IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

*

In Re: Motion To Intervene And Unseal Search Warrant Records	**Case No. 8:25-mc-00539-TJS**

*

*

*

****

UNITED STATES' NOTICE OF *EX PARTE* FILING OF FURTHER PARTIALLY REDACTED SEARCH WARRANT AFFIDAVIT

The United States hereby provides notice that it has filed a proposed further redacted version of the search warrant affidavit in this matter *ex parte* to the Court.

Respectfully submitted,

KELLY O. HAYES
UNITED STATES ATTORNEY

By: /s/
Thomas M. Sullivan
Robert I. Goldaris
Assistant United States Attorneys

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT [redacted]	Case No. 8:25-mj-02126-TJS Filed Under Seal

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, [redacted] being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since [redacted] I attended New Agent training at the FBI Academy in Quantico, Virginia. I am currently assigned to the FBI's Baltimore Field Office where I work a variety of national security and cyber investigations involving counterintelligence, export control violations, counter-proliferation, and illicit finance, many of which involve violations of Title 18 of the United States Code. During my tenure, I have conducted physical and electronic surveillance, executed search warrants, debriefed confidential sources, and reviewed court records. [redacted]

2. The facts in this affidavit come from my observations, training, experience, and information obtained from other Agents, witnesses, and third-party experts. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a search warrant, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. I have not,

however, excluded any information known to me that would undermine a determination of probable cause.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to search the residence of John Robert Bolton, II ("Bolton"), located at [redacted] ("**TARGET RESIDENCE**"), which is described more fully in Attachment A-1. Based on my training, experience, and the facts as set forth in this affidavit, I respectfully submit there is probable cause to believe that John Robert Bolton II committed violations of federal criminal law, including violations of Title 18, United States Code, Section 793(d), Title 18, United States Code, Section 793(e), and Title 18, United States Code 1924(a) (collectively, the "Subject Offenses"), and that evidence, fruits, and instrumentalities of the Subject Offenses, more particularly described in Attachment B, will be found within the **TARGET RESIDENCE**.

THE RELEVANT STATUTES

4. Title 18, United States Code, Section 793(d) provides:

> Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it . . . shall be [subject to criminal penalties].

5. Title 18, United States Code, Section 793(e) provides:

> Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which

> information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be [subject to criminal penalties].

6. Title 18, United States Code, Section 1924(a) provides:

> Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be [subject to criminal penalties].

CLASSIFIED AND NATIONAL DEFENSE INFORMATION

7. Executive Order 13526 governs the classification of national security information. Information in any form may be classified if it: (1) is owned by, is produced by or for, or is under the control of the U.S. Government; (2) could, if disclosed, cause one or more specified levels of harm to the United States; and (3) is classified by or under an Original Classification Authority ("OCA") who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. OCAs, also called original classifiers, are individuals authorized to classify information and make classification decisions.

8. Pursuant to Executive Order 12958, signed on April 17, 1995, as amended by Executive Order 13292 on March 25, 2003, and Executive Order 13526 on December 29, 2009, national security information is classified as "TOP SECRET," "SECRET," or "CONFIDENTIAL," as follows:

a. Information is classified as TOP SECRET if the unauthorized disclosure of that information reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

b. Information is classified as SECRET if the unauthorized disclosure of that information reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

c. Information is classified as CONFIDENTIAL if the unauthorized disclosure of that information reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

9. The classification marking "NOFORN" stands for "Not Releasable to Foreign Nationals" and denotes that dissemination of that information is limited to United States persons.

10. The classification marking "SI" stands for "Special Intelligence," and denotes intelligence information derived from the monitoring of foreign communications signals by individuals other than the intended recipients.

11. Classified information related to intelligence sources, methods, and analytical processes is designated as Sensitive Compartmented Information ("SCI"). SCI is to be processed, stored, used, or discussed in an accredited Sensitive Compartmented Information Facility ("SCIF"), and only individuals with the appropriate security clearance and additional SCI permissions are authorized to have access to such national security information.

12. The National Institute of Standards and Technology defines a SCIF as an area, room, group of rooms, buildings, or installation certified and accredited as meeting Director of National Intelligence security standards for the processing, storage, and/or discussion of sensitive compartmented information.

13. Intelligence Community Directive 705, titled "Sensitive Compartmented Information Facilities," signed on May 26, 2010, by the Director of National Intelligence, provides that "all SCI must be processed, stored, used, or discussed in an accredited SCIF."

14. Pursuant to Executive Order 13526, information classified at any level can be lawfully accessed only by persons determined by an appropriate U.S. Government official to be

eligible for access to classified information, and who signed an approved non-disclosure agreement, received a security clearance, and have a need to know the classified information.

15. Executive Order 13526 also states that classified information contained on automated information systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that (1) prevents access by unauthorized persons and (2) ensures the integrity of the information.

16. The term "national defense information" (herein "NDI") has been defined broadly by the Fourth Circuit Court of Appeals in *United States v. Morison*, 844 F.2d 1057, 1071 (4th Cir. 1988), to include "all matters that directly or may reasonably be connected with the national defense of the United States against any of its enemies. It refers to the military and naval establishments and the related activities of national preparedness." *Morison* and subsequent appellate decisions have consistently construed the term to include information dealing with military matters and more generally with matters relating to United States foreign policy and intelligence capabilities. Thus, based upon my experience, training, and discussions with other subject-matter experts, I submit that there is probable cause to believe that the information removed and retained without authorization by John Robert Bolton, II, as described below, constitutes NDI for purposes of Sections 793(d) and 793(e) of Title 18 of the United States Code.

JURISDICTION

17. This Court has jurisdiction to issue the proposed warrant because the property to be searched and seized is located within the district where the warrant will be issued pursuant to Rule 41(b)(1). Specifically, the **TARGET RESIDENCE** is located within the District of Maryland.

PROBABLE CAUSE

18. John Robert Bolton, II, is a 76-year-old United States citizen who resides in Bethesda, Maryland. Bolton is a former public servant, with nearly four decades of service in positions of trust within the U.S. government. Bolton is an attorney, who previously served as, among other things, General Counsel and Assistant Administrator for the U.S. Agency for International Development; Assistant Attorney General at the Department of Justice; Assistant Secretary and Under Secretary at the Department of State; U.S. Ambassador to the United Nations; and Assistant to the President for National Security Affairs ("APNSA"), commonly referred to as the National Security Advisor.

19. [redacted]

Bolton's Tenure as APNSA, Home SCIF, and Separation from Government Service

20. Bolton's most recent position within the U.S. government was APNSA. He held that position from April 9, 2018, to September 10, 2019. For his duration as APNSA, Bolton held a TOP SECRET/SCI security clearance.

21. As APNSA, Bolton directed and supervised the work of the National Security Council ("NSC") staff on behalf of the President of the United States. Bolton had access to, and was responsible for, safeguarding the most sensitive national-security information, including both classified and National Defense Information.

22. While in consideration for his appointment as APNSA, Bolton executed a Classified Information Nondisclosure Agreement ("NDA"), titled Standard Form 312 ("SF-

[1] [redacted]

312"), and two Sensitive Compartmented Information ("SCI") NDAs, titled Standard Form 4414 ("SF-4414") on April 5, 2018. By signing the SF-312, Bolton acknowledged that "the unauthorized disclosure . . . of classified information by me could cause damage or irreparable injury to the United States" and agreed "never [to] divulge classified information" without "prior written notice of authorization from" the relevant government agency. By signing the two SF-4414s, Bolton also promised "never [to] divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization." In both agreements, Bolton acknowledged that the disclosure of classified information "may constitute a violation, or violations, of United States criminal laws."

23. On September 4, 2018, the U.S. Government granted an interim accreditation for a SCIF within the **TARGET RESIDENCE**. The SCIF was located in a corner of the basement of the **TARGET RESIDENCE**. Final accreditation for the SCIF was approved on September 17, 2018. The SCIF was approved for the processing and closed storage of classified information, including Top Secret information. The SCIF was decertified on October 16, 2019.

24. Based on my education, training, and experience, I know that the installation of a SCIF within the **TARGET RESIDENCE** indicated that Bolton anticipated storing classified materials within the **TARGET RESIDENCE** during his tenure as APNSA. Once he was no longer APNSA, effective September 10, 2019, his need-to-know expired, and any authorization for having access to the classified documents in the **TARGET RESIDENCE** was subsequently revoked.

25. A letter was sent to Bolton by the White House Counsel and Legal Advisor to the NSC on September 10, 2019, upon Bolton's separation from service with the U.S. government. The letter reminded Bolton of his continuing responsibility and obligation to "protect all

confidential, privileged, and classified information and to provide for the safe return of all government property that you received in connection with your position at the Executive Office of the President ("EOP")." The letter further stated,

> As the Assistant to the President for National Security Affairs, you were entrusted with information protected from disclosure, including classified information that related to some of the most sensitive matters of national security. You were previously advised that unauthorized disclosure, unauthorized retention, or negligent handling of certain classified information could cause irreparable injury to the United States or be used to advantage by a foreign nation. . . . All of these obligations extend beyond your period of employment at the EOP and the period in which you have access to classified information.

A copy of the letter was sent as an attachment to Bolton's personal AOL email address (the "Bolton AOL Account").

26. Accordingly, U.S. government records indicate that staff from the NSC visited the **TARGET RESIDENCE** on or about September 10, 2019, to retrieve any classified information and government property that had been provided to enable secure communications or the storage of classified material. Government emails from December 13, 2019, document that Bolton confirmed that the NSC Director of Security had cleared any classified documents from the SCIF at the **TARGET RESIDENCE** and denied possessing additional classified documents at his home.

27. An email from Bolton's assistant (herein "Bolton's Assistant") to the Legal Advisor to the NSC, sent on September 11, 2019, stated, "They came and got his secure phone and classified documents from his scif yesterday . . . he has nothing else to turn over to you upon his separation from the government . . ."

28. According to an NSC email obtained from the National Archives and Records Administration ("NARA"), Bolton met with two NSC officials, including a Deputy Legal Advisor, on September 13, 2019, to discuss his separation from government service and post-

government obligations. The Deputy Legal Advisor asked Bolton if he had any classified documents or Presidential Records Act ("PRA") documents to turn over in accordance with his legal obligations and the September 10, 2019, letter from the White House Counsel. The Deputy Legal Advisor clarified that the request included any handwritten notes, legal pads, or records in other locations. Bolton stated that all classified documents had been cleared from the **TARGET RESIDENCE** and he had none to turn over. Bolton also asked for a copy of his NDA read-offs, which are documents created during out-processing that detail obligations for safeguarding information learned while an employee was privy to classified information.

29. Government records indicate that Bolton made attempts to re-accredit his home SCIF in February 2020, even though he was no longer an employee of the U.S. government. Bolton's Assistant wrote over email on February 24, 2020, that Bolton was re-installing a SCIF in the **TARGET RESIDENCE** and needed the contact information for someone at the NSC who could accredit the SCIF. The NSC Director of Security responded the same day to say that installing an accredited SCIF in the **TARGET RESIDENCE** was "not a viable option."

2020 Book Pre-Publication Review

30. According to government records, Bolton submitted a draft manuscript for his book "The Room Where It Happened: A White House Memoir" to the NSC for the required pre-publication review process on or about December 30, 2019. A letter sent from Ellen J. Knight ("Knight"), the NSC Senior Director for Records, Access and Information Security Management to Bolton's attorney on January 23, 2020, acknowledged receipt of Bolton's manuscript, and notified Bolton that, based on a preliminary review, the manuscript appeared to contain

significant amounts of classified information, to include information classified at the TOP SECRET level.[2]

31. Another letter was sent via email from Knight to Bolton's attorney on February 7, 2023. The letter suggested that Bolton modify and resubmit the manuscript due to the large volume of classified information contained in the manuscript. The letter further stated,

> As written, the manuscript is very detailed, suggesting that it was likely produced from notes written by your client during his service at the White House. When your client received his employee debriefing, he stated that he did not have any notes or other records from his government service. Any notes that remain in your client's possession regarding the accounts in the manuscript may fall under the requirements of the Presidential Records Act and be subject to litigation holds. Please confirm whether your client has retained any notes or other records from his government service.

32. FBI Agents, accompanied by staff from the Office of the White House Counsel and federal prosecutors, interviewed Knight on February 13, 2020. Knight confirmed that she is an OCA, and one of her duties is to review material intended for publication as part of the pre-publication process. Knight had worked for the National Archives and NSC dealing with classification and declassification for approximately nine years at the time of the interview. Knight and her staff rely on Executive Order 13526 for categories of information that can be withheld from publication for national security, and the NSC security classification guidelines.

33. As explained by Knight, one of her staff completed the first review of the Bolton manuscript, and Knight completed the second, as per normal operating procedure. Knight and her staff identified a significant amount of classified material in the manuscript, up to the TOP

---

[2] In ruling on the government's request for a temporary restraining order and preliminary injunction to stop the release of the book, Judge Royce C. Lamberth stated in the court's order that "Bolton has gambled with the national security of the United States. He has exposed his country to harm and himself to civil (and potentially criminal) liability." *United States v. Bolton*, 468 F. Supp. 3d 1, 7 (D.D.C. June 20, 2020).

SECRET level. Knight stated that the material was more current and sensitive than what Knight and her staff typically see in pre-publication submission. Knight indicated that, in all her experience, she had never seen that level of classified material and specificity of detail in a manuscript submitted for review. There were quotes from foreign leaders from negotiations with the President and details of foreign military actions which had not yet been publicly acknowledged by the foreign governments. Based on her experience in reviewing manuscripts for pre-publication review and the level of detail contained in Bolton's submission, Knight surmised that Bolton either had an incredible memory or had to be writing from notes he would have taken as APNSA. Knight explained that any such notes were likely classified, fall under the PRA, and should have been turned over by Bolton at the conclusion of his government service.

34. During her interview, Knight expressed concern that Bolton may have retained notes containing classified information due to the extensive detail contained in the manuscript. She also stated that Bolton was known for carrying around a yellow legal notepad for taking notes, and noted there are public photographs of him carrying that style of notepad. There were no yellow notepads or notes found when Bolton was debriefed and his records collected, which added to Knight's concern about Bolton retaining notes. Knight stated that she was not personally present during Bolton's outbriefing, but that her Director for Records Management was present when White House Security collected and secured Bolton's records from his White House office.

35. A letter sent via email from Knight to Bolton's attorney on February 24, 2020, references and described a meeting held in person on the previous Friday between Knight and Bolton to review the manuscript. According to the letter, Knight reviewed instances of classified information in the manuscript and Bolton "appeared to acknowledge" the need to modify the

manuscript to remove classified information. Attached to the email was a photocopy of notes taken by Bolton during the meeting, which had been redacted to remove classified information.

Hack of Bolton AOL Account by Foreign Entity

36. On or about July 6, 2021, Bolton's Assistant contacted the FBI via e-mail to alert the FBI that an entity, believed by Bolton's Assistant to be in Iran, obtained access to the Bolton AOL Account. Bolton's Assistant wrote the following:

> I'm alerting you that evidently someone has gotten into Amb. Bolton's AOL account. See the attached – it looks as though it is someone in Iran that has changed the two factor authentication – added their email and phone number to his account…We noticed this morning that all of his "unread emails" that are in bold are quickly going to "read" status – going unbold which means they are reading his emails...If there is anything you can help us with, that would be appreciated.

37. An FBI Special Agent provided the following response to Bolton's Assistant via telephone: "During the course of an FBI cybercrime investigation, we developed information which indicated that one or more e-mail accounts under your control may have been compromised by a nation-state cyber actor around late June 2021. The [Bolton AOL Account] was specifically identified." The response is similar to advisements provided to other hacking victims. The FBI provided the following recommended steps to mitigate the harm caused by the hack: "It is recommended that you review the status of accounts under your control, and take any responsive actions which you may deem necessary, to include: Resetting account passwords; Deleting temporary passwords; Deleting unrecognized message handling rules; Removing unrecognized associated e-mail accounts; Removing unrecognized associated devices, and/or; Enabling multi-factor authentication."

38. On or about July 28, 2021, Bolton's Assistant contacted the FBI via e-mail to report that she and Bolton received a threatening e-mail that she believed to be related to the

hack of Bolton's AOL account in June 2021. The e-mail was sent on July 25, 2021, from an account using a name of a person known to Bolton and Bolton's Assistant. The e-mail, the subject of which was "Re:New PW," as forwarded to the FBI, stated:

> I do not think you would be interested in the FBI being aware of the leaked content of John's email (some of which have been attached), especially after the recent acquittal.
>
> This could be the biggest scandal since Hillary's emails were leaked, but this time on the GOP side!
>
> Contact me before it's too late ...

The original e-mail appeared to contain one or more attachments, which were removed from the e-mail that was forwarded to the FBI.

39. Bolton's Assistant prefaced the e-mail, when forwarding it to the FBI Special Agent, with the following message: "Just sending you the text (not the documents he attached since there might be sensitive information in them) of the last email that he sent to me so you can see what he said. I'll circle back to you after I tell Amb. Bolton all of this[.]"

40. Bolton's Assistant sent the following e-mail follow-up to the FBI to explain the information that had been obtained by the hacker(s):

> Just wanted to give you an update. This person emailed me over the weekend stating that he had sensitive documents that he got from Bolton's account and was threatening to release them to the public. What he has are a few of the early drafts of Bolton's book which I think he intercepted when Bolton was working on the road and sent them to himself. We don't know what other stuff he was able to get access to.

41. On or about July 29, 2021, Bolton's Assistant also sent the following follow-up email: "We are going to be deleting most of Amb. Bolton's emails (both in deleted folder and sent items but there are a lot of emails that got deleted automatically by AOL so it's hard to really remember everything that was in his account)[.]"

42. On or about August 5, 2021, the same account that sent the first threating message followed up with the following second message threatening to leak deleted portions of Bolton's manuscript: "OK John ... As you want (apparently), we'll disseminate the expurgated sections of your book by reference to your leaked email... Good luck Mr. Mustache!"

Discovery of Classified Material in Bolton Account

43. The FBI conducted a review of an account ("Account 1") used by a known cyber actor from an adversarial nation that was obtained with lawful authority. Account 1 was used for the spear-phishing of government officials of countries of interest to the adversarial nation, organizations and think-tanks involved in the development and implementation of government policy for those same countries, and the acquisition and storage of material unlawfully obtained from email accounts.

44. During a routine review of Account 1 contents by the FBI, an email was discovered that contained material judged by the FBI personnel to potentially contain classified and/or NDI material (DOCUMENT 1).

45. DOCUMENT 1 was an email sent from the Bolton AOL email account to himself, on or about June 21, 2019, during Bolton's tenure as APNSA. The document contained information regarding the activities of a militia group being operated by a foreign nation. The email started [redacted] START HERE..." [redacted] correspond to the initials of Bolton's [redacted]

46. On or about June 9, 2022, the FBI sent a copy of DOCUMENT 1 to the relevant U.S. intelligence agency for an OCA review. That agency confirmed that the information in the body of DOCUMENT 1 contained information classified at the TOP SECRET/SCI level. In my experience, information classified at this level often constitutes National Defense Information.

47. The FBI's investigation has revealed no record or indication that Bolton sought or received permission to utilize a personal AOL email account to process, retain, or send classified information.

48. The FBI's investigation has revealed no record of Bolton providing the June 21, 2019, email to the U.S. government in the course of surrendering all classified information in his possession upon leaving government service.

49. Based on the facts outlined above, as well as on my training and experience, I believe that on or about June 21, 2019, Bolton, without authorization, put information classified at the TOP SECRET/SCI level into the Bolton AOL Account. That account is not an authorized or secure location for the storage of classified information. He then then transmitted that information to himself [redacted], persons not authorized to receive it, using a system not authorized for the processing or transmittal of classified information.

Prior Legal Process on Bolton Email Accounts

50. On or about September 20, 2022, legal process was served on Yahoo Inc. for the Bolton AOL Account, to include search warrants and 2703(d) orders. An initial search warrant was served on Yahoo for the Bolton AOL Account for the dates June 6, 2019, to July 6, 2019.

51. On September 21, 2022, the responsive records received from Yahoo indicated that there were zero emails within the inbox and sent box for the requested time period. Yahoo records identified a second account (herein the "Bolton Google Account"), as a recovery email account for the Bolton AOL Account.

52. On November 1, 2022, pursuant to a court order under 18 U.S.C. § 2703(d), Yahoo provided header information for the Bolton AOL Account. These responsive records showed 39 emails in the account dated in 2018, only one of which was sent from the Bolton

AOL Account. There were zero emails dated 2019 or 2020 in the account. A review of records dated in 2021 revealed zero emails in the account for the months of January, March, April, May, and June. There was one email dated in February 2021, 71 in July 2021, 583 in August 2021, 645 in September 2021, 611 in October 2021, 524 in November 2021, and 417 in December 2021. All of the emails in the account dated 2021 were sent by Bolton from the Bolton AOL Account except for the one in February 2021. Based on my training and experience, these findings within the responsive records from Yahoo reveal that the contents of the Bolton AOL Account from the time period that Bolton served as National Security Advisor through 2020 have been deleted.

53. Deletion of records was further supported by the fact that on or about July 29, 2021, Bolton's Assistant emailed the FBI, in response to the hacking of the Bolton AOL Account, stating, "We are going to be deleting most of Amb. Bolton's emails both in deleted folder and sent items" in the Bolton AOL Account.

54. On November 1 and November 8, 2022, pursuant to a Court order under 18 U.S.C. 2703(d), Google LLC provided header information for the Bolton Google Account.

55. The 2703(d) order response from Google LLC identified one email sent from the Bolton Google Account to this same account in 2018, while Bolton was the National Security Advisor. The Bolton Google Account also contained five emails sent from Bolton's official White House email account while he was serving as National Security Advisor, three of which were sent to himself only. An additional six emails were sent from the Bolton Google Account to Bolton's White House account while he was National Security Advisor. All of the emails Bolton sent himself are considered relevant given that Bolton has previously emailed classified information to himself, as demonstrated by the June 21, 2019, email described above.

56. A search warrant was served on Yahoo Inc. for the Bolton AOL account for the time period August 12, 2018 to August 16, 2018. The returns confirmed that the Bolton AOL account had been purged of emails for the relevant time period.

Additional Legal Process on Accounts Used by [redacted]

57. The FBI further reviewed the contents of Account 1 and determined that it contained, among other unlawfully obtained material, emails from the Bolton AOL Account. Discovered in the review was an email sent from the Bolton AOL Account, on or about November 23, 2018, to [redacted] an account known to be used by [redacted] and [redacted] Attached to the e-mail was a 25-page document in Microsoft Word format containing information related to a U.S. intelligence agency (herein "DOCUMENT 2"). The document is labeled with a date and location and written in a narrative diary style. As with DOCUMENT 1, DOCUMENT 2 began with the phrase "[redacted] START HERE." [redacted] and [redacted] correspond to the initials of [redacted]

58. The FBI sent DOCUMENT 2 to the relevant U.S. intelligence agency for an OCA review. That agency confirmed that the information in the body of DOCUMENT 2, which Bolton sent to his [redacted], was classified at the SECRET//NOFORN level.

59. On or about April 18, 2024, search warrants were served on Yahoo Inc. and Google LLC for the contents of the [redacted] and the [redacted] for the time period of November 21, 2018 to November 25, 2018—the time period that would be expected to contain DOCUMENT 2.

60. DOCUMENT 2, previously assessed to contain classified information, was present in the responsive search warrant returns for the [redacted] and the [redacted] Expanded search warrants were served on Yahoo and Google for the [redacted] and [redacted] for the time period of Bolton's tenure as APNSA, April 9, 2018 to September 10, 2019.

61. In the returns for the expanded search warrants, an additional e-mail was discovered by FBI personnel that was assessed to potentially contain classified information (herein "DOCUMENT 3"). The e-mail was a 22-page Word Document matching the diary-style format of DOCUMENT 2. The document contained information related to a U.S. intelligence agency.

62. On or about August 1, 2024, FBI provided the relevant intelligence agency with a copy of DOCUMENT 3 for OCA review. The agency confirmed that one paragraph within the document contained information classified SECRET//REL TO USA, FVEY, and two paragraphs contained information classified TOP SECRET/SCI.

63. During the course of the investigation, the FBI recovered approximately 15 Word documents and two e-mails written in the style of a narrative diary entry, from the time period when Bolton was National Security Advisor. Of these 17 documents, 14 also have headings that include a date and geographic location. In reviewing Bolton's Outlook schedules, and referencing open-source news reporting, the dates on these documents appear to correspond to times when Bolton was traveling to, or from, the locations cited in the document headings, while serving as National Security Advisor.

64. Based on my training, experience, and education, including my familiarity with the facts and circumstances of this investigation, and discussions with other FBI personnel,

including subject-matter experts, most, if not all, of these 17 narrative-style documents appear to contain classified information, including information and categories/classes of information that would typically be classified at the Top Secret or SCI compartmented level.

65. Based on may training, experience, and education, including my familiarity with the facts and circumstances of this investigation, it is my conclusion that Bolton was routinely documenting classified and/or National Defense Information for his own use, and, on multiple occasions, retained or transmitted that information electronically via the Bolton AOL Account.

Bolton's Use of "Archive"

66. A review of all of the materials recovered over the course of the investigation, including the 17 narrative documents, reveals that Bolton frequently wrote short emails to himself and/or [redacted], about his official work on behalf of the U.S. Government, including certain information that he designated as for "the archive."

67. DOCUMENT 2 and DOCUMENT 3 contain 22 total references to keeping or saving documents for an archive. The following is a sample of references:

a. "Diagrams of all the day's events in the Archives"

b. "He had written it up in a memo I will try to find again and file in the archives."

c. "I have filed several versions of the statement in the Archives, roughly in chronological order"

d. "Copy of the e-mail in the Archives"

e. "copy in the archives" (Referring to a joint communique signed by U.S. President Donald Trump and Polish President Andrzej Duda)

f. "Notes by one staffer in attendance at the meeting in the archives." (Referring to an all-hands meeting of Situation Room staff)

g. "…which he later got to me in hard copy in New York. A copy is in the archives, and for the purposes of the quotes I will use in this Diary, I will quote the actual text, and not just my notes from the phone call." (Referring to a letter from North Korean Supreme Leader Kim Jong Un sent to Secretary of State Mike Pompeo.)

68. Based on my training and experience, the context of the references, including references to hard copies and to files appearing in a specific order, indicate that the archive is a physical archive rather than a digital archive.

69. A review of the investigative material also revealed instances when Bolton made references to keeping material known to be classified in his archive. In one instance, Bolton wrote the following: "A reporting cable from Embassy Ankara (. . . filed in the archives)." FBI analytical staff obtained a copy of the cable, which matches Bolton's description of the content, and is classified SECRET//NOFORN.

70. In another instance, Bolton wrote a narrative diary entry dated "…August 24-27 (Biarritz, en route to Kiev…)," which corresponds to a trip Bolton took with the administration to the G7 Summit in Biarritz, which started on August 23, 2019. In the entry, Bolton describes a communication with a foreign nation regarding recent actions by an adversary nation, and wrote about the FBI assessment of the issue: "see their assessment, filed in the archives." The description of the communication and issue match an FBI assessment provided in a Letterhead Memorandum to the National Security Council on August 12, 2019, that is classified SECRET//NOFORN.

71. Based on my training and experience, I know the classified material believed to be possessed by Bolton may be kept in different formats. The majority of the narrative diary entries were composed and sent in a Microsoft Word Document, rather than in the body of an

email. The entries also run as long as 49 pages, and have entries spanning multiple listed dates and locations. It is therefore likely the documents were composed in Microsoft Word and saved to a computer and/or cloud drive, and/or printed for further storage.

72. In my experience, it is not common for individuals to use solely employer-issued devices when writing documents intended to be kept after the employment ends. Therefore, I believe that the material described above likely was stored electronically or in hard copy in a location personal to Bolton, rather than solely on a government-owned device. Based on my training and experience, individuals who intend to keep sensitive documents after their employment ends or intend to publish books about their employment are likely to retain that information rather than deleting or destroying it.

73. Moreover, the inclusion of [redacted] START HERE" at the beginning of narrative diary entries indicate that Bolton likely sent these messages to his [redacted], persons not authorized to receive classified or national defense information, for the purposes of their review, likely while they were in a different location than Bolton. Therefore, the entries are likely saved to more than one place, potentially including on devices used by [redacted] and/or in hard copy.

74. I know from my training and experience that an archive containing sensitive and/or personal information to be used in drafting other documents would likely be kept in a secure place accessible to the owner, such as the owner's home or office.

75. Based on my training, experience, and education, including my familiarity with the facts and circumstances of this investigation, and discussions with other FBI personnel, I respectfully submit that there is probable cause to believe that evidence of the unlawful retention

and transmission of classified information and National Defense Information—including copies of documents containing such information—are located in the **TARGET RESIDENCE**.

EVIDENCE OF BOLTON'S KNOWLEDGE OF RULES GOVERNING THE HANDLING OF CLASSIFIED INFORMATION

76. Throughout Bolton's government career, including as a Department of Justice official and as National Security Advisor to the President, he has been given access to classified information and national defense information. Bolton has made numerous public statements about (1) the sensitivity of classified information; (2) the myriad adverse impacts on national security if classified information is mishandled; (3) his personal experience and practice in handling classified information (including through the use of secure communications facilities and SCIFs); and (4) his frequent criticism of how other government officials have handled classified information, including his opinions about whether the mishandling of classified or national defense information by one or more individuals constitutes a federal crime.

77. During a September 2, 2016, interview with Fox Business Network,[3] for example, Bolton discussed the then-recent revelation about a former Secretary of State's use of a private email server for government business, including the credibility (or lack of credibility) of the former Secretary of State's story about how it happened: "I remember those sorts of things because if you're conscious of the need to protect classified information you'll remember what the rules are[.]"

78. During a January 16, 2017, interview on Fox Business Network, Bolton continued to address the seriousness of the allegation involving Russian hacking of Democratic National Committee computer servers, and the consequences of mishandling classified information,

---

[3] John Bolton: Clinton displayed gross negligence with her emails. Fox Business https://youtu.be/20sSuoFHcGI?si=Qs-bFGLAaGXmw8QA.

stating, "Look, as I've said before, I believe it's still to this day, if I had done at the State Department what Hillary Clinton did, I'd be wearing an orange jumpsuit now." When asked about his opinion why government officials did not move their conversation to a secure government communications network, Bolton replied, "[H]ere's communication of sensitive information for dummies, the way I would look at it. You're either on a secure governmental system or you're not. You're not on a secure governmental system, you got a problem[.]"[4]

79. During an April 18, 2025, podcast interview, Bolton offered his views on allegations that U.S. government officials had communicated sensitive government information using Signal, an encrypted messaging platform:

> Initially, I was totally without words. I couldn't-I couldn't find-I couldn't find a way to express how stunned I was that anybody would do this. You simply don't use commercial means of communication, whether it's supposedly an encrypted app or not for for these kinds of discussions. You know, you don't know where they're gonna go. You could start off talking about a newspaper article, but but obviously you could get into classified material. I understand why you need to have group chats, but as I've been saying the place for the group chats are the Situation Room where everybody's in place some people may have to appear via secure video teleconference facilities, and and we've got great capacity to do that. But, but having chat groups where you're writing two or three sentences that this is not what you would call sophisticated national security analysis at work, and on an unsecured channel. It just, there's there's no excuse for it.[5]

80. When asked to comment about an administration official's characterization of the Signal situation as overblown, Bolton disagreed, stating, "I don't think that's a valid point. The question is what was the potential damage to the United States this kind of behavior caused[.]" Bolton went on to discuss how the unauthorized disclosure of classified information can cause damage to U.S. national security, and how that information is useful to foreign adversaries:

---

[4] *Id.* at 3:43.

[5] LEMON DROP – Bolton on Signal-Gate, Trump, and the Constitutional Crisis, available at https://youtu.be/7QLsu2fMpRc (Apr. 18, 2025). Starting at 10:25.

> [W]hat were they doing off of secure government channels, that is the original sin here. That is the question neither one of them has yet answered. You just referred to potential damage: has actual damage been done, though I think actual damage is possible because of the way foreign intelligence services operate, the way our own intelligence services operate. You take everything you can get. You take every piece of information in this case about American military operations against the Houthis in Yemen it tells you something that otherwise you wouldn't know about American capabilities, American tactics, American approaches to this kind of thing and that is useful to the Russians, the Chinese, the Iranians, the North Koreans, and others as well. How that fits into the body of knowledge they already have is a question I can't answer, but it can't help, that's for sure.[6]

81. During an April 25, 2025 interview on CNN, Bolton discussed that a person's ability to access classified information was a function not just of a person's security clearance level, but that the person receiving the classified information had a need to know the information:

> I think the second example of a Signal chat group . . . really shows a terrible lack of judgment and communicating with the people in this group in particular who have absolutely no need to know about any upcoming U.S. military operation leads me to wonder what he's doing on the job on a minute to minute hour by hour basis that he's got time to to knock out signal messages to to friends and family.[7]

82. Bolton addressed his concerns that the potential mishandling of classified information by high-level government officials might have adverse downstream consequences:

> This is not just for the people who are directly involved in that Signal group chat. It's for the thousands of other people in the federal government who handle sensitive information and are held to a higher standard, and they need to know that those standards apply up and down the line[.][8]

THE TARGET RESIDENCE

83. Based on my training and experience, I know that individuals who engage in offenses like the Subject Offenses are likely to have documents and media within their

---

[6] John Bolton Reacts to War Group Chat Leak - Channel 4 News, Mar. 26, 2025, found at https://youtu.be/13n1577TBk4.

[7] Trump's NSA RIPS INTO His SLOPPY Defense Secretary on A Fresh Signal SCANDAL https://youtu.be/z_OJ0uphV1E?si=_pNesP122dyYYXYQ (Apr. 25, 2025) (emphasis added).

[8] *Id.* at 15:47.

residences and offices that constitute evidence, fruits, and instrumentalities of those crimes. Furthermore, I know that it is common for those involved in the Subject Offenses to keep and conceal this information and these records, documents, and things in both hard-copy and digital form within computers, laptops, tablets, iPads, flash drives, cellular telephones, and other electronic storage devices.

84. According to a Real Property Data Search of the Maryland Department of Assessments and Taxation, the owner of the **TARGET RESIDENCE** is "John R Bolton" and [redacted]

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

85. As described above and in Attachment B, these applications seek permission to search for electronic devices, documents and other records that might be found in the **TARGET RESIDENCE,** in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other electronic storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

86. *Probable cause.* I submit that if a computer or storage medium is found in the **TARGET RESIDENCE**, there is probable cause to believe that records involving the Subject Offenses will be stored on that computer or storage medium, 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 computer, 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 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, computers' internal hard drives—contain electronic evidence of how a 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."

87. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET RESIDENCE** 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, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of 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. In my training and experience, information

stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers 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 storage medium 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, computer 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 computer 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. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

88. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a location (including a person) for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from a premises such as the **TARGET RESIDENCE**, or from an individual pursuant to a search warrant, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time in the **TARGET RESIDENCE** could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data in the **TARGET RESIDENCE.** However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

89. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

UNLOCKING BIOMETRICALLY SECURED DEVICES

90. The warrant for the **TARGET RESIDENCE** also would permit law enforcement to obtain from Bolton the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to the above-referenced warrants. I seek this authority based on the following:

91. 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 an alphanumeric password or pattern password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer only one of these features, while others offer a combination of these features, and the user of such a device can select the features that the user would like to utilize.

92. Additionally, I know that some encrypted messaging applications, such as certain versions of Signal and WhatsApp, offer users the ability to unlock the application using biometric authentication tools.

93. 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, some Apple devices offer 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.

94. 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, Apple offers a facial recognition feature 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 similar to Face ID.

95. 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.

96. As discussed in this affidavit, I believe that one or more digital devices will be

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

97. 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. These circumstances might, or might not, include: (1) when more than 48 hours has passed since the last time the device was unlocked, (2) when the device has not been unlocked for 8 hours and the passcode or password has not been entered in the last 6 days, (3) when the device has just been restarted or powered on, (4) when attempts to unlock via fingerprint have failed a specified number of times, (5) when the device has received a remote lock command. Thus, in the event that law enforcement encounters a locked device, the opportunity to unlock the device via fingerprint may exist only for a short time.

98. In my training and experience, the person who is in possession of a device, or who has the device among his or her belongings at the time the device is found, is likely a user of the device. However, I know that in some cases, it may not be possible to know with certainty who is the user of a given device, including if the device is found in a common area of a premises without any identifying information on the exterior of the device.

99. Accordingly, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to the requested warrants and may be unlocked using one of the aforementioned biometric features, the requested warrants would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of Bolton to the fingerprint

scanner of the device(s); and/or (2) hold the devices in front Bolton's face for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by the warrants.

CONCLUSION

100. Based on the above facts, I submit that there is probable cause to believe that Bolton has committed the Subject Offenses and there is probable cause to believe that the **TARGET RESIDENCE**, as further described in Attachment A, will contain evidence, fruits, and instrumentalities of the Subject Offenses, as described in Attachment B.

101. Thus, I respectfully request that the Court issue a search warrant authorizing the search of information described in Attachment A, to seek the items described in Attachment B.

REQUEST FOR SEALING

102. I further request that the Court order all papers in support of these applications, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the target(s) of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give Bolton or others who may be involved in this criminal activity an opportunity to flee, destroy or tamper with evidence (including electronic accounts that can be deleted before law enforcement is aware of their existence), change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

[redacted]
Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 21st day of August, 2025.

HONORABLE TIMOTHY J. SULLIVAN
CHIEF UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

The **TARGET RESIDENCE** is a residence located at [redacted] The **TARGET RESIDENCE** is a [redacted]

[redacted]

ATTACHMENT B

Particular Things to be Seized

All items, records, documents, files, or materials, in whatever form they exist, that constitute evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Section 793(d), Title 18, United States Code, Section 793(e), and Title 18, United States Code 1924(a), (the "Subject Offenses") involving John Robert Bolton II (Bolton) [redacted] occurring on or after April 9, 2018, including:

1. All physical documents and records with or without classification markings that appear to be classified, relate to Bolton's former position as Assistant to the President for National Security Affairs, or appear to be diary entries or material that Bolton was saving for an "archive," along with any containers or boxes (including any other contents) in which such documents are located, as well as any other containers or boxes that are collectively stored or found together with the aforementioned documents and containers or boxes;

2. Information, including communications in any form, regarding the retrieval, storage, or transmission of classified material or information related to the national defense;

3. Any digital devices[9] electronic storage media[10] and/or their components, that may constitute instrumentalities of, or contain evidence of the Subject Offenses, including:

    a. any digital device or other electronic storage media used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, or optical scanners;

    b. any magnetic, electronic, or optical storage device capable of storing data, such as USB devices, SD cards, CDs, DVDs, optical disks, smart cards, PC cards, electronic notebooks, and personal digital assistants;

    c. any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

---

[9] Digital devices" include any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units; laptop, desktop, notebook, or tablet computers; computer servers; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, routers and switches; electronic/digital security devices; wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, and Blackberries; digital cameras; digital gaming devices; global positioning satellite devices (GPS); or portable media players.

[10] "Electronic storage media" is any physical object upon which electronically stored information can be recorded, including hard drives, flash memory, USB devices, SD cards, CD, DVDs, and other magnetic or optical media.

d. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

e. any physical keys, encryption devices, dongles, and similar physical items that are necessary to gain access to the computer equipment, storage devices, or data; and

f. any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data.

4. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media 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, "chats," instant messaging logs, photographs, and correspondence;

b. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

c. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

d. evidence of the times the digital device or other electronic storage media was used;

e. evidence of access to electronic accounts of people other than Bolton, including Google, Apple, Microsoft 365, and social media platforms.

f. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

g. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media; and

h. contextual information necessary to understand the evidence described in this attachment.

5. Information[11] that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the Subject Offenses or (ii) communicated about matters relating to the Subject Offenses, including records that help reveal their whereabouts;

6. Information that constitutes evidence indicating state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning, related to the Subject Offenses;

7. Information as to the identities, roles and responsibilities of coconspirators, accomplices, and aiders and abettors in the commission of the Subject Offense, including but not limited to records that would reveal their whereabouts;

8. Communications of any kind with other individuals regarding the Subject Offense;

9. Passports, visas and travel records (solely as to Bolton);

10. All appointment books, schedules, calendars, list of contacts, telephone message slips, phone records, diaries, memos, and all other similar items (solely as to Bolton).

11. All records, documents, programs, applications, and materials that show indicia of occupancy, residency, control and/or ownership of the **TARGET RESIDENCE**, including but not limited to utility bills, telephone bills, loan payment receipts, rent documents, canceled envelopes, keys, photographs and bank records.

12. All safes, whether combination or lock type, and their contents, and all storage facility and safety deposit box records and keys

13. Records and things evidencing the use of an Internet Protocol ("IP") address to communicate with the internet including:

    a. records of IP addresses used; and

    b. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorited" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

---

[11] As used herein, the terms "records," "documents," and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); any photographic form; or any physical form.

14. This warrant authorizes the search and forensic analysis of electronic devices containing the foregoing evidence if:

    a. The electronic devices are found within rooms known or discovered to be used by Bolton, [redacted]

    b. A person inside the premises advises officers executing the warrant that the electronic devices were used by Bolton, [redacted]

    c. Officers reasonably believe the device was utilized in connection with the use of an electronic device falling into one of the two categories listed above.

15. This warrant does not authorize the search or forensic analysis of electronic devices that do not fall within the scope of the preceding paragraph.

With respect to the search of any electronic device falling within the scope of this warrant believed to be owned, possessed, or used by Bolton, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Bolton to the fingerprint scanner of a device; (2) hold the device in front of the face of Bolton and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by the warrant.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

2. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

3. "scanning" storage areas to discover and possible recover recently deleted files;

4. "scanning" storage areas for deliberately hidden files; or

5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.