UNITED STATES DISTRICT COURT

for the

Southern District of California

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

One (1) Apple iPhone, blue in color; One (1) Apple iPad Pro, Model # A2764, Serial # C34D7Q63DN; and One (1) Apple MacBook, silver in color

Case No. '23 MJ00156

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

See Attachment A, incorporated herein by reference.

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

See Attachment B, incorporated herein by reference.

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1752(a)(1) & (a)(2) 40 U.S.C. § 5104(e)(2)(D) & (e)(2)G)	Entering and remaining in a restricted building or grounds; disorderly and disruptive conduct in a restricted building or grounds; disorderly conduct in a Capitol Building; parading, demonstrating or picketing in a Capitol building

The application is based on these facts:

See Attached Affidavit of ATF Special Agent Arnesha Bahn, incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Arnesha Bahn, ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 01/17/2023 @ 5:12 PM

Judge's signature

City and state: San Diego, California

KAREN S. CRAWFORD
U.S. Magistrate Judge
Printed name and title

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

I, Arnesha Bahn, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following electronic devices:

1. One (1) Apple iPhone, blue in color;

2. One (1) Apple iPad Pro, Model # A2764, Serial # C34D7Q63DN; and

3. One (1) Apple MacBook, silver in color,

(hereinafter, "the **Devices**") described further in Attachment A.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms & Explosives and a Task Force Officer with the Federal Bureau of Investigations ("FBI"). I have been so employed since April of 2013. As part of my duties as an FBI Task Force Officer, I investigate criminal violations relating to criminal activity in and around the Capitol grounds on January 6, 2021. I am currently assigned to the San Diego Field Office's Joint Terrorism Task Force. During my investigations, I have interviewed subjects and witnesses regarding allegations, prepared subpoenas for telephone and online information, and I have analyzed these records to identify information pertinent to the investigation. I have prepared and executed search warrants both at physical locations and for online data. Over the course of my career, I have become familiar with the manner in which criminal activity is carried out, and the efforts of persons involved in such activity to avoid detection by law enforcement. As a federal agent, I am authorized to investigate

violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

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.

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 Title 18, U.S.C. Sections 1752(a)(1) (entering and remaining in a restricted building or grounds) and 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds) and Title 40, U.S.C. Sections 5104(e)(2)(D) (disorderly conduct in a Capitol building or grounds) and 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol building) (the "Target Offenses") that have been committed by VICTOR SEAN DENNISON ("DENNISON") and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, DENNISON, as well as others observed by DENNISON.

II. PROBABLE CAUSE

A. Background – the U.S. Capitol on January 6, 2021

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 were 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 United States Congress convened at the United States Capitol, which is located at First Street, SE, in Washington, D.C. 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 United States 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.

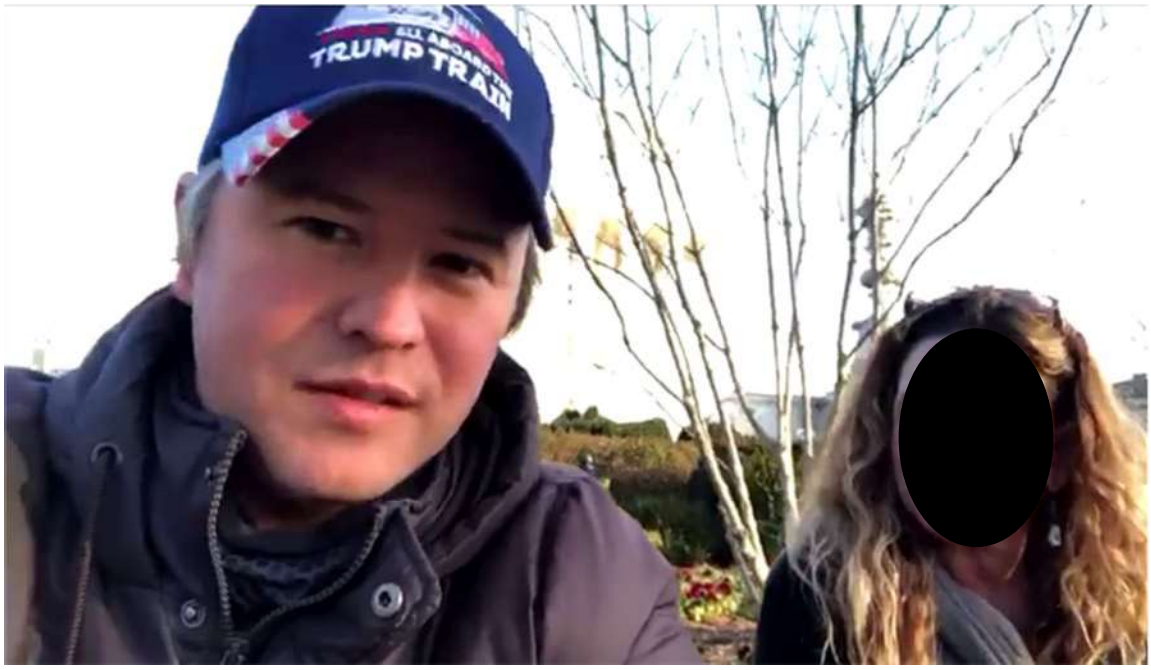
9. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President

Mike Pence, were instructed to—and did—evacuate the chambers. Accordingly, the joint session of the United States Congress was effectively suspended until shortly after 8:00 p.m. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the sessions resumed.

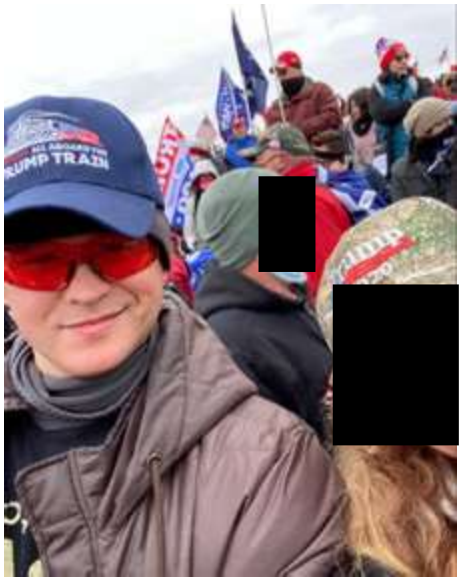
10. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

B. Facts Specific to DENNISON

11. On January 18, 2021, an anonymous citizen (T-1) submitted to the FBI's tip line a video that had been posted to the Facebook page of username "facebook.com/seandennison1," subsequently identified as VICTOR SEAN DENNISON. T-1 said he got the video from DENNISON'S Facebook friend. T-1 does not know DENNISON. In the video clip that T-1 submitted, DENNISON said that he entered the U.S. Capitol building on January 6, 2021. The video appears to have been filmed in the Washington D.C. area. DENNISON is wearing a gray puff-jacket and a baseball cap with the slogan "ALL ABOARD THE TRUMP TRAIN" stitched on it. A still of the video clip is below. DENNISON is on the left.



12. During the investigation, the FBI also identified a photograph, copied below, of DENNISON, posted to a third party's Facebook account, which depicts DENNISON wearing red-tinted sunglasses, as well as the same gray puff- jacket and baseball cap worn in the video clip mentioned above. Based on the background of the photographs, DENNISON appears to be in Washington, D.C.



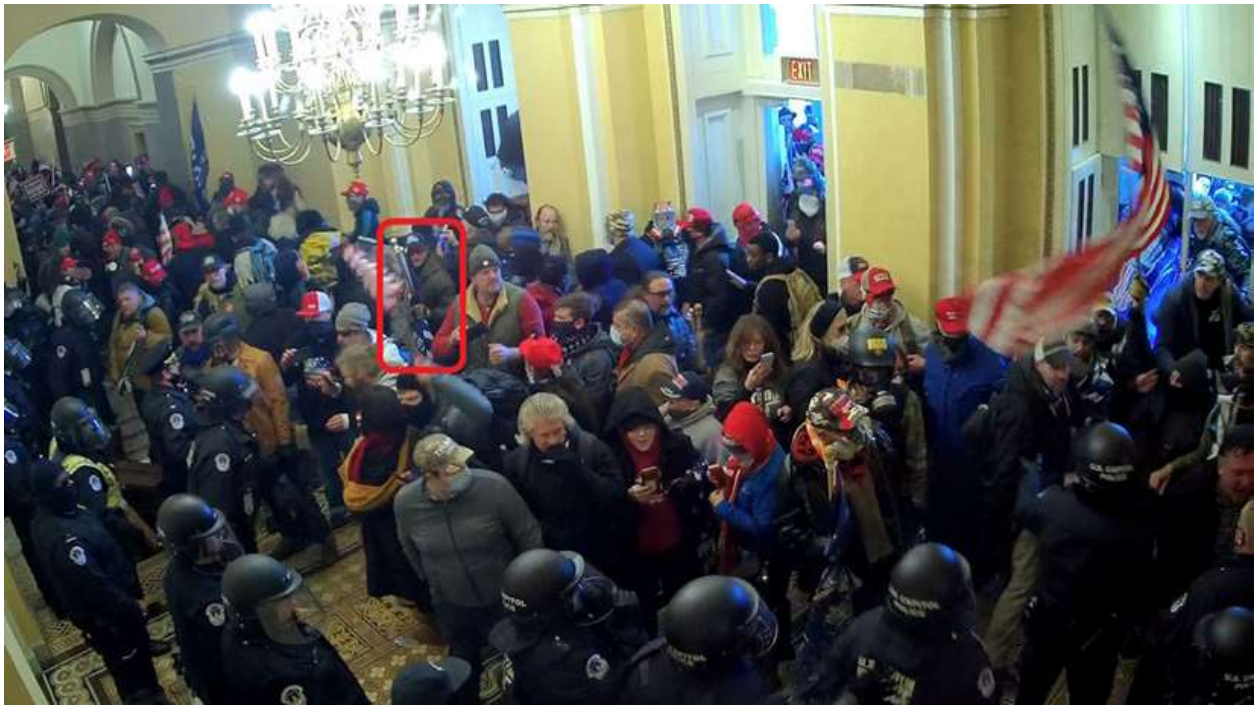
13. On June 9, 2021, the FBI interviewed DENNISON by telephone. DENNISON stated that he traveled to Washington D.C., to attend a pro-Trump rally, which was scheduled for January 6, 2021. He further stated that, after attending President Trump's speech at the Ellipse near the White House, DENNISON walked to the U.S. Capitol building with a large crowd. DENNISON said that his cellphone service was bad and that the service seemed to be, "All jammed up,' due to everyone streaming and taking videos. DENNISON stated that he then noticed a group at one of the doors that had been breached. He observed a man with a hammer in his hand and then noticed that a window had been smashed next to the door. DENNISON admitted to investigators that he entered the U.S. Capitol building after noticing the doors had been breached. DENNISON also admitted to seeing Capitol Police dressed in riot gear inside the Capitol building. DENNISON told the interviewing agents that he exited the Capitol building after hearing someone state, "They're going to start shooting people." DENNISON said the statement frightened him.

DENNISON said that upon exiting the Capitol, he attempted to call a companion but noticed that his cellphone battery was dead.

14. DENNISON also confirmed that on January 7, 2021, he made a video of himself and another individual in front of the U.S. Supreme Court, in which they described their experiences the day before, including DENNISON'S entry into the U.S. Capitol building. In the video, DENNISON's companion stated, "We're like ok, we're in and we're making headway and we're getting in, and the cops are now backing off and that's a symbol that we're winning." DENNISON interjected with, "Ok, so here's some more on that . . . the point she's talking about, I had already gone inside, and I had a chance to inspect the scene and decided to remove myself from the area."

15. Through a review of on closed-circuit television within the U.S. Capitol Building (otherwise referred to as "CCTV") footage, the FBI also identified DENNISON entering the U.S. Capitol building on January 6, 2021. The footage shows DENNISON enter the U.S. Capitol building at 2:49 p.m. and exit at 2:51 p.m. EST. Dennison entered and exited the building through the Senate Wing Door, an area of the Capitol Building elevated above ground level and accessible through exterior stairs. At approximately 2:14 p.m., rioters broke open a window adjacent to the Senate Wing Door, climbed through the window, and forced the door open from inside the building. Stills from the Capitol surveillance footage, depicting Dennison entering the Capitol building through the Senate Wing Door, are below. DENNISON is circled in red. Notably,

DENNISON is wearing the same distinctive clothing as in the photographs copied above.



16. The FBI took three further steps to identify DENNISON. *First*, I compared his California driver license photograph to the photographs above and concluded the photographs

appear to match. *Second*, on May 20, 2021, DENNISON was interviewed by a U.S. Customs and Border Protection ("CBP") officer while attempting to cross the U.S.-Mexico border. On August 10, 2021, the FBI showed the same CBP officer the above screen capture of DENNISON from January 6, 2021. [*See above,* ¶12 at p.6.] The CBP Officer confirmed the man in the photograph was DENNISON. *Third*, on November 18, 2021, the FBI showed the same CBP Officer surveillance footage from Capitol CCTV (screenshots of which are copied above), showing DENNISON inside the U.S. Capitol building on January 6, 2021. The CBP Officer confirmed the individual in the blue hat and red sunglasses was DENNISON.

17. On January 12, 2023, U.S. Magistrate Judge G. Michael Harvey of the United States District Court for the District of Columbia issued a federal complaint charging DENNISON with the Target Offenses, and arrest warrant [Criminal Case No.23-mj-0011]. On Friday, January 13, 2023, at approximately 11:00 a.m., DENNISON drove a 1999 Lincoln Navigator into the United States at the San Ysidro Port of Entry. CBP officers at the Port of Entry arrested DENNISON pursuant to that warrant and conducted a border search of his person and vehicle. Pursuant to that search, found the **Devices** on his person and in his car. Custody of those items were turned over to FBI Special Agents and Task Force Officers, and are now being held at the FBI San Diego Field Office, 10385 Vista Sorrento Pkwy, San Diego, CA 92121.

18. Based on the foregoing, I submit that there is probable cause to believe that DENNISON violated 18 U.S.C. § 1752(a)(1) and (2), which makes it a crime to (1) knowingly enter or remain in any restricted building or grounds without lawful authority to do; and (2) knowingly, and with intent to impede or disrupt the orderly conduct of Government business or official functions, engage in disorderly or disruptive conduct in, or within such proximity to, any

restricted building or grounds when, or so that, such conduct, in fact, impedes or disrupts the orderly conduct of Government business or official functions; or attempts or conspires to do so. For purposes of Section 1752 of Title 18, a "restricted building" includes a posted, cordoned off, or otherwise restricted area of a building or grounds where the President or other person protected by the Secret Service, including the Vice President, is or will be temporarily visiting; or any building or grounds so restricted in conjunction with an event designated as a special event of national significance.

19. I also submit that there is probable cause to believe that DENNISON violated 40 U.S.C. § 5104(e)(2)(D) and (G), which makes it a crime to willfully and knowingly (D) utter loud, threatening, or abusive language, or engage in disorderly or disruptive conduct, at any place in the Grounds or in any of the Capitol Buildings with the intent to impede, disrupt, or disturb the orderly conduct of a session of Congress or either House of Congress, or the orderly conduct in that building of a hearing before, or any deliberations of, a committee of Congress or either House of Congress; and (G) parade, demonstrate, or picket in any of the Capitol Buildings.

20. I know, based on my training and experience, that it is common for subjects in a criminal investigation to store personal effects, including mobile phones, electronic devices and media storage devices within their residences and vehicles. I also know that cell phones, computers and other electronic devices are expensive, and people routinely retain such devices for many months or years.

21. I also know that hundreds of people have been arrested in connection to the riot that occurred at the U.S. Capitol on January 6, 2021. During searches of the majority of those people's homes and vehicles from early 2021 through present in multiple jurisdictions, law enforcement

has recovered clothing, paraphernalia, tools, and devices that were worn, used or carried on January 6, 2021. For example, in mid-February 2022, the home of a defendant in the District of Massachusetts was searched. During that search law enforcement found the sweatshirt and backpack the defendant wore while committing crimes on January 6, 2021, at the United States Capitol. Law enforcement also found a folder containing a D.C. metro transit fare card and receipt for the purchase of that card dated January 6, 2021. In early March 2022, the home of a defendant in the Eastern District of New York was searched. During that search law enforcement found the hat, sunglasses, and other objects the defendant wore or carried while committing crimes on January 6, 2021, at the United States Capitol.

22. 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. *See Mobile Fact Sheet*, PEW RESEARCH CENTER (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.

23. 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 or law enforcement operations have been known to use anonymizing services 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.

24. I also know that 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 DENNISON's cell phone may also be saved to other digital devices. Moreover, here, as widely reported in the news media related to this matter, many individuals committing the Target Offenses 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 that DENNISON possessed during the offenses.

25. Although it has been over two years since the events of January 6, 2021, based on my training and experience and the training and experience of other agents involved in the investigation of the U.S. Capitol insurrection, I believe that evidence of the Target Offenses will still be found on DENNISON'S phone and/or other electronic devices used by DENNISON. I am aware that more than 700 people throughout the country have been arrested for offenses arising out of the riot. In many of these cases, the FBI sought and obtained warrants to search a defendant's cellular telephone at the time of the defendant's arrest, often occurring many months after January 6, 2021. Frequently, defendants charged in connection with the Capitol riot have kept cellular telephones and other digital devices that they used at the Capitol and, on such devices, have retained evidence related to the Capitol riot. I am specifically aware of several searches of digital devices that the FBI has conducted in the past few months in which the FBI recovered a

digital device that contained evidence related to the January 6, 2021, Capitol riot. For example, on November 22, 2021, the FBI seized a cellular telephone pursuant to a search warrant in the Eastern District of North Carolina. A search of the phone revealed relevant text messages and photographs, including a photograph of the defendant inside the U.S. Capitol building and a photograph of a canister of pepper spray that appears similar to the canister the defendant used against law enforcement officers on January 6, 2021. On December 1, 2021, in a separate matter, the FBI seized a cellular telephone pursuant to a search warrant issued in the Northern District of Illinois. The cellular phone contained photographs and text messages pertaining to Capitol riot activities. In a third case, on December 9, 2021, the FBI seized a cellular telephone pursuant to a search warrant issued in the District of New Jersey. The defendant had retained videos from January 6, 2021, on his phone. As a final example, on December 20, 2021, the FBI seized a cellular telephone pursuant to a search warrant issued in the Northern District of Illinois. On the phone, the FBI discovered messages that included the defendant admitting to two assaults on law enforcement officers on January 6, 2021.

III. COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

26. As described above and in Attachment A, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found in the **Devices.** One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless

communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices, including DENNISON's phone, are found, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including the above specified offenses, use digital devices, like DENNISON's phone, 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" messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep

track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation. Based on my knowledge of the planning activities of other subjects who illegally entered the U.S. Capitol Building on January 6, 2021, I know that some of these individuals used end-to-end encrypted messaging applications such as Telegram and Signal to discuss their plans to travel to the U.S. Capitol, and in some cases, used these platforms to discuss conspiracies to disrupt the certification of the election.

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.

27. As further described in Attachment B, this application seeks permission to search for 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.

IV. METHODS TO BE USED TO SEARCH DIGITAL DEVICES

28. 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, I request 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.

29. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures regarding the Device(s) that may contain data subject to seizure pursuant to this warrant:

(1) Upon securing any Device(s), law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices on scene when arresting DENNISON. Law enforcement, with the aid of a technical expert, will then obtain a forensic image of the Device(s). A forensic image captures all the data on the hard

drive or other media without the data being viewed and without changing the data. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. The digital devices, or any forensic images thereof will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B. After verified images have been obtained, the owner of the Device(s) will be notified and the original devices returned within forty-five (45) days of seizure, absent further application to this court.

(2) 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.

(3) In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to decide 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. As noted above, the identification and extraction process may take weeks or months. The personnel conducting the identification and extraction of the data from any wireless phones will complete the analysis within ninety (90) days, absent further application of the court. As to any other Device(s) (e.g., computers, hard drives, tablets) seized during the execution of the warrant, the personnel conducting the identification and extraction of data from these Device(s) will complete the analysis within one-hundred and twenty (120) days.

A. Genuine Risks of Destruction

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

B. Prior Attempts to Obtain Data

31. The United States has not yet attempted to obtain this data by other means.

V. CONCLUSION

32. Based on the facts and opinions set forth above, there is probable cause to believe that DENNISON has committed violations of Title 18, U.S.C. Section 1752(a)(1) (entering and

remaining in a restricted building or grounds) and (2) (disorderly and disruptive conduct in a restricted building or grounds) and Title 40, U.S.C. Section 5104(e)(2)(D) (disorderly conduct in a Capitol building or grounds) and (G) (parading, demonstrating, or picketing in a Capitol building) and that evidence of these crimes, contraband, fruits of the crimes, things otherwise criminally possessed, as well as property designed or intended for use or which is or has been used as a means of committing the crimes, will be located on DENNISON.

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

//

//

//

/

//

//

//

//

//

//

//

//

//

34. Because this is an ongoing investigation and premature disclosure of the investigation could endanger agents and officers, cause target subjects or others to flee and cause destruction of evidence, I request that this affidavit, the application for the search warrants (and the attachments), the search warrants (and the attachments), and all other associated sealing orders be sealed until further court order.

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

DATE: January 17, 2023

Arnesha Bahn
Special Agent, Bureau of Alcohol, Tobacco, Firearms & Explosives
Task Force Officer, FBI San Diego Joint Terrorism Task Force

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone this 17th day of January, 2023.

Hon. KAREN S. CRAWFORD
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF ITEM(S) TO BE SEARCHED

1. One (1) Apple iPhone, blue in color;
2. One (1) Apple iPad Pro, Model # A2764, Serial # C34D7Q63DN; and
3. One (1) Apple MacBook, silver in color,

(hereinafter, "the Devices") which Devices were seized on January 13, 2023 at the San Ysidro Port of Entry by San Diego Customs and Border Protection Officers from the vehicle and/or person of Victor Sean Dennison, and which are presently in the custody of the Federal Bureau of Investigation at the FBI San Diego Field Office, located at 10385 Vista Sorrento Pkwy, San Diego, CA 92121.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Items, documents, and records contained or stored in electronic format which constitutes evidence, instrumentalities, fruits and contraband concerning violations of Title 18, U.S.C. Sections 1752(a)(1) (entering and remaining in a restricted building or grounds) and 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds) and Title 40, U.S.C. Sections 5104(e)(2)(D) (disorderly conduct in a Capitol building or grounds) and 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol building) (the "Target Offenses") that have been committed by VICTOR SEAN DENNISON ("DENNISON") and other identified and unidentified persons, as described in the search warrant affidavit. The Target Offenses occurred on January 6, 2021, however, evidence of the Target Offenses that was created or occurred before or after January 6, 2021 may be seized. The evidence that may be seized includes but is not limited to the following:

a. Evidence concerning planning to unlawfully enter the U.S. Capitol, on January 6, 2021, including any maps or diagrams of the building or its internal offices;

b. Evidence concerning unlawful entry into the United States Capitol, including any property of the United States Capitol;

c. Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;

d. Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;

e. Evidence relating to a conspiracy to illegally enter and/or occupy the United States Capitol Building on or about January 6, 2021;

f. Evidence concerning the breach and unlawful entry of the United States Capitol, and any conspiracy or plan to do so, on January 6, 2021;

g. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;

h. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties while in the United States Capitol on January 6, 2021;

i. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;

j. Evidence of any conspiracy, planning, or preparation to commit the above offenses on January 6, 2021;

k. Evidence concerning efforts after the fact to conceal evidence of the above offenses related to January 6, 2021, or to flee prosecution for the same;

l. Evidence concerning materials, devices, or tools that were used to unlawfully enter the United States Capitol on January 6, 2021 by deceit or by force, including weapons and elements used to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;

m. Evidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the United States Capitol on January 6, 2021;

n. Evidence of the state of mind of the DENNISON and/or other co-conspirators, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the January 6, 2021 criminal activity under investigation; and

o. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the January 6, 2021 criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

2. Items, documents, and records contained or stored in electronic format —including but not limited to communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:

a. Any records and/or evidence revealing DENNISON's presence at the January 6, 2021, riot;

b. Any physical records, such as receipts for travel, which may serve to prove evidence of travel of to or from Washington D.C. from December of 2020 through January of 2021;

c. DENNISON's (and others') motive and intent for traveling to the United States Capitol on or about January 6, 2021; and

d. DENNISON's (and others') activities in and around Washington, D.C., specifically the United States Capitol, on or about January 6, 2021.

3. With respect to each Device described in Attachment and the search warrant affidavit:

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

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

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

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

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

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

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

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

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

The search of the Device(s) for the above described items will be conducted as provided in the "Methods to be Used to Search Digital Devices" section of the affidavit submitted in support of this search warrant.