UNITED STATES DISTRICT COURT

for the

District of Columbia

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

THE OFFICE LOCATED AT [redacted]

UNDER RULE 41

Case No. 25-sw-241

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, hereby incorporated by reference.

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

See Attachment B, hereby incorporated by reference.

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 793(d),(e), 18 U.S.C. § 1924(a)	(Conspiracy to gather, transmit or lose defense information); (Unauthorized removal and retention of classified documents and material)

The application is based on these facts:

See Affidavit in Support of the Application for Search Warrant

- ☐ 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]
Applicant's signature

[redacted] Special Agent
Printed name and title

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

Date: 08/22/2025

Judge's signature

City and state: Washington, D.C.

Moxila A. Upadhyaya, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ☑ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Columbia

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

THE OFFICE LOCATED AT [redacted] UNDER RULE 41

Case No. 25-SW-241

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Jurisdiction of the District of Columbia
(identify the person or describe the property to be searched and give its location):

See Attachment A, hereby incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, hereby incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before September 4, 2025 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Moxila A. Upadhyaya, U.S. Magistrate Judge
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: 22 MAG 08/21/2025

M. Upadhyaya
Judge's signature

City and state: Washington, D.C.

Moxila A. Upadhyaya, U.S. Magistrate Judge
Printed name and title

Return

Case No.: 25-SW-241	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

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

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
Property to Be Searched

The **TARGET OFFICE** is an office located at [redacted] The office is [redacted] Known features of the office include [redacted] The **TARGET OFFICE** is any office known to be occupied or otherwise used by Bolton, and any secured or shared storage space, to include safe(s), file cabinets, and locked or unlocked containers. (hereinafter "SUBJECT MMW)

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), 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, [redacted] 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 OFFICE**, 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 three 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.

16. Safes, both combination and key type, and their contents, which can contain evidence of the commission of the SUBJECT OFFENSES or proceeds from the commission of the SUBJECT OFFENSES.

17. Keys, passwords, monetary instruments, including cash (all denominations and currencies) and cryptocurrency wallets, precious metals and other objects which could constitute proceeds of illicit activity.

18. Indicia of ownership, including, receipts, invoices, bills, canceled envelopes, and keys, which provides evidence of identity as to individuals committing the SUBJECT OFFENSES; and

19. Digital devices used in the commission of, or to facilitate, the above-described SUBJECT OFFENSES, including storing, maintaining, keeping or downloading classified materials.

20. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device(s)," seizure of:

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

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

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

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

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

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

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

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

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

j. All information that constitutes fruits, contraband, evidence, and instrumentalities of the SUBJECT OFFENSES as described in the affidavit submitted in support of this Warrant and identified in paragraph (1) above.

k. Information that constitutes evidence of the identification or location of the user(s) of the Device; and

l. Information that constitutes evidence concerning how and when the Device was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Device user.

21. Routers, modems, and network equipment used to connect computers to the Internet.

During the execution of the search of the TARGET LOCATION described in Attachment A, law enforcement personnel are also specifically authorized to obtain from the Subject, (but not any other individuals present at the TARGET LOCATION at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). Law enforcement are authorized to attempt to unlock any such Device(s)'s security features in order to search the contents as authorized by this warrant by compelling the display of such a physical biometric characteristic; that is, (1) by pressing or swiping the fingers or thumbs of the aforementioned person against the fingerprint scanner of any such Device(s) and/or (2) by holding in front of the face of the aforementioned person to activate the facial recognition or iris recognition feature of any such Device(s).

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. Specifically, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request

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.

As used above, the terms "records" and "information" includes 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); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies). The term "digital devices" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF THE OFFICE LOCATED AT [redacted] UNDER RULE 41	**Case No. 25-SW-241** **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 an office used by John Robert Bolton, II ("Bolton"), located at [redacted] ("**TARGET OFFICE**" or PREMISES), which is described more fully in Attachment A, for things described in Attachment B, to include electronic devices contained therein. 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 OFFICE**.

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 OFFICEE** is located within the District of Columbia.

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]

20. Bolton maintains the **TARGET OFFICE** located at [redacted] Washington, D.C. 20036. The John Bolton PAC and the Foundation for American Security and Freedom are two organizations known to be associated with Bolton. Both organizations list the **TARGET OFFICE** address as their official address. The FBI previously interviewed Bolton eight times between October 2020 and June 2025 at the **TARGET OFFICE** address and it was documented as his office. According to Federal Election Commission filings, Bolton began using the **TARGET OFFICE** in approximately December 2014, and still uses it.

Bolton's Tenure as APNSA, [redacted] ***and Separation from Government Service***

[1] [redacted]

21. 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.

22. 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.

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

24. [redacted]

16, 2019.

25. [redacted]

26. 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").

27. [redacted]

28. [redacted]

29. [redacted]

30. [redacted]

31. 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]

32. 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.

33. [redacted]

[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).

[redacted]

34. [redacted]

[redacted]

35. [redacted]

[redacted]

36. 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

37. [redacted]

38. [redacted]

[redacted]

39. [redacted]

[redacted]

[redacted]

[redacted]

40. [redacted]

[redacted]

41. [redacted]

[redacted]

[redacted]

42. [redacted]

43. [redacted]

44. [redacted]

45. [redacted]

46. [redacted]

47. [redacted]

48. [redacted]

49. [redacted]

50. [redacted]

51. [redacted]

52. [redacted]

[redacted]

53. [redacted]

[redacted]

54. [redacted]

[redacted]

55. [redacted]

[redacted]

56. [redacted]

[redacted]

[redacted]

57. [redacted]

[redacted]

58. [redacted]

[redacted]

59. [redacted]

[redacted]

60. [redacted]

[redacted]

[redacted]

61. [redacted]

[redacted]

62. [redacted]

[redacted]

63. [redacted]

[redacted]

64. [redacted]

[redacted]

65. [redacted]

66. [redacted]

67. [redacted]

68. [redacted]

[redacted]

69. [redacted]

[redacted]

70. [redacted]

[redacted]

71. [redacted]

[redacted]

72. [redacted]

[redacted]

[redacted]

73. [redacted]

[redacted]

74. [redacted]

[redacted]

75. [redacted]

[redacted]

76. 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 OFFICE**.

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

77. 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.

78. 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[.]"

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

79. 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, 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]

80. 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]

81. 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

---

[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.

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:

> [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]

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

82. 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]

83. 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 OFFICE

84. 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 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.

85. According to open-source documents, Bolton began using the **TARGET OFFICE** in approximately December 2014, and still uses it.

---

[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.

TECHNICAL TERMS

75. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage

devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as

described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address,

an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across

shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

86. 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 OFFICE**, 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). One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are

found at the TARGET LOCATIONS, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

87. Individuals who engage in criminal activity, including theft and transmission of national defense information, use digital devices, like the Device(s), to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device(s), documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; store information related to their cryptocurrency activity, including use of digital wallets and back up recovery materials; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of the materials with national defense information contained therein, including copies and other forms of the information. As discussed above, BOLTON likely secreted the classified and national defense information using such Device(s) and has likely kept other such material in the TARGET LOCATIONS.

88. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

89. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or

no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

90. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices,

I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

91. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this

data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

92. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

93. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

94. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

95. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-

virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

96. I know that when individuals like BOLTON use a digital device to commit the SUBJECT OFFENSES the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.asdfa

97. *Probable cause.* I submit that if a computer or storage medium is found in the **TARGET OFFICE**, 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."

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

88. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to

recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or

deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256

encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

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

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data;

scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

4. The TARGET OFFICE is a functioning office that conducts legitimate business. The seizure of the digital devices may limit Bolton's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what digital devices must be seized or copied, and what digital devices need not be seized or copied. Where appropriate, law enforcement personnel executing the warrant will copy data, rather than physically seize digital devices, to reduce the extent of disruption. If Bolton or his employees so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing

function of the legitimate business. If, after inspecting seized digital devices, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve evidence, the government will return it.

BIOMETRIC ACCESS TO DEVICE(S)

90. This warrant permits law enforcement agents to obtain from the person of BOLTON (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometic access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

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 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.

92. 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.

93. 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 Android devices and is called "Trusted Face." During the Trusted Face 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 (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

94. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

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, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently 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.

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. 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 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. 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.

98. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from

the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

99. The proposed warrant does not authorize law enforcement to require that the ~~aforementioned person(s)~~ SUBJECT state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION

91. 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 OFFICE**, as further described in Attachment A, will contain evidence, fruits, and instrumentalities of the Subject Offenses, as described in Attachment B.

92. 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.

[redacted]
Special Agent
Federal Bureau of Investigation

Subscribed and sworn persistent to Fed. R. Crim. P. 4.1 and 41(d)(3) on August 22 (mdh), 2025.

M. A.

MOXILA A. UPADHYAYA
UNITED STATES MAGISTRATE JUDGE

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
25-SW-241	8/22/2025 11:03 a.m.	John R. Bolton

Inventory made in the presence of : [redacted]

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

1 Dell Optiplex 3070

1 HP Laptop Model 17

1 Dell Laptop XPS

USB Flash Drive, black with green center

1 Binder titled "U.S. Dept of State Diplomatic Security: An Introductory Security Briefing Prepared for the 2000-2001 Transition Team

1 Dell Optiplex SFF Plus 7010

Travel Memo documents with pages labeled Secret

US Mission to the United Nations - Confidential documents

U.S. Government Strategic Communications Plan - Confidential Documents

Confidential Documents with [redacted] heading

Weapons of Mass Destruction classified Documents

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 9/5/2025

[redacted]

Executing officer's signature

[redacted], Special Agent

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF THE OFFICE LOCATED AT [redacted] **UNDER RULE 41**	**Case No. 25-sw-241** **Filed Under Seal** **HSD Filing**

ORDER

This matter having come before the Court pursuant to applications filed on this docket on August 22, 2025, including the search warrant, and the application and affidavit in support thereof, and all attachments thereto and other related materials such as this application and order, (collectively, the "Warrant"), the Court finds that, because of such reasonable grounds to believe the disclosure will result in flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, and serious jeopardy to the investigation, the United States has established that a compelling governmental interest exists to justify the requested sealing.

1. IT IS THEREFORE ORDERED that the application is hereby GRANTED, and that the warrant, the application and affidavit in support thereof, all attachments thereto and other related materials, the instant application to seal, and this Order are sealed until otherwise ordered by the Court. The government, however, is authorized to provide the application material to defense counsel in any case involving a charged defendant, subject to a protective order.

2. IT IS FURTHER ORDERED that the Clerk's office shall not make any entry on the public docket of the Warrant until further order of the Court.

Date: August 22, 2025

M. Upadhyaya

MOXILA A. UPADHYAYA
UNITED STATES MAGISTRATE JUDGE

U.S. District and Bankruptcy Courts
for the District of Columbia
A TRUE COPY
ANGELA D. CAESAR, Clerk
By Maricarmen Giron
Deputy Clerk

cc: TEJPAL S. CHAWLA
Assistant United States Attorney
United States Attorney's Office
601 D Street, N.W.
Washington, D.C. 20530