

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

V.

IAN A. BRINKSMAN,

Defendant.

Case No. 1:26-mj-423

**AFFIDAVIT IN SUPPORT OF A CRIMINAL
COMPLAINT AND ARREST WARRANT**

I, John W. Althen, being duly sworn, declare and state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation (FBI). I have been so employed since approximately August 2004. As a Special Agent of the FBI, I have participated in the investigation of violations of various federal criminal laws, including investigations involving national security and espionage. I have conducted and/or participated/assisted in surveillance, interviews of witnesses and subjects, applications for and the execution of physical and electronic searches, and arrests. In my current position, I am responsible for conducting and assisting in investigations into the activities of individuals whose conduct may constitute a threat to national security and/or a violation of federal law. As a result of my training, education, and experience, I am familiar with the manner in which criminal activity is carried out, and the efforts of persons involved in such activity to avoid detection by law enforcement. As a Special Agent of the FBI, I am authorized to investigate violation of laws of the United States, and execute warrants issued under the authority of the United States.

2. I make this affidavit in support of a criminal complaint charging Ian BRINKSMAN (“BRINKSMAN”) with the unlawful transmission of national defense information, in violation of 18 U.S.C. §793(d).

3. Unless otherwise noted, the conclusions and beliefs expressed in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I have drawn from my training, experience, and knowledge of the investigation. The facts contained in this affidavit come from my review of the evidence, my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. Except as explicitly set forth below, I have not distinguished in this affidavit between facts of which I have personal knowledge and facts of which I have hearsay knowledge. This affidavit is intended only to demonstrate that probable cause exists in support of the requested criminal complaint and does not include all information known to me or to other law enforcement officers regarding this investigation.

STATUTORY BACKGROUND

4. United States Government information that is sensitive, controlled, or classified is governed by Executive Order, policies and regulations, and federal law. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States Government; (2) falls within one or more of the classification levels set forth in the Executive Order, specifically TOP SECRET, SECRET, and CONFIDENTIAL; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security of the United States.

5. Under Executive Order 13526, the unauthorized disclosure of material classified at the “TOP SECRET” level (“TS”), by definition, “reasonably could be expected to cause exceptionally grave damage to the national security” of the United States. Exec Order 13526 § 1.2(a)(1), 75 Fed Reg. 707, 707-08 (Jan. 5, 2010). The unauthorized disclosure of information classified at the “SECRET” level (“S”), by definition, “reasonably could be expected to cause serious damage to the national security” of the United States. Exec. Order 13526 § 1.2(a)(2). The unauthorized disclosure of information classified at the “CONFIDENTIAL” level (“C”), by definition, “reasonably could be expected to cause damage to the national security” of the United States. Exec. Order 13526 1.2(a)(3).

6. Sensitive Compartmented Information (“SCI”) is classified information related to intelligence sources, methods, and analytical processes. SCI is to be processed, stored, used, or discussed in an accredited Secured Compartmented Information Facility (“SCIF”), and only individuals with the appropriate security clearance and additional SCI permissions are authorized access to such classified national security information. For any unauthorized persons to receive access to such classified information, the originating United States agency must determine that such release is appropriate.

7. Pursuant to Executive Order 13526, information classified at any level shall be lawfully accessed only by persons determined by an appropriate United States government official to be eligible for access to classified information, who has signed an approved non-disclosure agreement, who has received a security clearance, and who has a “need to know” the classified information. Classified information shall only be stored or discussed in an approved facility.

8. Under 18 U.S.C. § 793(d), “[w]hoever, lawfully having possession of, access to, control over, or being entrusted with any document . . . 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 fined or imprisoned not more than ten years, or both.

9. The elements of Section 793(d) are as follows:
 - a. The defendant had lawful possession of, access to, control over, or was entrusted with;
 - b. 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;
 - c. The defendant had reason to believe the information could be used to the injury of the United States or the advantage of any foreign nation;
 - d. The defendant communicated, delivered, or transmitted (or attempted or caused to be communicated, delivered, or transmitted) the above material to any person not entitled to receive it; and
 - e. The defendant did so willing.

PROBABLE CAUSE

Background on BRINKSMAN's Employment

10. Beginning in or around 2020, BRINKSMAN worked as an employee of a U.S. government agency based in the Eastern District of Virginia. In or around September 2022,

BRINKSMAN began working as an employee for a third-party company (“Company 1”) as a contractor to the same U.S. government agency. BRINKSMAN works as a developer for systems integration.¹

11. At all times relevant to this affidavit, BRINKSMAN possessed a TS/SCI security clearance in connection with his work for the U.S. government.

12. As further detailed below, email records, phone records, and open-source information reveal that BRINKSMAN has an ongoing personal relationship with an individual who maintains an online publication on Substack² (“Individual 1”). Individual 1 published articles on Substack and has referred to her Substack account as “her new independent publication” for “[r]eporting on Congress, War, and political economy.” A fundraising article reportedly published by Individual 1 in September 2026 stated “over the past year [Individual 1 has] published reporting based on classified [relevant U.S. government agency] assessments that I believe the public deserves to know about.” Individual 1’s social media profile shows Individual 1 commenting in a public post, “I also accept leaks.”

13. BRINKSMAN works inside of a SCIF. At the U.S. government facility where he works, BRINKSMAN is required to wear a badge and badge in and out of both the building where he works and the specific SCIF in which he works.

14. As a condition of his employment, BRINKSMAN signed various non-disclosure agreements, to include one signed on December 18, 2025, in which BRINKSMAN was granted

¹ According to the U.S. government agency where BRINKSMAN works, BRINKSMAN conducts data transfers between classified and unclassified systems as part of his typical work duties.

² Substack is an online platform that provides publishing, payment, analytics, and design infrastructure to support subscription-based content, including newsletters, podcasts, and video. It allows writers to send digital content directly to subscribers.

access to SCI materials. This non-disclosure agreement states, “I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to the advantage by a foreign nation.” The non-disclosure agreement further cautioned that “unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including provisions of Sections 793, 794, 798, and 952.”

16. As another condition of his employment, BRINKSMAN also completed numerous training courses related to the handling of classified information. For example, BRINKSMAN completed trainings related to classification and system administrator security in March and September 2026, respectively. Through the course of his employment, BRINKSMAN was advised and trained on the proper handling and storage of classified information.

BRINKSMAN's Access to Classified Intelligence Reports and Contact with Individual 1

17. In or around 2022, BRINKSMAN requested access to a specific repository of classified intelligence (“the Classified Database”). U.S. government records reflect that BRINKSMAN first accessed the Classified Database on August 11, 2022.

18. On or about March 11, 2026, Individual 1 contacted BRINKSMAN via cell phone at approximately 8:41 a.m.³ BRINKSMAN used a cell phone with the number ending in 6350 to receive this call and to make the calls described below.⁴ Less than an hour later that same day, BRINKSMAN accessed records from the relevant government agency that owns the Classified Database. Specifically, information from the government agency shows BRINKSMAN accessed

³ All call times are listed in Eastern Daylight Time (“EDT”).

⁴ Call records show more than 800 calls or attempted calls between BRINKSMAN and Individual 1 to date in 2026.

a specific classified report in the Classified Database (“Report 1”), which was marked TOP SECRET, at 9:09 a.m. and then again at 10:01 a.m.

19. According to records from the relevant government agency, BRINKSMAN exited the facility where he works at approximately 11:15 a.m. and then re-entered the building at 11:23 a.m., and departed the facility again at 1:02 p.m. Later, on the same day at approximately 8:08 p.m., Individual 1 called BRINKSMAN (for approximately 14 minutes). BRINKSMAN entered the campus of the facility where he works at 8:16 p.m. and then entered his workspace at approximately 8:27 p.m. He finally departed the facility at 10:01 p.m.

20. On or about March 11, 2026, the same date that BRINKSMAN accessed Report 1, Individual 1 posted an article on Substack with a similar content (“Article 1”). Based on my review of Article 1, it contains certain content similar to Report 1. An Original Classification Authority has confirmed that Article 1 contains classified information up to the TOP SECRET level that reflects the information in Report 1.

21. On or about May 12, 2026, BRINKSMAN called Individual 1 at approximately 8:25 a.m. (for approximately 10 minutes). Later that same day, records from the relevant government agency which owns the Classified Database reflect that BRINKSMAN accessed another classified report in the Classified Database (“Report 2”), which was marked TOP SECRET, at 11:26 a.m. According to badge swipe records, BRINKSMAN exited the secure facility at approximately 12:57 p.m. BRINKSMAN then called Individual 1 at 1:07 p.m. (for approximately three minutes), at 4:34 p.m. (for approximately 27 minutes), at 5:04 p.m. (for approximately 10 minutes), and at 5:15 p.m. (for approximately 10 minutes). Similar to the sequence of events on March 11, 2026, shortly thereafter, Individual 1 posted an article on or about the next day, May 13, 2026, with similar content (“Article 2”). Based on my review of Article 2,

it contains certain content similar to Report 2. An Original Classification Authority has confirmed that Article 2 contains classified information that reflected classified information in Report 2.

22. On or about May 26, 2026, BRINKSMAN called Individual 1 at 8:18 a.m. (for approximately 8 minutes). According to badge swipe records, BRINKSMAN entered the government facility where he works at 8:54 a.m. Less than twenty minutes later, records from the relevant government agency which owns the Classified Database reflect that BRINKSMAN accessed another classified Report in the Classified Database ("Report 3") at 9:10 a.m. BRINKSMAN departed the secure facility at approximately 3:00 p.m. Less than fifteen minutes later, BRINKSMAN proceed to call Individual 1 at 3:13 p.m. (for approximately 12 minutes), at 3:30 p.m. (for approximately 10 minutes), and again at 6:44 p.m. (for approximately 3 minutes). Similar to the sequence of events on March 11 and May 12, 2026, shortly thereafter, Individual 1 posted an article on or about May 28, 2026, with similar content ("Article 3"). Based on my review of Article 3, it contains certain content similar to Report 3. An Original Classification Authority has confirmed that Article 3 contains classified information that reflected classified information in Report 3.

23. On or about July 28, 2026, Individual 1 called BRINKSMAN at approximately 8:24 a.m. (for approximately 18 minutes). On that same date, records from the relevant government agency which owns the Classified Database reflect that BRINKSMAN accessed a report in the Classified Database ("Report 4"), which was marked TOP SECRET, at 10:32 a.m. According to records from the relevant government agency, BRINKSMAN exited the facility where he works at approximately 11:32 a.m. BRINKSMAN proceeded to call Individual 1 at approximately 11:45 a.m. (for approximately 18 minutes) and then re-entered the building at 12:19 p.m. BRINKSMAN called Individual 1 again at approximately 2:45 p.m. (for approximately three minutes). Individual

1 posted an article on or about July 29, 2026, with similar content ("Article 4"). Based on my review of Article 4, it contains certain content similar to that of Report 4. An Original Classification Authority has confirmed that Article 4 contains classified information that reflected classified information in Report 4.

24. On or about August 24, 2026, BRINKSMAN contacted Individual 1 at 8:29 a.m. (for approximately 22 minutes) and again at 12:16 p.m. (for approximately 45 minutes). On or about August 24, 2026, access records from the relevant government agency which owns the Classified Database again reflect that BRINKSMAN accessed a classified report in the Classified Database ("Report 5") on two separate occasions at 2:42 p.m. and 2:49 p.m. BRINKSMAN contacted Individual 1 again at 5:40 p.m. (for approximately 20 minutes).

25. On or about August 25, 2026, BRINKSMAN contacted Individual 1 at 8:13 a.m. (for approximately two minutes) and then Individual 1 contacted BRINKSMAN at 8:24 a.m. (for approximately 17 minutes). Access records from the relevant government agency also reflect that BRINKSMAN accessed Report 5 again at 8:53 a.m. BRINKSMAN then contacted Individual 1 at 3:49 p.m. (for approximately 12 minutes), and Individual 1 contacted BRINKSMAN at 4:10 p.m. (for approximately 30 minutes).

26. On or about August 26, 2026, BRINKSMAN contacted Individual 1 at 8:28 a.m. (for approximately 23 minutes). Access records from the relevant government agency also reflect that BRINKSMAN accessed Report 5 again at 9:53 a.m. on the same day. Report 5 was marked TOP SECRET.

27. On or about October 1, 2026, Individual 1 called BRINKSMAN at approximately 8:34 a.m. (for approximately six minutes). A little over an hour later, BRINKSMAN accessed Report 5 again in the Classified Database at 9:39 a.m. According to records from the relevant

government agency, BRINKSMAN exited that facility where he works at approximately 12:03 p.m. Individual 1 called BRINKSMAN at approximately 12:11 p.m. (for approximately 47 minutes). BRINKSMAN re-entered the building at 1:05 p.m. BRINKSMAN later called Individual 1 at approximately 5:40 p.m. (for approximately 37 minutes). Individual 1 posted an article on or about October 5, 2026, with similar content (“Article 5”). Based on my review of Article 5, it contains certain content similar to that of Report 5. An Original Classification Authority has confirmed that Article 5 contains classified information that reflected classified information in Report 5.

28. I understand that individuals at BRINKSMAN’s workplace are not permitted to have their cell phones or personal electronic devices with them while at work. In my training and experience, most people at BRINKSMAN’s workplace keep electronic devices, including cell phones, in their vehicles for easy retrieval and use. Based on my training and experience, the short window between BRINKSMAN’s access of these Reports and BRINKSMAN’s re-entry to his work site would have provided him sufficient time to leave his location in the facility, go to his vehicle to communicate with Individual 1 regarding the information BRINKSMAN had accessed from the Classified Database using a personal cell phone, and then return to the facility.

29. BRINKSMAN’s work facility is located in the Eastern District of Virginia, and he accessed Articles 1 through 5 in the Eastern District of Virginia.

30. According to the relevant U.S. government agency where BRINKSMAN works, none of these Reports—Reports 1, 2, 3, 4, or 5—was within the scope of BRINKSMAN’s work. All five Reports have various classification markings, to include TS and all the include TS/SCI classification banners at the top of the Reports. Material that is TS/SCI “reasonably could be expected to cause exceptionally grave damage to the national security” of the United States. Exec

Order 13526 § 1.2(a)(1), 75 Fed Reg. 707, 707-08 (Jan. 5, 2010). I know based on my training and experience that TS/SCI information is typically closely held. Based on a classification review conducted by the relevant equity holder, Articles 1 through 5 contain classified information. Each of Articles 1 through 5 contained similar content lifted from Reports 1 through 5.

31. Additionally, records from the relevant government agency reflect that BRINKSMAN was one of no more than six individuals who accessed the relevant Substack page from the federal government facility between March 1 and October 5, 2026. Other than BRINKSMAN, records from the relevant government agency reflect none of the other individuals who accessed the relevant Substack page during this time period viewed all five of the Articles and also accessed the five Reports.

32. On or about October 10, 2026, law enforcement reviewed a notebook that was left on BRINKSMAN's desk. The corners of several pages were torn out of the notebook. I know based on my training and experience, that people often take notes to be able to pass along full verbatim or near verbatim quoted information.

33. BRINKSMAN and Individual 1 also corroborated on a separate article later posted to Individual 1's Substack account. The article related to geopolitical issues in the Middle East. Specifically, on March 13, 2026, at approximately 10:20 a.m., an email notification was generated from Individual 1 to BRINKSMAN that a Google Document had been shared for editing. The Google Document had a title referencing a specific country. At approximately 10:32 a.m., an email notification was generated from BRINKSMAN to Individual 1 stating, "instead of ending with 'if' maybe change to 'combat operations.'" At approximately 10:32 a.m., an email notification was generated from Individual 1 to BRINKSMAN marked as "Resolved." Later the same day,

Individual 1 posted an article on a public website with a title referencing the same identified country. At this point, the government has not identified classified equities in this article.

34. On or about November 20, 2025, prior to accessing of all of the classified reports described herein, BRINKSMAN sent an email from his Gmail account to a friend stating, “So yeah, I’m still laying low and trying to figure out what’s next (once the dust finally settles.) The lady I’ve been seeing is a journalist and recently went independent. So I’ve been helping her get that off the ground. Her venture focuses on foreign policy. So, I’m getting a surprising amount enrichment/fulfilment from working on that.”

35. Based on the content contained in other emails from both BRINKSMAN’s Gmail account and BRINKSMAN’s email account with the third-party company who employs BRIINKSMAN it is clear that BRINKSMAN and Individual 1 are in a relationship. Based on my training and experience, I believe that Individual 1 is the “lady” and “journalist” referenced in BRINKSMAN’s November 20, 2025, email referenced above.

36. As a requisite for maintaining his security clearance, BRINKSMAN is required to seek prepublication approval before publishing anything in the media. Based on my investigation, I understand BRINKSMAN has sought prepublication review for any articles he has co-authored with Individual 1.

[remainder of page intentionally left blank]

CONCLUSION

37. I submit that this affidavit establishes probable cause to believe BRINKSMAN committed a violation of 18 U.S.C. §793(d). Therefore, your affiant respectfully requests that the Court issue an arrest warrant BRINKSMAN.

s/ John Althen

John Althen
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to, in accordance
with Fed. R. Crim. P. 4.1, by telephone
on this 23 th day of October 2026.



Honorable William E. Fitzpatrick
United States Magistrate Judge