

Exhibit 1

AUSA: Sullivan USAO 2022R00343

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

UNITED STATES DISTRICT COURT

for the
District of Maryland

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

THE PREMISES LOCATED AT [REDACTED]

Case No.

8:25-mj-02126-TJS

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

See attachment A

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

See attachment B

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	Gathering, transmitting or losing defense information
18 U.S.C. § 1924	Unauthorized removal and retention of classified documents or material

The application is based on these facts:

See affidavit of FBI Special Agent [REDACTED]

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

[REDACTED]
Applicant's signature

[REDACTED]
Printed name and title

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3).

Date: August 21, 2025

City and state: Greenbelt, Maryland

[Signature]
Judge's signature

Timothy J. Sullivan, Chief United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT [REDACTED]

*
*
*
*
*

UNDER SEAL

8:25-mj-02126-TJS

GOVERNMENT'S MOTION TO SEAL

The United States of America, by and through undersigned counsel, hereby moves this Honorable Court for an Order sealing the Search Warrant, the Application, and the Affidavit in support thereof, together with this Motion in the above-referenced matter:

1. The Affidavit submitted in support of the above-referenced Search Warrant contains information regarding an ongoing investigation relative to alleged violations of Title 18 U.S.C. § 793 (Gathering, transmitting or losing defense information) and 18 U.S.C. § 1924 (Unauthorized removal and retention of classified documents or material). The target is unaware of the investigation and if they became aware, may flee or take steps to destroy or conceal the evidence sought pursuant thereto.

2. In order to justify sealing the Affidavit, the Government must demonstrate that: (1) there is a compelling Government interest requiring materials to be kept under seal and (2) there is no less restrictive means, such as redaction, available. In re Search Warrants Issued on April 26, 2004, 353 F. Supp. 2d 584 (D. Md. 2004).

3. Disclosure of the Affidavit at this time could seriously jeopardize the investigation as it would reveal the names and pictures of the targets and the locations of the search before the Search Warrant can be executed. Further, continued investigation based on the results from the Search Warrant could be jeopardized if the Affidavit is prematurely unsealed. Indeed, if the documents are not sealed, given the nature of the charges, disclosure would in all

likelihood compromise the integrity of the investigation by, among other things, causing the target to flee or take steps to destroy or conceal evidence, which would adversely affect the outcome of the investigation.

4. The procedures for sealing are set forth in Baltimore Sun Co. v. Goetz, 886 F.2d 60 (4th Cir. 1989). “The judicial officer may explicitly adopt the facts that the government presents to justify the sealing.” Id. at 65. This motion and the Court’s reasons for sealing should also be sealed. See id. Notice of the sealing is required, but the notice requirement is satisfied by the docketing of the order sealing the documents. Id.

WHEREFORE, the Government respectfully requests that the Search Warrant, Application, and the Affidavit in support thereof, together with this motion and the Court’s reasons for sealing, if made express in the Order, be placed under seal.

Respectfully submitted,

Kelly O. Hayes
United States Attorney

By:

Thomas M. Sullivan
Thomas M. Sullivan
Assistant United States Attorney

KOH

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT [REDACTED]
[REDACTED]

*

*

UNDER SEAL

*

*

8:25-mj-02126-TJS

*

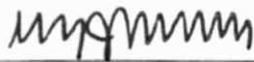
*

*

ORDER

Upon review of the Motion of the United States of America, the Court hereby adopts the Government's proffer of the reasons for sealing as presented therein, and it is this ^{21st} day of August 2025, **ORDERED** that the Search Warrant, the Application, and the Affidavit in support thereof, and this Motion, shall be **SEALED** until further Order of this Court.

It is further **ORDERED** that the Clerk of the Court provide a copy of this Order to the United States Attorney's Office.



Honorable Timothy J. Sullivan
Chief United States Magistrate Judge

AUSA: Sullivan 2022R00343

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

☒ Original☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the
District of Maryland

In the Matter of the Search of

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

THE PREMISES LOCATED AT [REDACTED]

Case No.

8:25-mj-02126-TJS

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 _____ District of _____ Maryland _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

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.

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 _____
Duty 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:

August 21, 2025 5:44pm
Judge's signature




City and state:

Greenbelt, Maryland

Honorable Timothy J. Sullivan, Chief United States Magistrate Judge

Printed name and title

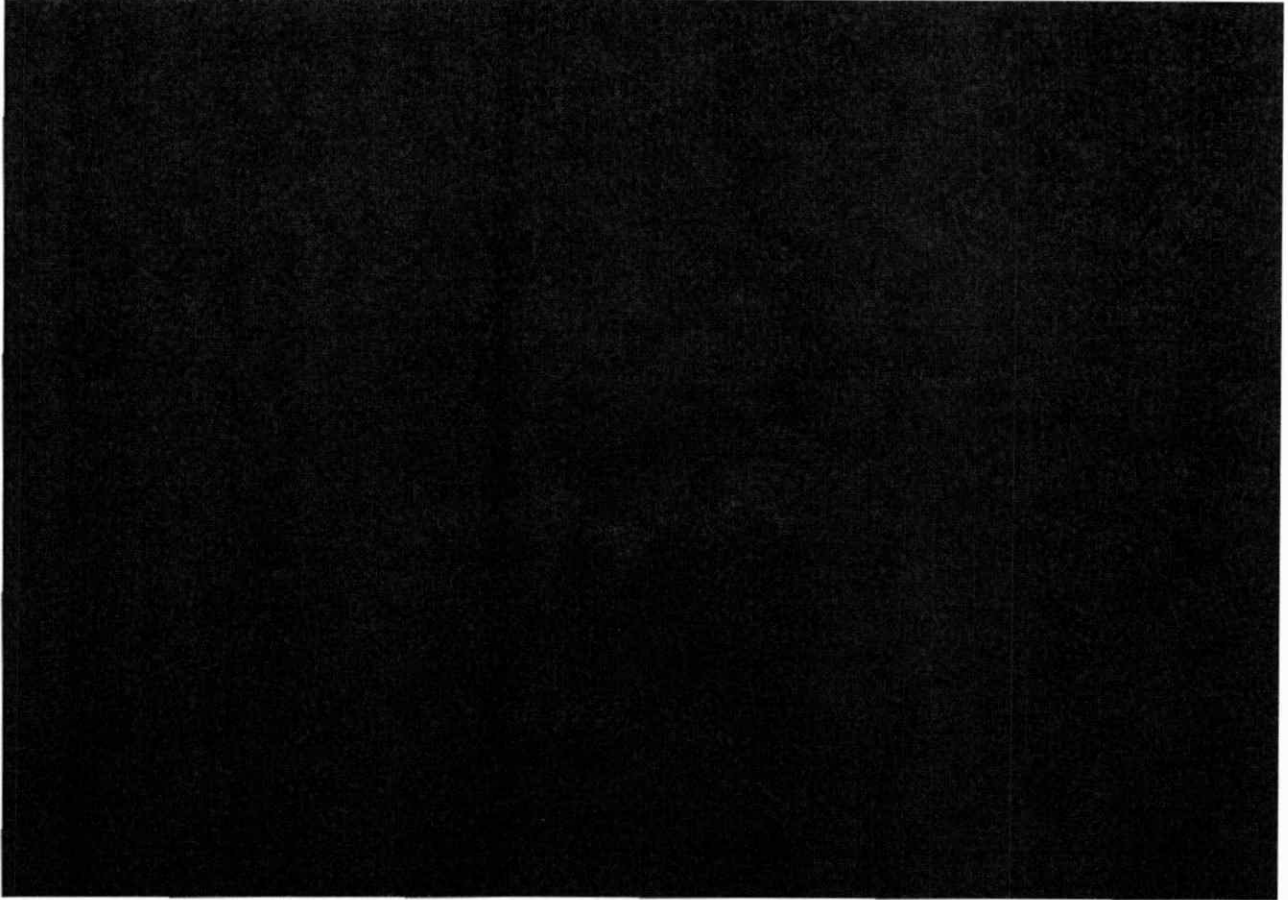
AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: 8:25-mj-02126-TJS	Date and time warrant executed: 8/22/2025 7:00am	Copy of warrant and inventory left with: John E. Balten
Inventory made in the presence of: 		
Inventory of the property taken and name(s) of any person(s) seized:		
<p>1 red iPhone w/ 2 camera lenses</p> <p>1 black iPhone in black case</p> <p>White binder labeled "Statements and Reflections to Allied Strikers..."</p> <p>Typed documents in folders labeled "Trump I - IV"</p> <p>4 boxes containing printed daily activities</p> <p>1 hard drive seagate brand</p> <p>1 Dell Precision Tower computer 3620</p> <p>1 Sandisk 64 GB USB drive</p> <p>1 Sandisk 64 GB USB drive</p> <p>1 Silver Dell XPS laptop w/cables</p> <p>1 Silver Dell Inspiron 2330 computer</p>		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned electronically along with the warrant to the designated judge pursuant to Fed. R. Crim. P. 4.1 and 41(f)(1)(D).</p>		
Date: 9/2/2025	 Executing officer's signature	
	 Printed name and title	

ATTACHMENT A
Property to Be Searched

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

[REDACTED] The **TARGET RESIDENCE** is a [REDACTED]
[REDACTED]



ATTACHMENT B

Particular Things to be Seized

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

1. All physical documents and records with or without classification markings that appear to be classified, relate to Bolton's former position as Assistant to the President for National Security Affairs, [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 devices⁹ electronic storage media¹⁰ 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. Information¹¹ that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the Subject Offenses or (ii) communicated about matters relating to the Subject Offenses, including records that help reveal their whereabouts;
6. Information that constitutes evidence indicating state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning, related to the Subject Offenses;
7. Information as to the identities, roles and responsibilities of coconspirators, accomplices, and aiders and abettors in the commission of the Subject Offense, including but not limited to records that would reveal their whereabouts;
8. Communications of any kind with other individuals regarding the Subject Offense;
9. Passports, visas and travel records (solely as to Bolton);
10. All appointment books, schedules, calendars, list of contacts, telephone message slips, phone records, diaries, memos, and all other similar items (solely as to Bolton).
11. All records, documents, programs, applications, and materials that show indicia of occupancy, residency, control and/or ownership of the **TARGET RESIDENCE**, including but not limited to utility bills, telephone bills, loan payment receipts, rent documents, canceled envelopes, keys, photographs and bank records.
12. All safes, whether combination or lock type, and their contents, and all storage facility and safety deposit box records and keys
13. Records and things evidencing the use of an Internet Protocol ("IP") address to communicate with the internet including:
 - a. records of IP addresses used; and
 - b. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorited" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

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

14. This warrant authorizes the search and forensic analysis of electronic devices containing the foregoing evidence if:
 - a. The electronic devices are found within rooms known or discovered to be used by Bolton, [REDACTED]
 - b. A person inside the premises advises officers executing the warrant that the electronic devices were used by Bolton, [REDACTED]
 - c. Officers reasonably believe the device was utilized in connection with the use of an electronic device falling into one of the two categories listed above.
15. This warrant does not authorize the search or forensic analysis of electronic devices that do not fall within the scope of the preceding paragraph.

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

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

1. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
2. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
3. "scanning" storage areas to discover and possibly recover recently deleted files;
4. "scanning" storage areas for deliberately hidden files; or
5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

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

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

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