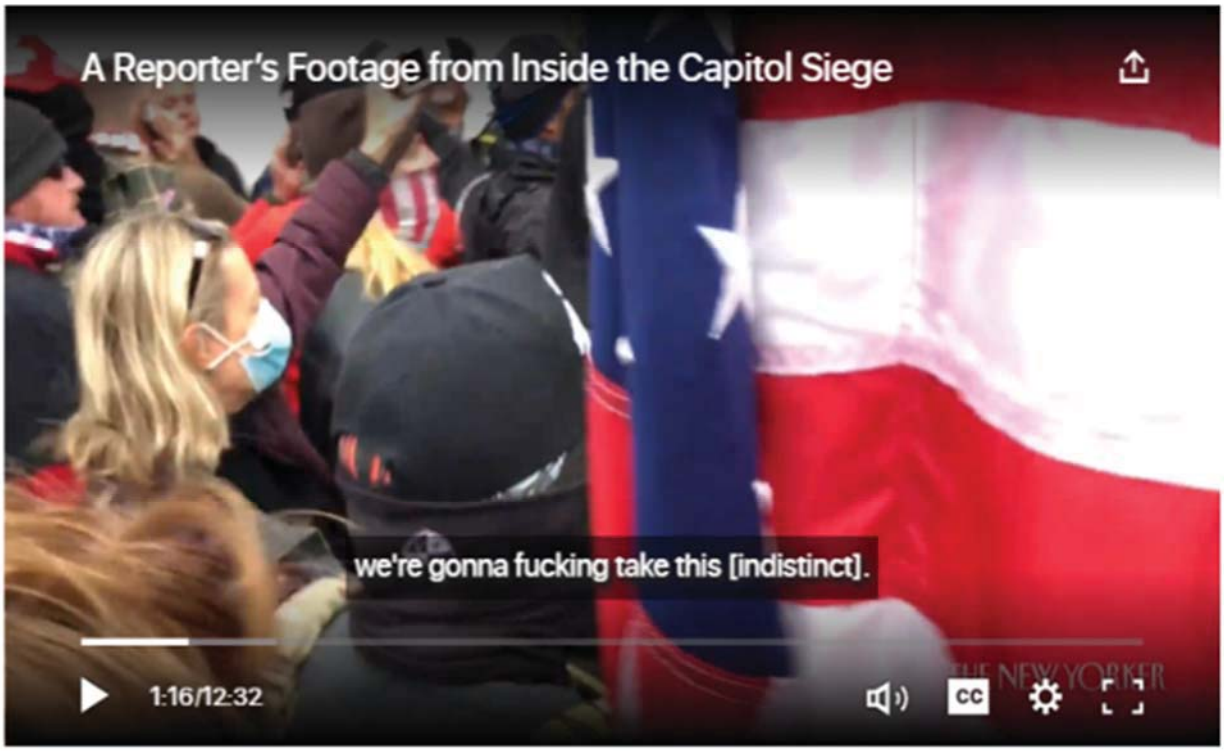
16. At around 1:30 p.m., USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

17. 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.

18. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by U.S. Capitol Police Officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

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



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

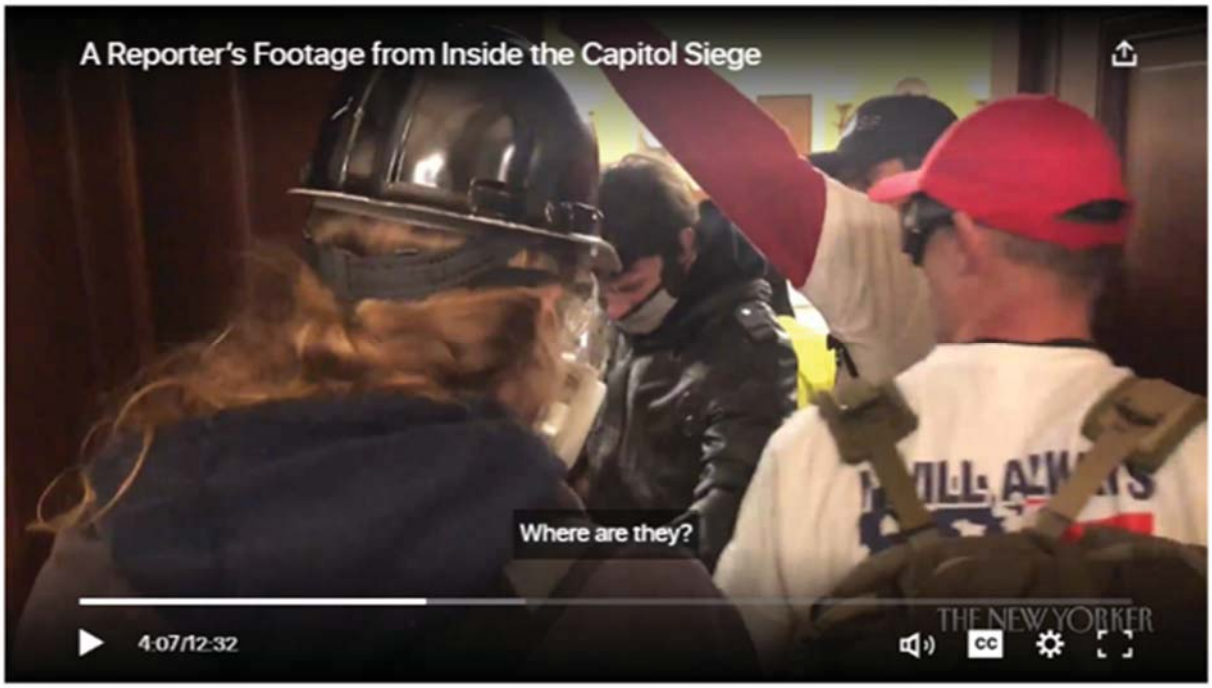
21. At approximately 2:30 p.m., known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on

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, several were admitted to the hospital, and at least one federal police officer died as a result of the injuries he sustained. 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.

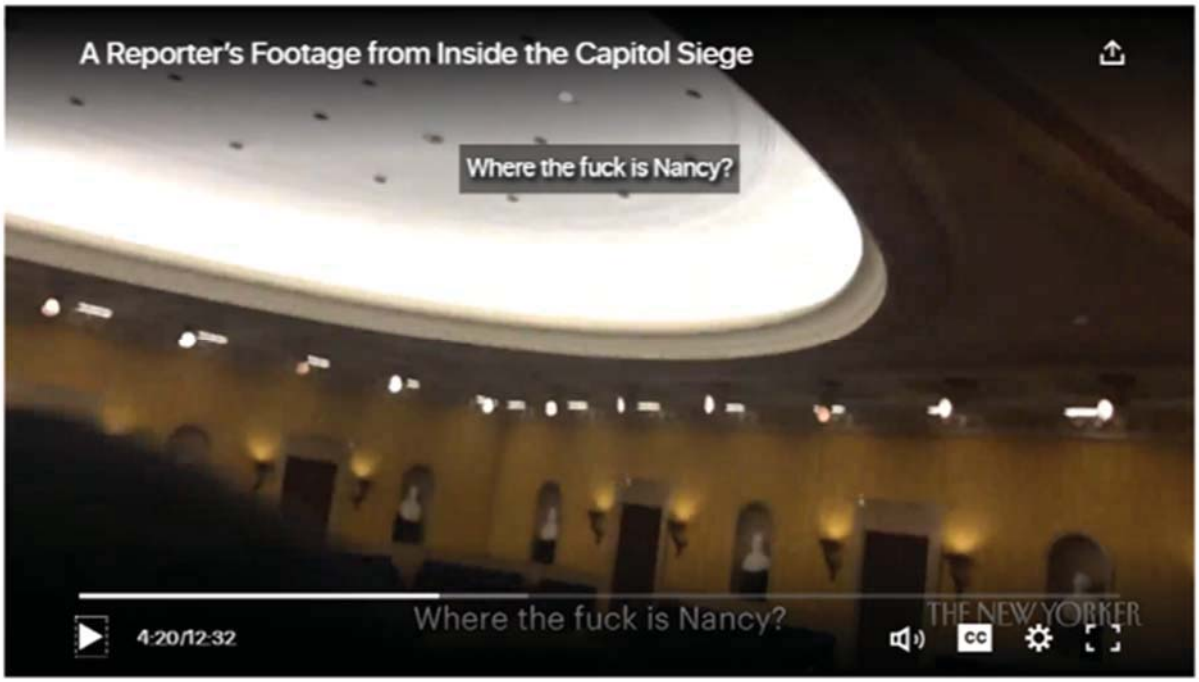
22. Also at approximately 2:30 p.m., USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

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

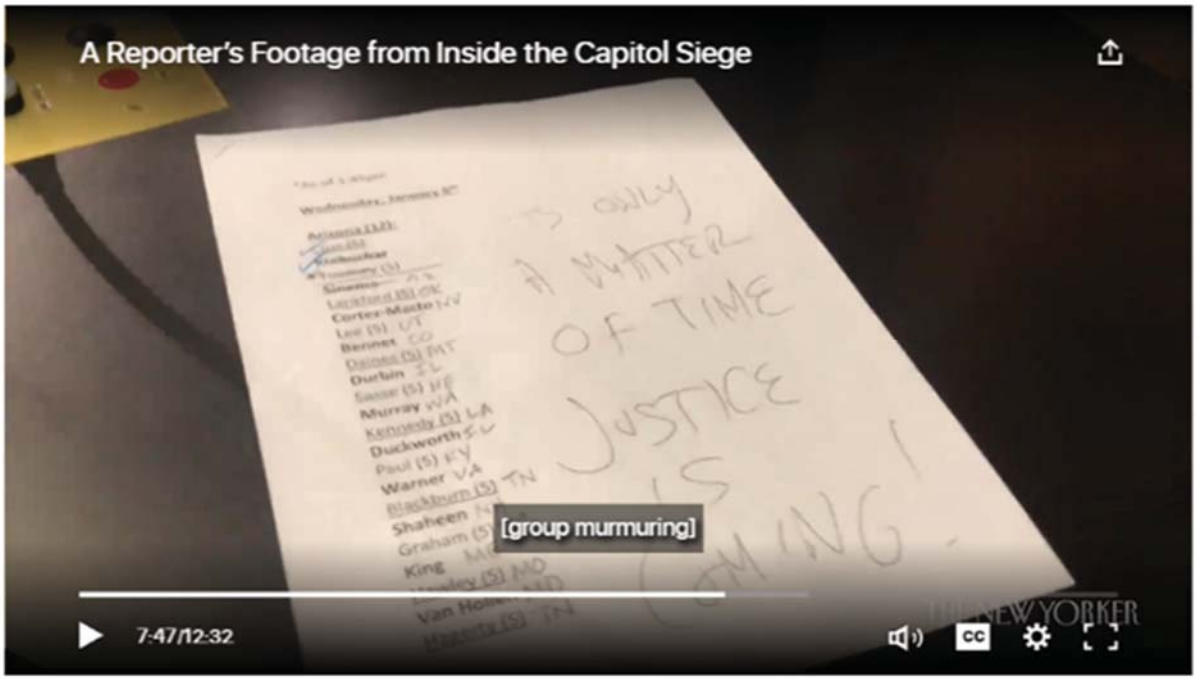
24. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, “Where are they?” as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word “they” is in reference to members of Congress.



25. 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.



26. An unknown subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated "A Matter of Time Justice is Coming."



27. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the US 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 were expected to be taken into custody.

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

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

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

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

32. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or

weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

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

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

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

36. 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.

B. Tipsters Identify HOSTETTER as Participating in the Capitol Rioters and HOSTETTER Posts Images on Social Media of the Riots from Inside the Capitol Complex

37. Between January 7 and 11, 2021, FBI Los Angeles received multiple tips, submitted online, via telephone, and via text, which I have reviewed, identifying HOSTETTER as one of the individuals present inside the Capitol Complex. According to an Orange County Register article, HOSTETTER is a former police

chief of La Habra, CA and a former Orange County Deputy Sheriff.[2] According to Internet searches, HOSTETTER retired as La Habra Police Chief in 2010 after a 23-year law enforcement career.[3]

38. On January 11, 2021, the Orange County Intelligence Assessment Center ("OCIAC")[4] provided me several screenshots from HOSTETTER's then-publicly available Instagram account, "@americanphoenixproject". The display name for @americanphoenixproject is "ALAN HOSTETTER". The profile description reads, "Founder of American Phoenix Project, Grandpa, Retired Police Chief and former Army Infantryman. Sound Therapist / MPA americanphoenix.org." The profile is public and contains several pictures of HOSTETTER, which I confirmed match his California Department of Motor Vehicle photograph. According to its website, the goal of the American Phoenix Project "is nothing less than a second American revolution." The American Phoenix Project seeks to enact a "Convention of States" under Article V of the U.S. Constitution. The group formed following the emergence of COVID-19 in the

---

[2] https://www.ocregister.com/2020/05/21/arrests-made-at-san-clemente-rally-fighting-stay-at-home-order (last viewed on January 13, 2021). Based upon my review of HOSTETTER's criminal history, I know he was arrested on May 21, 2020 for violation of California Penal Code Section 404.6(A) causing a riot and destroying property. To date, no charges have been filed in that matter.

[3] https://www.ocregister.com/2010/09/29/la-habra-police-chief-retires/ (last viewed on January 13, 2021).

[4] The Orange County Intelligence Assessment Center provides an integrated, multi-disciplined, information and intelligence sharing network to collect, analyze, and disseminate information on all criminal risks and safety threats to law enforcement.

United States and governmental responses to the COVID-19 pandemic in 2020.

39. Several Instagram posts by @americanphoenixproject which appear to be from January 6, 2021 are tagged with "United States Capitol." These posts appear to depict the U.S. Capitol building and appear to be taken from within the secure area of the Capitol Complex. All of the photos posted that I reviewed appear to be taken by a smart phone with a camera or a digital camera.

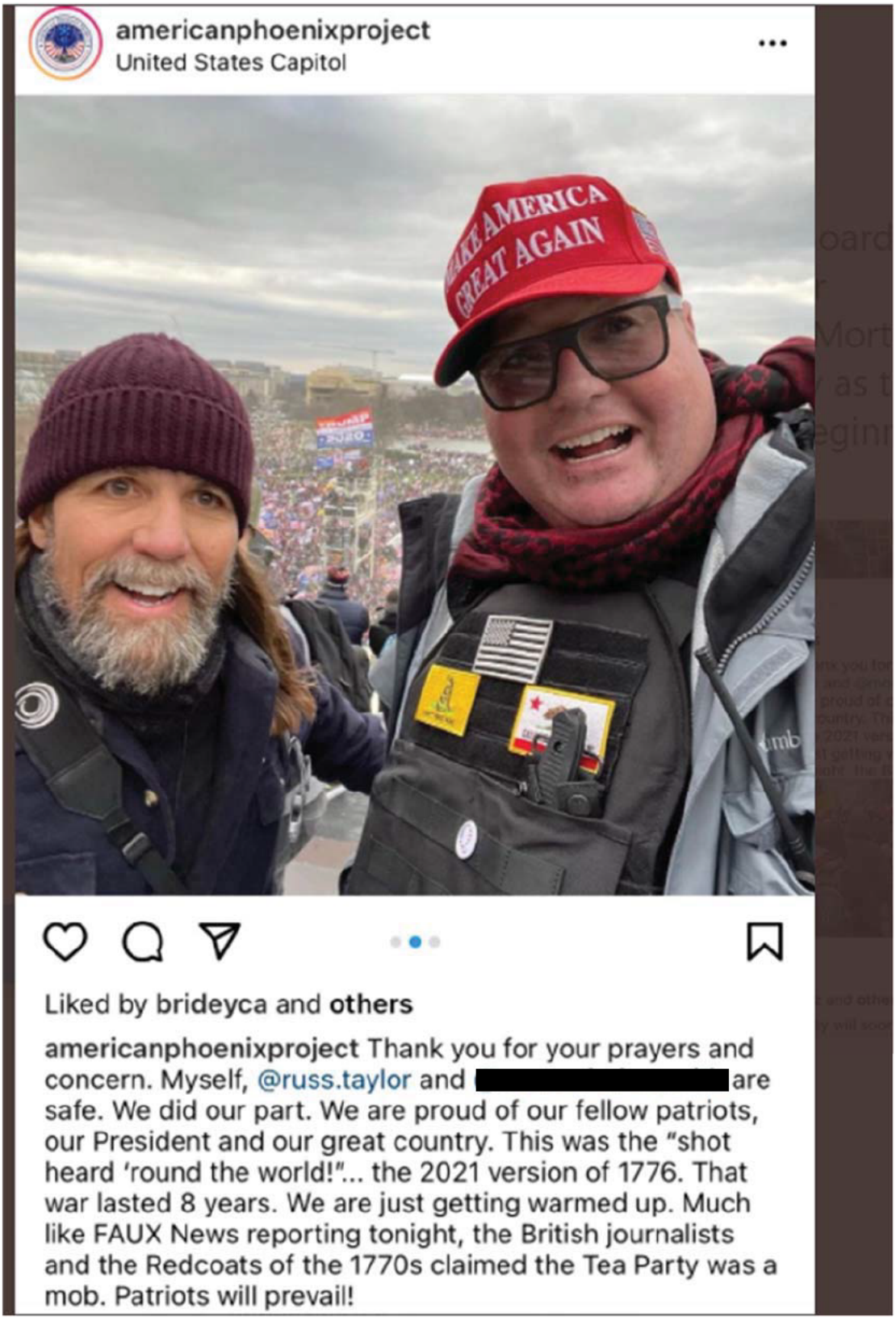
40. Based on the images depicted and my knowledge of the events on January 6, 2021, I believe the photos in the Instagram posts described above were taken on January 6, 2021. On January 13, 2021, I reviewed Instagram @americanphoenixproject and found these posts have been deleted.

41. According to a screenshot of a post @americanphoenixproject made on December 16, 2020, HOSTETTER wrote, "The time has come when good people may have to act badly...but not wrongly." (ellipsis in original.) HOSTETTER thanked Instagram @russ.taylor, believed to be used by TAYLOR, described more fully below, for a gift of "#thebattleaxe representing the many battles yet to come." The posted photo depicts HOSTETTER (right), TAYLOR (center), and one other man (left). HOSTETTER held a tomahawk axe in the photograph. The photograph also shows that the third man wore a t-shirt emblazoned with a large image in red, white, and blue colors featuring a "Q". I know based on my training and experience that the Q design relates to and promotes "QAnon," a collection

of Internet conspiracies, including that the United States Congress and Vice President Mike Pence unconstitutionally "stole" the November 3, 2020 presidential election from President Donald J. Trump.

42. In another post by @americanphoenixproject (on what appears to be the date of the Capitol riots, January 6, 2021), (included below) HOSTETTER wrote "this was the shot heard 'round the world!"...the 2021 version of 1776. That war lasted 8 years. We are just getting warmed up. Much like FAUX News reporting tonight, the British journalists and the Redcoats of

the 1770s claimed the Tea Party was a mob. Patriots will prevail!" HOSTETTER also wrote, "we did our part." In the photo, HOSTETTER wearing a magenta colored knit hat, a blue shirt, a grey jacket, black and grey scarf, and there appears to be a bag or backpack strapped across his chest with a white circle emblem or logo. HOSTETTER is standing next to TAYLOR, whom I identified after comparing this photo to TAYLOR's California Department of Motor Vehicle photo. TAYLOR is wearing what appears to be a bulletproof vest which has several patches affixed to it. One patch is bright yellow appearing to be a "Don't Tread on Me" patch, one patch is an American flag in subdued blue and black, and one patch appears to be the state flag of California. Also, the photo shows what appears to be a knife inserted into a pocket on the bulletproof vest and handheld radio. TAYLOR is also wearing a bright red baseball style cap with the words "Make America Great Again" printed on it. Based on my knowledge of the investigation, the two are in an elevated position on the Capitol portico, which was a restricted area on January 6, 2021. The two men are taking a "selfie" photograph, facing the Capitol, with their backs to the National Mall and Capitol reflecting pool.

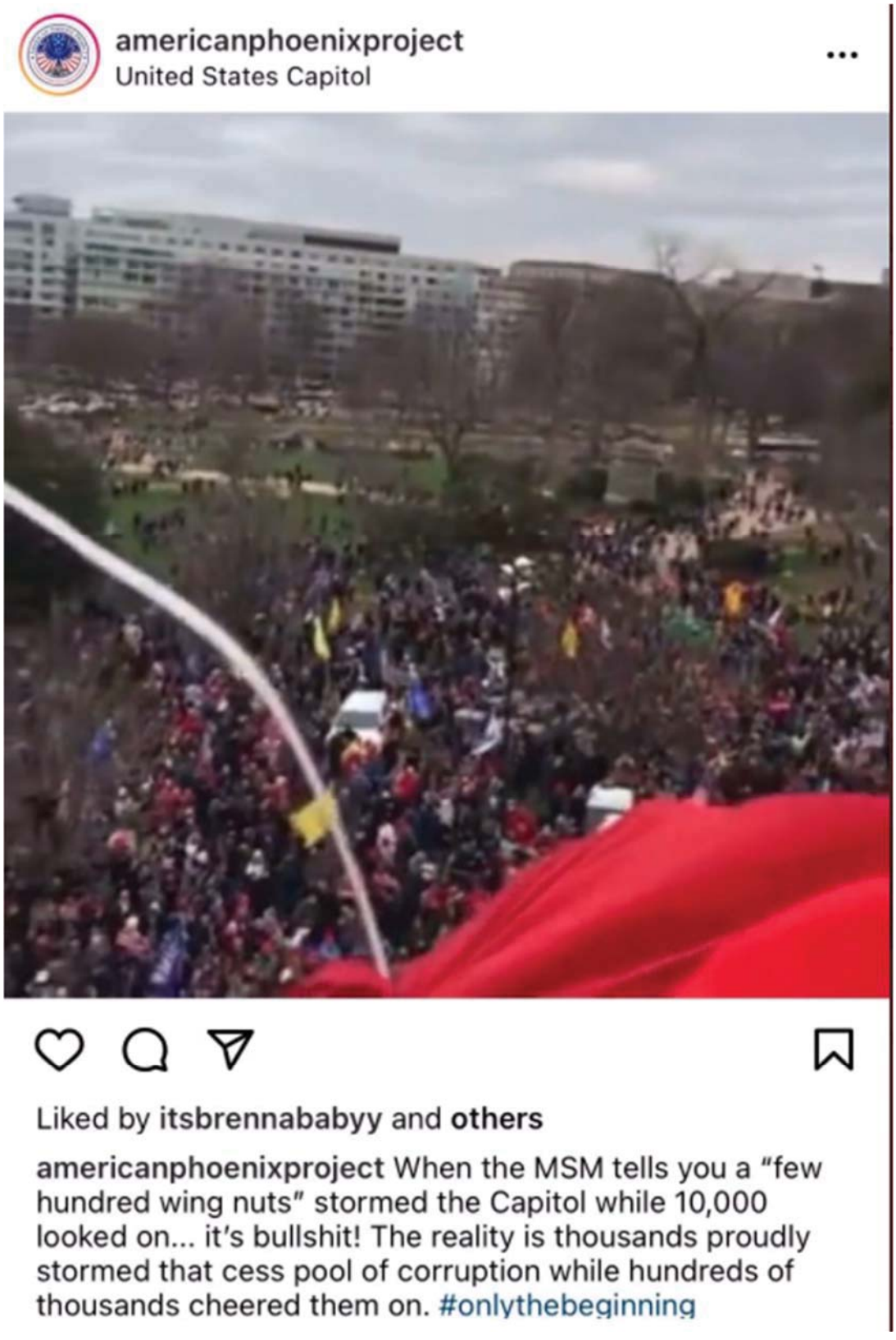

americanphoenixproject
United States Capitol
MAKE AMERICA GREAT AGAIN
Liked by brideyca and others
americanphoenixproject Thank you for your prayers and concern. Myself, @russ.taylor and [redacted] are safe. We did our part. We are proud of our fellow patriots, our President and our great country. This was the "shot heard 'round the world!"... the 2021 version of 1776. That war lasted 8 years. We are just getting warmed up. Much like FAUX News reporting tonight, the British journalists and the Redcoats of the 1770s claimed the Tea Party was a mob. Patriots will prevail!

43. In a separate image in the same post, HOSTETTER is seen waving an American flag near or at the top of the stairs on the portico on the West Front of the U.S. Capitol building, which was a restricted area on January 6, 2021. According to numerous videos and media reports rioters entered the U.S. Capitol building through the doors just behind where HOSTETTER is standing.

44. Additionally, in live news reporting from January 6,

2021, TAYLOR is seen waving an American flag near or at the top of the stairs on the portico on the West Front of the U.S. Capitol building, a restricted area. On both pictures below, TAYLOR is seen with a bright yellow patch affixed to his bulletproof vest and a bright red hat. According to numerous videos and media reports rioters entered the U.S. Capitol building through the doors just behind where TAYLOR is standing.

45. In another Instagram post I reviewed, HOSTETTER writes "When the MSM [mainstream media] tells you a 'few hundred wing nuts' stormed the Capitol while 10,000 looked...it's bullshit! The reality is thousands proudly stormed that cess pool of corruption while hundreds of thousands cheered them on. #onlythebeginning." HOSTETTER included a photo taken from an elevated position on the Senate (North) side of the West Front Capitol portico of the crowd below, a restricted area on January 6, 2021.



46. In the below photograph, which was published in the

news media, TAYLOR is seen on one of the West Front landings, a restricted area of the Capitol grounds. TAYLOR is wearing what appears to be the same bulletproof vest as in other photos. The vest appears to have a bright yellow patch affixed to it, and he is holding a gas mask in his left hand. TAYLOR is making a gesture with his right hand toward a line of Metropolitan Police officers who are wearing riot gear. Based on my knowledge of the investigation, I also believe this photo was taken on January 6, 2021.

C. HOSTETTER Traveled To and From D.C. in the SUBJECT VECHILE

47. According to California Motor Vehicles records, HOSTETTER is the registered owner of the SUBJECT VECHILE 1 --

the 2020 Chevy Silverado truck with California plate [redacted] – and it is registered to the SUBJECT PREMISES 1.

48. On January 12, 2021, I queried a law enforcement database containing information from license plate readers ("LPR") located near major U.S. highways and roadways. According to my search, the SUBJECT VEHICLE 1 was recorded on December 31, 2020, traveling eastbound on I-40 in Arizona and, on January 1, 2021, near Amarillo, TX. SUBJECT VEHICLE 1 was also recorded on January 9, 2021 traveling westbound near Amarillo, TX. Based on these results, it appears HOSTETTER departed Orange County for Washington, D.C. on December 31, 2020, and departed Washington, D.C. for Orange County on or about January 7, 2021 the day after the Capitol riots.

49. On January 7, 2021, a tipster contacted the FBI via the National Threat Operations Center. The tipster reported that HOSTETTER traveled to Washington, DC to engage in the above described riot. According to the tipster, HOSTETTER made multiple posts to HOSTETTER's Instagram @americanphoenixproject regarding HOSTETTER's travel and involvement in the riot.

50. January 11, 2021, the FBI Los Angeles contacted the tipster directly. The tipster provided the aforementioned Instagram screenshots to the FBI. I reviewed those screenshots. On January 2, 2021, HOSTETTER, using Instagram "@americanphoenixproject," posted "Only 3% of Americans actually fought in our War of Independence. There will likely be 3% of us again that will commit fully to this battle but, just as in 1776, patriots will prevail. Things are going to come to a head

in the U.S. over the next several days. Stay tuned!" Based on my training and experience, I know that militia extremists sometimes call themselves three percenters ("III%ers" or "threepers") based on the myth that only three percent of American colonists took up arms against the British during the American Revolution. Some III%ers regard the present-day U.S. Government as analogous to British authorities during the Revolution in terms of infringements on civil liberties. While many independent or multi-state militia groups incorporate III% in their unit names, the term is less indicative of membership in a single overarching group than it is representative of a common belief in the notion that a small force with a just cause can overthrow a tyrannical government if armed and prepared..[5] The Southern Poverty Law Center categorizes the III%ers as an anti-government extremist group.[6]

D. Previously Authorized Warrants

50. On January 19, the Honorable Douglas F. McCormick, United States Magistrate Judge authorized warrants for the disclosure of historical cell-site information and prospective cell-site information and GPS information on the following phone numbers (21-MJ-00019):

a. [redacted]-9134 (the "Telephone Number-9134"), a cellular telephone issued by Verizon Wireless, believed to be used by HOSTETTER; and

[5] https://www.thethreepercenters.org/ (last viewed on January 14, 2021).

[6] https://www.splcenter.org/fighting-hate/extremist-files/ideology/antigovernment (last viewed on January 14, 2021).

b. [redacted]-7934 ("Telephone Number-7934"), a cellular telephone issued by Cingular/AT&T Wireless, and believed to be used by TAYLOR.

51. On January 19, 2021, I executed the warrants and provided them to the carriers listed above. On January 20, 2021, AT&T provided me records for TAYLOR's phone, Telephone Number-7934. According to the records, telephone calls to Telephone Number-7934 are being automatically forwarded to a different cellular and there is no historical cell-site information, prospective cell-site information, or GPS information available for Telephone Number-7934. According to AT&T, Telephone Number-7934 may be powered off, out of the service area or in an area where location information was not available. Accordingly, to obtain information regarding the TAYLOR's location, historical cell-site information, prospective cell-site information, and GPS information was required from the additional phone TAYLOR is using phone number [redacted]-9210 ("Telephone Number-9210").

52. On January 20, 2021, the Honorable Douglas F. McCormick, United States Magistrate Judge, authorized warrants for the disclosure of historical cell-site information and prospective cell-site information and GPS information on Telephone Number-9210 (21-MJ-00029).

E. Results of Previously Executed Warrants

53. On January 19, 2021, I executed the warrants and provided them to the carriers above. On January 20, 2021, Verizon provided me records for Telephone Number-9314.

According to these records, HOSTETTER was located in Big Bear, CA. According to my review of cell-site information provided to me, on January 21, 2021, HOSTETTER left Big Bear, CA and made several stops in and around Ontario, CA. HOSTETTER then drove to San Clemente, CA and briefly stopped at or near his residence in [redacted] CA. HOSTETTER then returned to Big Bear, CA.

54. On January 21, 2021, I executed the warrant on Telephone Number-9210. On January 21, 2021, AT&T provided me records for Telephone Number-9210. According to my review, I determined TAYLOR was located at the SUBJECT RESIDENCE 2.

55. On January 13, 2021, FBI surveillance observed SUBJECT VEHICLE 1 inside the gated garage of SUBJECT PREMISES 1, in the first parking space. HOSTETTER was not observed at that time. As of January 15, 2021, the SUBJECT VEHICLE 1 was no longer observed by FBI surveillance at SUBJECT PREMISES 1. SUBJECT VEHICLE 1 was later located by FBI surveillance on January 22, 2021 in Big Bear, CA.

F. Evidence of the Subject Offense is Likely to Be Found on Digital Devices Inside the SUBJECT PREMISES and SUBJECT VEHICLES or on the persons of HOSTETTER and TAYLOR

56. As described above, there is evidence that HOSTETTER had in his possession a digital device while at the U.S. Capitol on January 6, 2021.

57. In addition, based on photos and videos of the offenses that date, numerous persons committing the SUBJECT OFFENSE 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 SUBJECT OFFENSE 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.

56. Moreover, it is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet from June 12, 2019, The Pew Research Center for Internet & Technology estimated that 96% of Americans owned at least one cellular phone, and that that same 2019 report estimated that 81% of Americans use at least one smartphone.[7]

57. Based on my training and experience, I know that individuals traveling outside of their cities of residence, and individuals attending large events such as the riots on January 6, 2021 in Washington, D.C. typically carry their cell phones with them in order to coordinate their travel plans, use web-based applications to get directions to unfamiliar locations, and communicate with friends and family both at the event and at home. Furthermore, based on my training and experience, I know that persons who engage in the SUBJECT OFFENSE will frequently use digital devices, including cell phones, computers, tablets, and other devices, to conduct their criminal activities, preserve photographs and videos in order to memorialize previous

---

56. [7] *See* Mobile Fact Sheet, https://www.pewresearch.org/internet/fact-sheet/mobile/ (last visited Jan. 9, 2021).

illegal activity, and maintain contact with others involved with the planning, targeting, and execution of their criminal activities.

58. Based on my review of public news reports following the events at the U.S. Capitol on January 6, 2021, I know that many individuals involved in the incident used their cell phones to take and share photographs and videos on social media applications, both during and after the incident. I know, based on my training and experience that these Internet-based applications require digital devices to operate and that photographs and videos that are posted to social media are generally stored on a digital device as well. Such evidence is therefore likely to be found on digital devices used by HOSTETTER and TAYLOR. Those devices are likely to have other evidence of their activity as well, including evidence of their location in the hours and days leading up to, during, and after the incident, Internet searches he conducted regarding the incident, and communications with other subjects regarding the incident.

59. 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, including photos of themselves 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.

60. 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:

[8]

[8] https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/ (Last viewed on January 24, 2021)

 [9]

 [10]

[9] https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1 (Last viewed on January 24, 2021)

[10] https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e (Last viewed on January 24, 2021)

61. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the offense that originally resided on the Subject's cell phone may also be saved to other digital devices within the SUBJECT PREMISES. Moreover, here, as widely reported in the news media related to this matter, many individual committing the SUBJECT OFFENSE kept and posted videos, photos, and commentary about their participation in these offenses, essentially bragging about their participation. Based on that, there is also probable cause to believe that evidence related to these offenses may have been transferred to and stored on digital devices beyond the particular digital device the Subject possessed during the offenses.

62. Based on my training and experience, I know that individuals typically store their digital devices, such as cell phones, tablets, and computers, at their personal residences and on their persons, where they can be easily accessed and used. Moreover, in this case, HOSTETTER and TAYLOR wore uniquely identifiable clothing including what appears to be a bulletproof vest, including patches and pins, a walkie-talkie and knife, as well as a gas mask. In my training, experience, and knowledge of the investigation, many individuals who engaged in to the January 6, 2021 riot returned to their homes with the same items

– such as unique clothing or bullhorns – that they used at the time they committed the SUBJECT OFFENSE. These items can prove that the individual shown in images captured on social media during a riot, for example, is the same person who lives at a given residence or used a particular item during the riot. It is possible that HOSTETTER and TAYLOR may still be wearing the clothing that is identified in the photographs above.

63. Based on my training and experience, and on conversations I have had with other law enforcement officers, I know that some individuals who participate in activities aimed at disrupting or interfering with governmental and/or law enforcement operations have been known to use anonymizing services and/or applications capable of encrypting communications to protect their identity and communications. By using such tools, in some cases, the only way to see the content of these conversations is on the electronic device that had been used to send or receive the communications.

64. Accordingly, I believe that evidence of the SUBJECT OFFENSE, including digital devices and other items used by HOSTETTER and TAYLOR to prepare for, commit, document, and discuss the SUBJECT OFFENSE, are likely to be found inside the SUBJECT PREMISES 1 and 2, in SUBJECT VECHILES 1 and 2, and on the person of HOSTETTER and TAYLOR.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[11]

65. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the 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,

[11] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. 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. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

e. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

66. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

67. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.
Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint

scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress HOSTETTER's or TAYLOR's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of HOSTETTER's or TAYLOR's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

VIII. CONCLUSION

68. For all the reasons described above, there is probable cause to believe that the items listed in Attachments B-1 and B-2, which constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1752 (Entering or Remaining in a Restricted Building or Grounds/Disruption of Orderly Conduct of Government Business) will be found at the SUBJECT PREMISES 1 and

2, in SUBJECT VEHICLES 1 and 2, and on the person of HOSTETTER and TAYLOR, as described in Attachments A-1 through A-6.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 26th day of January, 2021.

/s/ Autumn D. Spaeth
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

PREMISES TO BE SEARCHED

SUBJECT PREMISES 1 is the residence located at [redacted] CA. The residence is located within a multi-unit apartment building with a gated garage underneath the apartments. [redacted]

The apartment has windows on either side of the recessed doorway. There is a ceramic apartment number with a white background and a blue/black number [redacted] to the right of the doorway. A Ring Doorbell was observed to the left of the door. There are windows from [redacted] and look down on the street below.

[redacted]

ATTACHMENT A-2

VEHICLE TO BE SEARCHED

SUBJECT VEHICLE 1 is a 2020 black Chevy Silverado truck, bearing California license plate number [redacted] and vehicle identification number [redacted], which is registered to Alan Hostetter.

ATTACHMENT A-3

PERSON TO BE SEARCHED

The person of Alan Hostetter ("HOSTETTER"), date of birth [redacted], with California Driver's License Number [redacted]. HOSTETTER's California Department of Motor Vehicle records lists him [redacted].

The search of HOSTETTER shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within HOSTETTER's immediate vicinity and control at the location where the search warrant is executed. The search shall not include a strip search or a body cavity search.

ATTACHMENT A-4

PREMISES TO BE SEARCHED

SUBJECT PREMISES 2 is the premises, garage, and any vehicle stored inside the garage, located at [redacted] CA. This address has also been listed as [redacted]. The residence is a 4,575 square foot single family, two story home with an attached garage. The home is white with brick accents. The residence has 5 bedrooms and 5 bathrooms.

[redacted]

ATTACHMENT A-5

VEHICLE TO BE SEARCHED

SUBJECT VEHICLE 2 is a 2020 black Cadillac SUV, bearing California license plate number [redacted] and vehicle identification number [redacted], which is registered to Russell Taylor.

ATTACHMENT A-6

PERSON TO BE SEARCHED

The person of Russell Taylor ("TAYLOR"), date of birth [redacted], with California Driver's License Number [redacted]. TAYLOR's California Department of Motor Vehicle records lists him as standing 6[redacted].

The search of TAYLOR shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within TAYLOR's immediate vicinity and control at the location where the search warrant is executed. The search shall not include a strip search or a body cavity search.

ATTACHMENT B-1

ITEMS TO BE SEIZED

1. The items to be seized are the evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1752 (Entering or Remaining in a Restricted Building or Grounds/Disruption of Orderly Conduct of Government Business), ("SUBJECT OFFENSE"), namely:

a. Items worn or used by Alan HOSTETTER on or about January 6, 2021, including a black scarf, blue jacket, magenta knit hat, and a black bag with white logo on the strap;

b. Equipment, items, or weapons designed for or capable of use in attacking United States Capitol Police or other law enforcement or government agents or employees;

c. Records, documents, receipts, and other materials indicating or describing HOSTETTER's travel to Washington, DC between December 30, 2020, to present date, including records, documents, receipts, and other materials indicating that any person traveling with HOSTETTER;

d. Registration or documents showing indicia of ownership or possession of the SUBJECT VEHICLE 1;

e. Any information indicating ownership or lease of SUBJECT RESIDENCE 1;

f. Location data from December 30, 2020 to present;

g. Records, documents, programs, applications, and materials (including communications, online postings, photos, videos, posters, flags, notes, jewelry, clothing, shirts, hats,

pants, magazines, location data, patches, search history, purchases, and books) that relate to:

i. HOSTETTER's preparations for, plans for, whereabouts on, and activities on January 6, 2021;

ii. HOSTETTER's presence at or inside the U.S. Capitol on January 6, 2021;

h. Any items taken from the U.S. Capitol on or about January 6, 2021;

i. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSE, and forensic copies thereof;

j. Cameras or video recording devices which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSE, and forensic copies thereof;

k. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. 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, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software 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;

iii. evidence of the attachment of other devices;

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

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. 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.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

i. The review of the electronic data obtained pursuant to this warrant 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 investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

j. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

k. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

l. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

m. Any magnetic, electronic, or optical storage device capable of storing digital data;

n. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

o. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

p. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

q. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

r. During the execution of this search warrant, law enforcement is permitted to: (1) depress HOSTETTER's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of HOSTETTER's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

s. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT B-2

ITEMS TO BE SEIZED

1. The items to be seized are the evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1752 (Entering or Remaining in a Restricted Building or Grounds/Disruption of Orderly Conduct of Government Business), ("SUBJECT OFFENSE"), namely:

a. Items worn or used by Russell TAYLOR ("TAYLOR") on or about January 6, 2021, including a bulletproof vest, patches, a red "Make America Great Again" baseball style hat, pins, and handheld radio;

b. Equipment, items, or weapons designed for or capable of use in attacking United States Capitol Police or other law enforcement or government agents or employees;

c. Records, documents, receipts, and other materials indicating or describing TAYLOR's travel to Washington, DC between December 30, 2020, to present date, including records, documents, receipts, and other materials indicating that any person traveling with TAYLOR;

d. Registration or documents showing indicia of ownership or possession of the SUBJECT VEHICLE 2;

e. Any information indicating ownership or lease of SUBJECT RESIDENCE 2;

f. Location data from December 30, 2020 to present;

g. Records, documents, programs, applications, and materials (including communications, online postings, photos, videos, posters, flags, notes, jewelry, clothing, shirts, hats,

pants, magazines, location data, patches, search history, purchases, and books) that relate to:

i. TAYLOR's preparations for, plans for, whereabouts on, and activities on January 6, 2021;

ii. TAYLOR's presence at or inside the U.S. Capitol on January 6, 2021;

h. Any items taken from the U.S. Capitol on or about January 6, 2021;

i. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSE, and forensic copies thereof;

j. Cameras or video recording devices which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSE, and forensic copies thereof;

k. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. 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, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software 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;

iii. evidence of the attachment of other devices;

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

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. 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.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

III. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

i. The review of the electronic data obtained pursuant to this warrant 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 investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

j. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

k. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

l. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

m. Any magnetic, electronic, or optical storage device capable of storing digital data;

n. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

o. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

p. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

q. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

r. During the execution of this search warrant, law enforcement is permitted to: (1) depress TAYLOR's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of TAYLOR's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

s. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.