

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO. 22-mj-8549-BER

IN RE SEALED SEARCH WARRANT

CRIMINAL COVER SHEET

1. Did this matter originate from a matter pending in the Northern Region of the United States Attorney's Office prior to August 8, 2014 (Mag. Judge Shaniek Maynard)? No
2. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to October 3, 2019 (Mag. Judge Jared Strauss)? No

Respectfully submitted,

JUAN ANTONIO GONZALEZ
UNITED STATES ATTORNEY

BY: _____

Assistant United States Attorney

99 Northeast 4th Street
Miami, Florida 33132-2111
Telephone: _____
E-mail: _____

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO. 22-mj-8549-BER

IN RE: SEARCH WARRANT

HIGHLY SENSITIVE DOCUMENT

MOTION TO SEAL

The United States of America, by and through the undersigned Assistant United States Attorney, hereby moves to seal this Motion, the Search Warrant, and all its accompanying documents, until further order of this Court. The United States submits that there is good cause because the integrity of the ongoing investigation might be compromised, and evidence might be destroyed.

The United States further requests that, pursuant to this Court's procedures for Highly Sensitive documents, all documents associated with this investigation not be filed on the Court's electronic docket because filing these materials on the electronic docket poses a risk to safety given the sensitive nature of the material contained therein.

Respectfully submitted,

JUAN ANTONIO GONZALEZ
UNITED STATES ATTORNEY

BY:

Assistant United States Attorney

99 Northeast 4th Street
Miami, Florida 33132-2111

FILED BY TM D.C.

Nov 28, 2022

**ANGELA E. NOBLE
CLERK U.S. DIST. CT.
S. D. OF FLA. - West Palm Beach**

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO. 22-mj-8549-BER

IN RE: SEARCH WARRANT

HIGHLY SENSITIVE DOCUMENT

SEALING ORDER

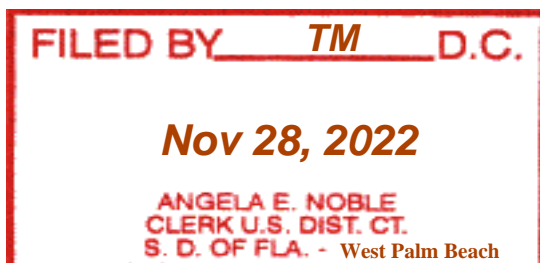
The United States of America, having applied to this Court for an Order sealing the Motion to Seal, the Search Warrant and all its accompanying documents, and this order and the Court finding good cause:

IT IS HEREBY ORDERED that the Motion to Seal, the Search Warrant and its accompanying documents, and this Order shall be filed under seal until further order of this Court. However, the United States Attorney's Office and the Federal Bureau of Investigation may obtain copies of any sealed document for purposes of executing the search warrant.

DONE AND ORDERED in chambers at West Palm Beach, Florida, this 28 day of November 2022.



HON. BRUCE E. REINHART
UNITED STATES MAGISTRATE JUDGE



AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the
Southern District of FloridaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 22-mj-8549-BER

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

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

See Attachment B

FILED BY TM D.C.

Nov 28, 2022

ANGELA E. NOBLE
CLERK U.S. DIST. CT.
S. D. OF FLA. - West Palm Beach

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. § 793(e)	Willful retention of national defense information
18 U.S.C. § 2071	Concealment or removal of government records
18 U.S.C. § 1519	Obstruction of federal investigation
18 U.S.C. § 1001	Material false statements
18 U.S.C. § 1623	Perjury

The application is based on these facts:

See attached Affidavit of FBI Special Agent [REDACTED]

☒ 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.

[REDACTED] Special Agent, FBI

Printed name and title

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

Date: 11/28/2022

City and state: West Palm Beach, Florida

[Signature]
Judge's signature

Hon. Bruce E. Reinhart, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, [REDACTED] being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence located at [REDACTED] [REDACTED] (“TARGET RESIDENCE”), as described in Attachment A, and the following cellular phones: (1) an Apple iPhone 12 Pro Max, [REDACTED], associated with phone number [REDACTED] (“TARGET PHONE 1”); and (2) an Apple iPhone 13 Pro Max, [REDACTED], associated with phone number [REDACTED] (“TARGET PHONE 2”) (collectively, the “TARGET PHONES”) found therein, for the items described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) [REDACTED] [REDACTED] During this time, I have received training at the FBI Academy located at Quantico, Virginia, specific to counterintelligence and espionage investigations. [REDACTED]

[REDACTED] Based on my experience and training, I am familiar with efforts used to unlawfully collect, retain, and disseminate sensitive government information, including classified National Defense Information (“NDI”), and with efforts to obstruct justice.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the TARGET RESIDENCE and the TARGET PHONES, as described in Attachment A, contain evidence of violations of 18 U.S.C. § 793(e) (willful retention of national defense information); 18 U.S.C. § 2071 (concealment or removal of government records); 18 U.S.C. § 1519 (obstruction of federal investigation), 18 U.S.C. § 1001 (material false statement); or 18 U.S.C. § 1623 (perjury), as further described in Attachment B.

PROBABLE CAUSE

Background on Investigation

5. The FBI is investigating potential violations of 18 U.S.C. §§ 793(e), 2071, 1519, 1001, and 1623 related to the improper removal and storage of classified national defense information in unauthorized spaces, as well as the unlawful concealment or removal of government records and obstruction of its investigation.

6. This investigation began as a result of a referral that the United States National Archives and Records Administration (“NARA”) sent to the United States Department of Justice (“DOJ”) on or about February 9, 2022 (hereinafter, the “NARA Referral”). The NARA Referral stated that on January 18, 2022, in accordance with the Presidential Records Act (“PRA”), NARA received from the office of former President Donald J. Trump (hereinafter “FPOTUS”), via representatives, fifteen (15) boxes of records (hereinafter, the “FIFTEEN BOXES”). The FIFTEEN BOXES, which had been transported from a property owned by FPOTUS at 1100 S. Ocean Blvd., Palm Beach, Florida, a residence and club known as “Mar-a-Lago,” were reported in the NARA Referral to contain, among other things, highly classified documents intermingled with other records.

7. After an initial review of the NARA Referral, the FBI opened a criminal investigation to, among other things, identify any person(s) who may have removed or retained classified information without authorization and/or in an unauthorized space. The FBI's investigation established that documents bearing classification markings, which appear to contain NDI, were among the materials contained in the FIFTEEN BOXES and were stored at Mar-a-Lago in an unauthorized location.

8. As further described below, on May 11, 2022, the Department of Justice ("DOJ") served a grand jury subpoena on counsel for the Office of the Former President (the "Office") seeking "any and all documents . . . bearing classification markings" in FPOTUS's and/or the Office's possession. On June 3, 2022, FPOTUS's counsel provided DOJ with a package of 37 documents bearing classification markings at the Confidential, Secret, and Top Secret levels. Counsel for FPOTUS provided DOJ with a written certification, signed by another person who was acting as the custodian of records on behalf of the Office for purposes of the subpoena, indicating that "a diligent search was conducted," that the "search was conducted after receipt of the subpoena, in order to locate any and all documents that are responsive to the subpoena" seeking all documents with classification markings in the custody or control of FPOTUS and/or the Office, and that "any and all responsive documents" were being provided. Counsel for FPOTUS indicated that all responsive documents had been located in one storage room located on the ground floor at Mar-a-Lago (hereinafter, "the storage room.").

9. After developing additional evidence that the June 3 production did not contain all of the documents with classification markings located at Mar-a-Lago, on August 8, 2022, the FBI executed a search and seizure warrant issued by a Magistrate Judge of the U.S. District Court for the Southern District of Florida. During the search, the FBI recovered from the storage room as

well as FPOTUS's office at Mar-a-Lago over 100 documents bearing classification markings, which had not been produced on June 3. The documents appeared to contain NDI. The search also yielded apparent government and/or Presidential records subject to the Presidential Records Act, 44 U.S.C. § 2201.

Background on NAUTA

10. NAUTA began his career in the U.S. Navy [REDACTED]

[REDACTED] NAUTA transitioned to work as a valet, or personal aide, for FPOTUS during FPOTUS's Presidential Administration (hereinafter "Administration"). [REDACTED]

[REDACTED] In or around the summer of 2021, NAUTA retired from the military and went to work as a civilian for FPOTUS as his "body man" or assistant. According to publicly available information filed with the Federal Election Commission, the Save America PAC, a political action committee created by FPOTUS, paid NAUTA \$149,167 between August 26, 2021, and August 30, 2022, which included \$6,375 in "advance consulting" fees.

11. NAUTA was involved in at least two key movements of FPOTUS's boxes at Mar-a-Lago: (1) in the weeks leading up to the provision of the FIFTEEN BOXES to NARA in January 2022, NAUTA and two other FPOTUS employees brought, at FPOTUS's request, the FIFTEEN BOXES from their location in a storage room at Mar-a-Lago to FPOTUS's residential entryway at Mar-a-Lago for FPOTUS's review; and (2) in the week before FPOTUS's representatives claimed on June 3 that they had conducted a diligent search for classified documents, NAUTA moved approximately 64 boxes out of the storage room at Mar-a-Lago and returned only about 25-30 prior to the review of the storage room for records responsive to the May 11 subpoena. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

12. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

13. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

14. [REDACTED]

[REDACTED]

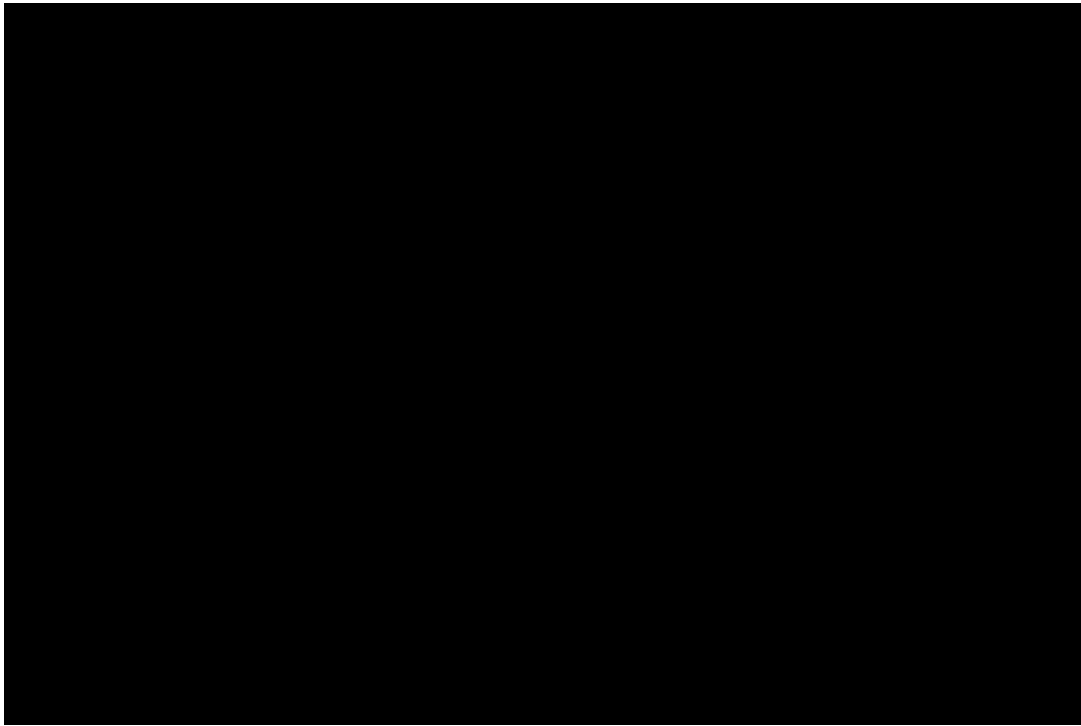
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



15. [REDACTED]

[REDACTED]

16. [REDACTED]

[REDACTED]

[REDACTED] The door to the storage room was painted gold and had no other markings on it.

17. In addition to the approximately eighty-five to ninety-five FPOTUS BOXES located in the storage room, there were also other boxes in the storage room with merchandise such as challenge coins, garment bags, memorabilia from Mar-a-Lago such as photograph frames, and other décor items.

Provision of the Fifteen Boxes to NARA

18. Over the course of 2021, NARA endeavored to obtain what appeared to be missing records subject to the Presidential Records Act (PRA), 44 U.S.C. § 2201. On or about May 6, 2021, NARA made a request for the missing PRA records and continued to make requests until approximately late December 2021, when NARA was informed twelve boxes were found and ready for retrieval at Mar-a-Lago. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

19. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

20. [REDACTED] took a photograph of the storage room and provided it to FPOTUS sometime between January 1-17, 2022, to show FPOTUS the number of boxes that were in the storage room. The storage photo, which appears below [REDACTED]

[REDACTED] captures approximately sixty-one of the FPOTUS BOXES located in the storage room:



21. [REDACTED]

[REDACTED]

[REDACTED]

22. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

23. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

24. [REDACTED]

[REDACTED]

25. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

26. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

27. From May 16-18, 2022, FBI agents conducted a preliminary review of the FIFTEEN BOXES provided to NARA and identified over 100 documents with classification markings in fourteen of the FIFTEEN BOXES. Several of the documents also contained what appears to be FPOTUS's handwritten notes.

Grand Jury Subpoena, Related Correspondence, and Production of Additional Classified Documents

28. On May 11, 2022, an attorney representing FPOTUS, “FPOTUS COUNSEL 1,” agreed to accept service of a grand jury subpoena requesting “[a]ny and all documents or writings in the custody or control of Donald J. Trump and/or the Office of Donald J. Trump bearing classification markings.” The return date of the subpoena was May 24, 2022.

29. After an extension was granted for compliance with the subpoena, on the evening of June 2, 2022, FPOTUS COUNSEL 1 contacted DOJ COUNSEL and requested that FBI agents meet him the following day to pick up responsive documents. On June 3, 2022, three FBI agents and DOJ COUNSEL arrived at Mar-a-Lago to accept receipt of the materials. In addition to FPOTUS COUNSEL 1, another individual, hereinafter “INDIVIDUAL 2,” was also present as the custodian of records for FPOTUS’s post-presidential office. The production included a single Redweld envelope, wrapped in tape, containing documents. FPOTUS COUNSEL 1 relayed that the documents in the Redweld envelope were found during a review of the boxes located in the storage room. INDIVIDUAL 2 provided a Certification Letter, signed by INDIVIDUAL 2, which stated the following:

Based upon the information that has been provided to me, I am authorized to certify, on behalf of the Office of Donald J. Trump, the following: a. A diligent search was conducted of the boxes that were moved from the White House to Florida; b. This search was conducted after receipt of the subpoena, in order to locate any and all documents that are responsive to the subpoena; c. Any and all responsive documents accompany this certification; and d. No copy, written notation, or reproduction of any kind was retained as to any responsive document.

30. During receipt of the production, FPOTUS COUNSEL 1 stated he was advised all the records that came from the White House were stored in the storage room at Mar-a-Lago and the boxes of records in the storage room were “the remaining repository” of records from the White

House. FPOTUS COUNSEL 1 further stated he was not advised there were any records in any private office space or other location in Mar-a-Lago. The agents and DOJ COUNSEL were permitted to see the storage room (although they were not permitted to look inside the boxes) and observed that approximately fifty to fifty-five boxes remained in the storage room. Considering that only FIFTEEN BOXES had been provided to NARA of the approximately eighty-five to ninety-five FPOTUS BOXES that had been located in the storage room, it appeared that approximately fifteen to thirty of the FPOTUS BOXES had previously been relocated elsewhere. The FBI agents also observed that the composition of boxes differed such that fewer Bankers boxes were visible, while more plain cardboard boxes and storage bins were present. Other items were also present in the storage room, including a coat rack with suit jackets, as well as interior décor items such as wall art and frames.

31. [REDACTED]

[REDACTED]

[REDACTED]

32. A review of the documents contained in the Redweld envelope produced pursuant to the grand jury subpoena revealed 37 unique documents bearing classification markings, some of which bore classification markings at the highest levels. Based on my training and experience, I know that documents classified at these levels typically contain NDI. Multiple documents also contained what appears to be FPOTUS's handwritten notes.

33. When producing the documents, neither FPOTUS COUNSEL 1 nor INDIVIDUAL 2 asserted that FPOTUS had declassified the documents.¹ The documents being in a Redweld

¹ 18 U.S.C. § 793(e) does not use the term "classified information," but rather criminalizes the unlawful retention of "information relating to the national defense." The statute does not define "information related to the national

envelope wrapped in tape appears to be consistent with an effort to handle the documents as if they were still classified.²

Surveillance Camera Footage Shows NAUTA removing boxes from the Storage Room Area Prior to FPOTUS Counsel 1's Review in Connection with the Subpoena

34. On July 6, 2022, in response to a grand jury subpoena for surveillance video from internal cameras located on the ground floor (basement) [REDACTED] representatives of the Trump Organization provided a hard drive to FBI agents. Upon review of the hard drive, the FBI determined that the drive contained video footage from four cameras in the basement hallway of Mar-a-Lago in which the door to the storage room is located. The footage on the drive begins on April 23, 2022, and ends on June 24, 2022. The recording feature of the cameras appears to be motion activated, so that footage is only captured when motion is detected within each camera's field of view.

35. One camera in particular, identified on the hard drive as "South Tunnel Liquor," provides a view of entry and exit into a room (hereafter anteroom) that leads to the storage room. The doorway to the anteroom itself is not visible in the camera view, as a refrigerator is directly

defense," but courts have construed it broadly. *See Gorin v. United States*, 312 U.S. 19, 28 (1941) (holding that the phrase "information relating to the national defense" as used in the Espionage Act is a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness"). In addition, the information must be "closely held" by the U.S. government. *See United States v. Squillacote*, 221 F.3d 542, 579 (4th Cir. 2000) ("[I]nformation made public by the government as well as information never protected by the government is not national defense information."); *United States v. Morison*, 844 F.2d 1057, 1071-72 (4th Cir. 1988). Certain courts have also held that the disclosure of the documents must be potentially damaging to the United States. *See Morison*, 844 F.2d at 1071-72.

² On May 25, 2022, while negotiating for an extension of the subpoena, FPOTUS COUNSEL 1 sent two letters to DOJ COUNSEL. In the second such letter, available at 22-mj-8332-BER (D.E. 125), FPOTUS COUNSEL 1 asked DOJ to consider a few "principles," which include FPOTUS COUNSEL 1's claim that a President has absolute authority to declassify documents. In this letter, FPOTUS COUNSEL 1 requested, among other things, that "DOJ provide this letter to any judicial officer who is asked to rule on any motion pertaining to this investigation, or on any application made in connection with any investigative request concerning this investigation."

between the camera and doorway, but the footage from this camera nonetheless establishes entry and exit to the anteroom because it is apparent when persons within the camera's field of view turn directly behind the refrigerator and then disappear from view. The anteroom, in addition to its entrance from the South Tunnel, has approximately four doors leading off it, one of which is the gold-painted door that leads to the storage room. The anteroom provides the only entrance to the storage room; however, other offices can also be entered from the anteroom, so it might be possible for persons to enter the storage room from those other offices without being visible in the surveillance camera footage.

36. By reviewing the camera footage provided by the Trump Organization in response to the subpoena, the FBI has determined the following:

On May 24, 2022, NAUTA is observed exiting the anteroom doorway with three boxes.

On May 30, 2022, four days after NAUTA's interview with the FBI during which the location of boxes was a significant subject of questioning, NAUTA is observed exiting the anteroom doorway with approximately fifty Bankers boxes, consistent with the description of the FPOTUS BOXES. FBI did not observe this quantity of boxes being returned to the storage room through the anteroom entrance in its review of the footage.

On June 1, 2022, NAUTA is observed carrying eleven brown cardboard boxes out the anteroom entrance. One box did not have a lid on it and appeared to contain papers.

The day after that, on June 2, 2022, NAUTA is observed moving twenty-five to thirty boxes, some of which were brown cardboard boxes and others of which were Bankers boxes consistent with the description of the FPOTUS BOXES, into the entrance of the ANTEROOM. Approximately three and a half hours later, NAUTA is observed escorting FPOTUS COUNSEL 1 in through the entrance of the anteroom, and FPOTUS COUNSEL 1 is not observed leaving until approximately two and a half hours later.

On June 3, 2022, FPOTUS COUNSEL 1 is escorted through the anteroom entrance by an unidentified individual wearing a jacket with "USSS POLICE" printed on the back. The unidentified individual and FPOTUS COUNSEL 1 exit the ANTEROOM entrance moments later. FPOTUS COUNSEL 1 appeared to be carrying a Redweld envelope after exiting the anteroom.

37. According to FBI's review of video footage, and as detailed in the paragraph above, NAUTA can be observed removing approximately 64 boxes from the storage room area between May 24 and June 1, 2022, but only returning 25-30 boxes to the storage room area on June 2, 2022. Notably, and as described above in paragraph 28, these boxes were removed following service of a grand jury subpoena but before FPOTUS COUNSEL 1's review of boxes in the storage room area to locate documents responsive to the subpoena.

38. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

NAUTA concealed information during his FBI interview [REDACTED]

39. On May 26, 2022, the FBI interviewed NAUTA and explained that the FBI was conducting an investigation as to whether classified documents were stored at Mar-a-Lago and that the FBI was particularly interested in where the boxes with classified documents were located and whether they had been moved outside the storage room.

40. [REDACTED]. During the interview, NAUTA claimed that the first time NAUTA saw the boxes was when NAUTA moved them from Pine Hall, the anteroom to FPOTUS's personal residential suite, to the moving truck to provide the boxes to NARA. [REDACTED]

[REDACTED]

[REDACTED] Further, in NAUTA's interview with the FBI on May 26, he had stated that he did not know where the boxes had come from prior to being located in

Pine Hall. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

41. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

42. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Execution of Search Warrant at Mar-a-Lago and Movement of Boxes After June 3

43. On August 8, 2022, the FBI executed a search warrant at Mar-a-Lago authorized by the Honorable Bruce E. Reinhart, U.S. Magistrate Judge in the Southern District of Florida. *See* 22-mj-83332-BER. The search yielded over 100 unique documents bearing classification markings, with some indicating the highest levels of classification and extremely limited distribution, found in both the storage room and FPOTUS's office at Mar-a-Lago. Based on my training and experience, I know that documents classified at these levels typically contain NDI.

44. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

45. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

46. [REDACTED]

[REDACTED]

The TARGET PHONES

47. TARGET PHONE 1, associated with phone number [REDACTED], is [REDACTED] [REDACTED] cellular phone and TARGET PHONE 2, associated with phone number [REDACTED], is [REDACTED] cellular phone. Verizon records confirm that the phone number associated with TARGET PHONE 1 has been effective [REDACTED]. Verizon records also show that TARGET PHONE 1 is an iPhone 12 Pro Max. The subscriber of TARGET PHONE 1 is listed as

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Apple records list [REDACTED], the phone number associated with TARGET PHONE 2, as the telephone number associated with [REDACTED] Apple iCloud account, with [REDACTED] as the email address associated with that iCloud account. Apple records also show that TARGET PHONE 2, an iPhone 13 Pro Max, is the device associated with [REDACTED] iCloud account [REDACTED] [REDACTED].

48. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

49. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Therefore, it is likely that relevant emails that [REDACTED] sent or received from [REDACTED] email account are on TARGET PHONE 1. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In my training and experience, a person using an iPhone often accesses and saves email on their phone. Therefore, it likely that relevant emails would also be located within TARGET PHONE 2.

50. On September 30, 2022, open-source research revealed that the phone number associated with TARGET PHONE 2 was registered with WhatsApp, an encrypted communication application. Open-source research also confirmed that the phone number associated with TARGET PHONE 1 was registered with both WhatsApp and Signal, another encrypted communication application. Accordingly, there may be stored communications through WhatsApp or Signal on the TARGET PHONES that pertain to this investigation.

51. Based upon this investigation, I believe that there may be stored communications within the TARGET PHONES that contain evidence detailing the removal of FPOTUS boxes, which likely contained classified information and NDI, from the White House to Mar-a-Lago and from the storage room at Mar-a-Lago. Furthermore, I believe there may be stored communications in the TARGET PHONES detailing efforts to mislead law enforcement. Finally, the data from the TARGET PHONES would also provide location information [REDACTED] that could indicate when and where [REDACTED] moved boxes, such as if [REDACTED] moved the boxes to a storage facility or other location outside of Mar-a-Lago. Apple has location services that could be used to determine where a user traveled with the user's phone.

TARGET RESIDENCE

52. Public records indicate that [REDACTED] has resided at the TARGET RESIDENCE [REDACTED]. Recent FBI surveillance has confirmed that [REDACTED] currently resides at the TARGET RESIDENCE: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

53. Based on my training and experience, individuals typically keep their personal cell phones and work cell phones that they regularly use on their persons, at their personal residence, or in their vehicles when they are driving.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

54. Based on my knowledge, training, and experience, I know that cellular telephones can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the TARGET PHONES. This information can sometimes be recovered with forensics tools.

55. There is probable cause to believe that things that were once stored on the TARGET PHONES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a device/computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media-in particular device/computers' internal hard drives-contain electronic evidence of how a device/computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

56. Based on my knowledge, training, and experience, I know that cellular telephones can store forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET PHONES because:

a. Data on the storage medium 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 traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of

peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a 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.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a 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 a storage medium.

f. I know that when an individual uses an electronic device to illegally solicit another to commit a crime of violence, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing

the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

57. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the TARGET PHONES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. In order to access the phone, it may be necessary to use [REDACTED] fingerprint or facial recognition, to unlock the phone. Accordingly, we request the authority to compel [REDACTED] to provide the necessary means to access the TARGET PHONES.

58. Based on my training and experience and on information I have learned from other agents, evidence of who was using a cellphone and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For example, such evidence could help determine whether [REDACTED] was the only person using the TARGET PHONES. In addition, information about the dates on which [REDACTED] used the TARGET PHONES could be relevant to proving various elements of the crimes under investigation, as described above.

59. The stored communications and files contained in the TARGET PHONES may provide direct evidence of the offenses under investigation. For example, text messages, instant

messages, emails, and voicemails could be direct or indirect evidence of who communicated with [REDACTED] before or after the June production and whether anyone communicated with [REDACTED]. Photos, videos, and other documents could show evidence of [REDACTED]

60. In addition, the user's account activity, logs, stored electronic communications, and other data on the TARGET PHONES, can indicate who has used or controlled the phone. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crimes under investigation.

61. Other information connected in the TARGET PHONES may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal evidence of the crimes under investigation or services used to communicate with others. Though your affiant knows that [REDACTED] uses WhatsApp to communicate, the full range of apps that [REDACTED] may use to communicate with persons relevant to this investigation remains unknown. Searching the TARGET PHONES will help determine whether [REDACTED] downloaded other apps that could be used for communication.

62. Therefore, the TARGET PHONES are likely to contain communications and information. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

63. *Unlocking the TARGET PHONES with biometric features.* The warrant I am applying for would permit law enforcement to obtain from [REDACTED] physical biometric features (such as fingerprint, thumbprint, or facial characteristics) to unlock the TARGET PHONES. I seek this authority based on the following:

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

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

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

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

e. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1)

more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 6 days. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s) found at the premises; and/or (2) hold the device(s) found at

the premises in front of the face to those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

REQUEST FOR SEALING

64. The United States request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss aspects of an ongoing criminal investigation that are neither public nor known to the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

FILTER PROCEDURES

65. [REDACTED] has been represented by attorneys in this matter since at least in or around [REDACTED]. A Filter Team will review seized communications and segregate potentially protected materials, i.e., communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. The Filter Team will have no future involvement in the investigation of this matter. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If at any time the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine (“protected materials”), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents can review the potentially privileged documents. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel for the privilege holder or a court order before providing these potentially protected materials to the

Prosecution Team. If possible, government attorneys will engage with the privilege holder to resolve privilege determinations before proceeding to court for judicial review.

CONCLUSION

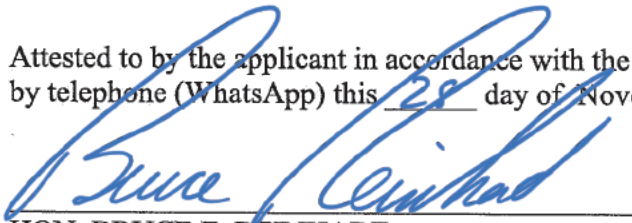
66. Based on the forgoing, I request that the Court issue the proposed search warrant.

Respectfully submitted,

A black rectangular redaction box covering the signature of the Special Agent.

Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1
by telephone (WhatsApp) this 28 day of November, 2022

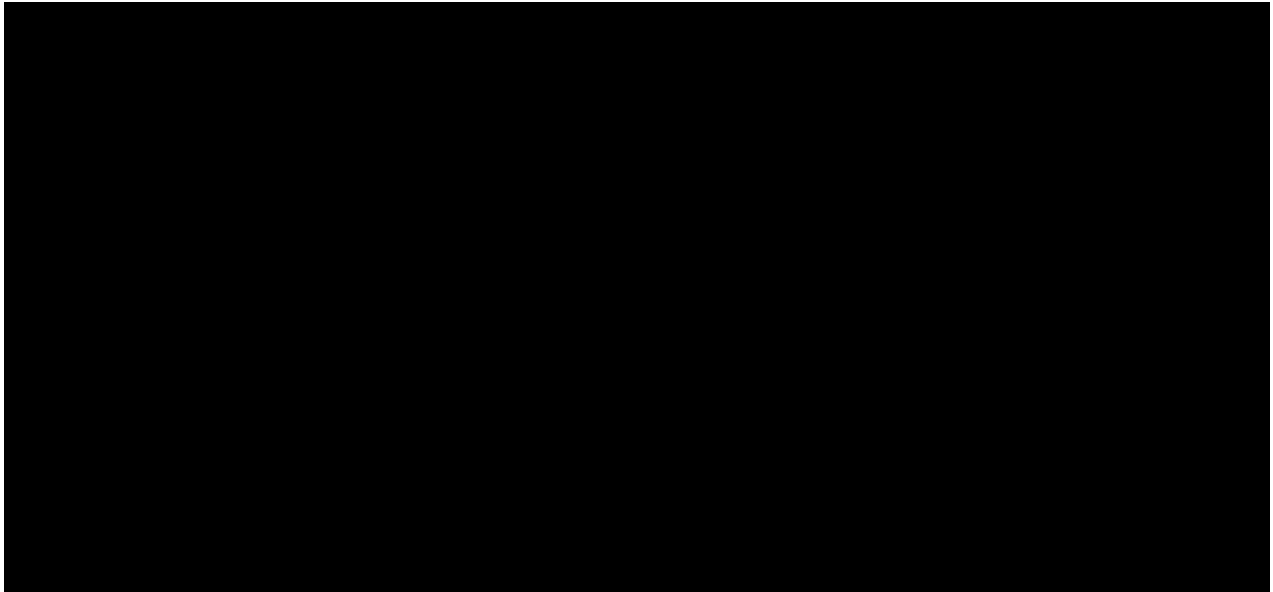
A blue ink signature of Bruce E. Reinhart, written over a horizontal line.

HON. BRUCE E. REINHART
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

The premises to be searched is [REDACTED]
[REDACTED] (“TARGET RESIDENCE”), as well as (1) an Apple iPhone 12 Pro Max, [REDACTED]
[REDACTED] associated with phone number [REDACTED] (“TARGET PHONE 1”); and
(2) an Apple iPhone 13 Pro Max, [REDACTED], associated with phone number [REDACTED]
[REDACTED] (“TARGET PHONE 2”)(collectively, “TARGET PHONES”), found therein. The
premises is an apartment [REDACTED] The front of the apartment
building is pictured below:



ATTACHMENT B

Particular Things to be Seized

The items to be seized by the government are (1) an Apple iPhone 12 Pro Max, [REDACTED], associated with phone number [REDACTED] (“TARGET PHONE 1”); and (2) an Apple iPhone 13 Pro Max, [REDACTED], associated with phone number [REDACTED] (“TARGET PHONE 2”)(collectively, “TARGET PHONES”), found therein.

During the execution of this warrant, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [REDACTED] and anyone else who is found with the TARGET PHONES and reasonably believed by law enforcement to be a user of the devices, to the fingerprint scanner of the devices (TARGET PHONES); and/or (2) hold the device in front of the face of [REDACTED] and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

for the
Southern District of Florida

Case No. 22-mj-8549-BER

Printed name and title

Case No.:

Copy of warrant and inventory left with:

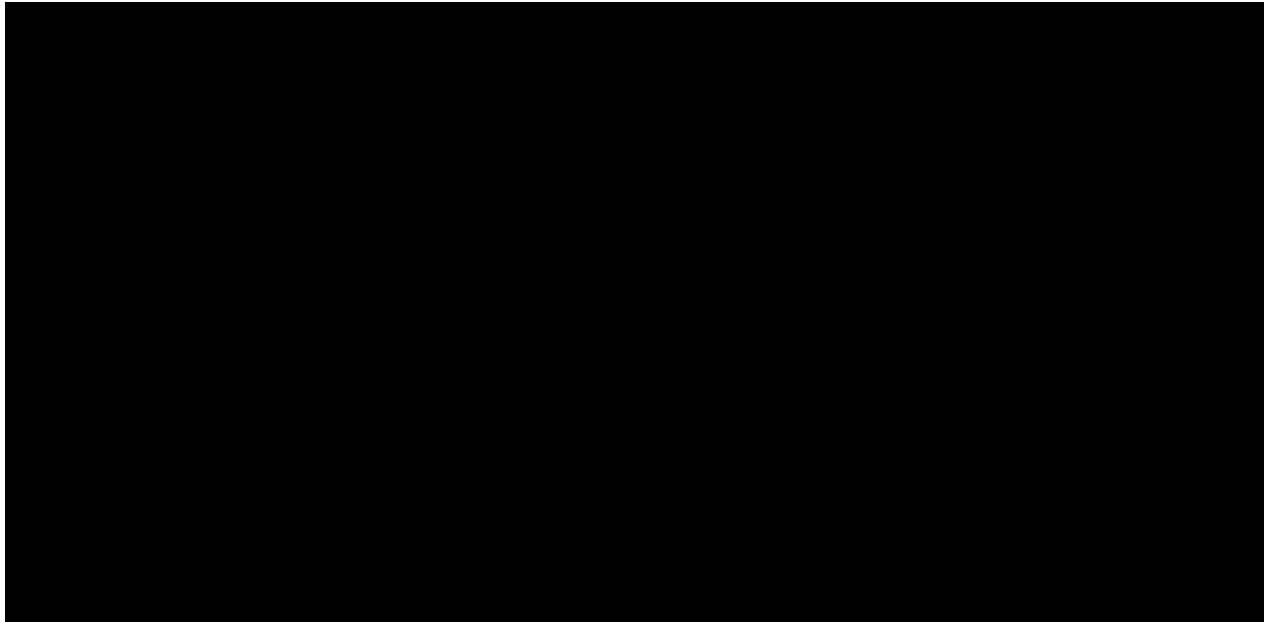
Inventory of the property taken and name of any person(s) seized:

Printed name and title

ATTACHMENT A

Property to Be Searched

The premises to be searched is [REDACTED]
[REDACTED] (“TARGET RESIDENCE”), as well as (1) an Apple iPhone 12 Pro Max, [REDACTED]
[REDACTED], associated with phone number [REDACTED] (“TARGET PHONE 1”); and
(2) an Apple iPhone 13 Pro Max, [REDACTED], associated with phone number [REDACTED]
[REDACTED] (“TARGET PHONE 2”)(collectively, “TARGET PHONES”), found therein. The
premises is an apartment [REDACTED]. The front of the apartment
building is pictured below:



ATTACHMENT B

Particular Things to be Seized

The items to be seized by the government are (1) an Apple iPhone 12 Pro Max, [REDACTED], associated with phone number [REDACTED] (“TARGET PHONE 1”); and (2) an Apple iPhone 13 Pro Max, [REDACTED], associated with phone number [REDACTED] (“TARGET PHONE 2”)(collectively, “TARGET PHONES”), found therein.

During the execution of this warrant, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [REDACTED] and anyone else who is found with the TARGET PHONES and reasonably believed by law enforcement to be a user of the devices, to the fingerprint scanner of the devices (TARGET PHONES); and/or (2) hold the device in front of the face of [REDACTED] and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.