EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

REDACTED AND UNSEALED

IN THE MATTER OF SEARCHES RELATED TO HANNAH NATANSON	)	No. 1:26sw54

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR WARRANTS TO SEARCH AND SEIZE

I, Matthew T. Johnson, a Federal Bureau of Investigation ("FBI") Special Agent, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), a position I have held since October 2004. As a Special Agent, I have received training at the FBI Academy located in Quantico, Virginia, including training on investigative methods and training specific to counterintelligence and espionage investigations. I am currently assigned to a squad at the FBI Washington Field Office, Counterintelligence Division, where I primarily investigate counterintelligence matters. As an FBI Special Agent, I have conducted or participated in witness and subject interviews, physical surveillance, service of subpoenas, the execution of search and arrest warrants, the seizure of evidence, including computer, electronic, and e-mail evidence, as well as requested and reviewed pertinent records. Based on my experience and training, I am familiar with the requirements for the handling of classified documents and information. I am also familiar with the methods used by individuals engaged in the unlawful use or disclosure of classified information.

2. Under Rule 41 of the Federal Rules of Criminal Procedure, I make this affidavit in support of applications for search warrants for the following locations and persons, all anticipated to be located within the Eastern District of Virginia:

A. 313 S. Royal Street, Alexandria, Virginia 22314-3715 ("Natanson Residence"), further identified in Attachment A-1, with items to be seized in Attachment B (collectively, the "Natanson Electronics");

B. A maroon 2013 Ford Fusion with Virginia license plate TRD 2309 ("Natanson Vehicle"); further identified in Attachment A-2, with items to be seized in Attachment B; and

C. The person of Hannah Natanson ("Natanson") further identified in Attachment A-3, with items to be seized in Attachment B.

3. The proposed search warrants seek authorization, pursuant to Rule 41(c), to search the Natanson Residence, the Natanson Vehicle, and the person of Natanson for evidence of violations of 18 U.S.C. § 793 (gathering, transmitting, or losing national defense information) (the "Target Offense") in the Natanson Electronics. Natanson is a reporter for the Washington Post. The warrants seek authority to seize the Natanson Electronics because there is probable cause to believe the devices contain "evidence of a crime," "contraband, fruits of crime, or other items illegally possessed," and "property . . . used in committing a crime." Specifically, for the reasons set forth below, there is probable cause to believe that the Natanson Electronics contain classified national defense information that was unlawfully removed from secure U.S. Government ("Government") facilities and unlawfully transmitted to one or more individuals who were not entitled to receive it.

4. On January 8, 2025, a United States Magistrate Judge in the District of Maryland found probable cause that Aurelio Luis Perez-Lugones ("Perez-Lugones") unlawfully retained classified national defense information and issued a criminal complaint charging him with violating 18 U.S.C. §793(e). The criminal complaint charging Perez-Lugones is attached hereto

as Exhibit 1. Perez-Lugones was arrested on January 8, 2026, and had his initial appearance on Friday, January 9, 2026.

5. As described below, there is probable cause to believe that Perez-Lugones removed classified national defense information from his workplace and transmitted the same on multiple occasions to Natanson, who, as described above, is a reporter for the Washington Post. The Washington Post published at least five news articles containing classified information provided by Perez-Lugones dated between October 31, 2025, and January 9, 2026. Natanson contributed to all five articles. Natanson is the owner and user of the Natanson Electronics.[1]

6. These warrants seek authorization from the Court to seize the Natanson Electronics in connection with the investigation of Perez-Lugones because there is probable cause to believe these devices contain classified national defense information unlawfully provided to Natanson by Perez-Lugones, potentially including classified information that has not yet been published. Through this warrant, the Government seeks to recover classified information that is evidence of Perez-Lugones's crimes and which, if disclosed, could harm national security.

7. The facts in this affidavit are from my personal observations derived from my participation in this investigation, my training and experience, and information obtained from a variety of other sources, including other law enforcement agents who have years of experience handling national security matters and investigations, witness interviews, public records, and

[1] This warrant does not seek authorization to search or seize devices that do not belong to Natanson. Recognizing that Natanson lives with her fiancé or partner, who based on information and belief is a government employee, law enforcement agents will make every reasonable effort to identify and exclude devices owned by him.

documents discussed herein. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter. I have not, however, excluded any information known to me that would defeat a determination of probable cause. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

8. Based on my training and experience and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the Natanson Electronics contain "evidence of a crime," "contraband, fruits of crime, and other items illegally possessed," and "property . . . used in committing a crime" related to Perez-Lugones's unlawful gathering, retention, and transmission of classified information. Therefore, pursuant to Rule 41(c)(1)-(3), I seek authorization to search the locations described in Attachments A-1, A-2, and A-3 for the purposes of seizing the devices and records further described in Attachment B.

PROBABLE CAUSE

STATUTORY AUTHORITY AND DEFINITIONS

9. Under 18 U.S.C. § 793(e) (the "Target Offense"), "[w]hoever 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 [commits a federal offense.]"

10. 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).

11. 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 to access such classified national security information. For a foreign government to receive access to classified information, the originating Government agency must determine that such release is appropriate.

12. Pursuant to Executive Order 13526, information classified at any level shall be lawfully accessed only by persons determined by an appropriate 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.

Perez-Lugones is Arrested for Unlawful Retention of National Defense Information

13. On January 8, 2026, Perez-Lugones was arrested and charged with unlawfully retaining classified national defense information in violation of 18 U.S.C. § 793(e). Specifically, as alleged in the criminal complaint, Perez-Lugones repeatedly took screenshots of classified information from classified systems, pasted those screenshots into unmarked Microsoft Word documents, and printed those Microsoft Word documents. On multiple occasions, Perez-Lugones also allegedly took handwritten notes containing classified information and then removed the handwritten notes from his secure workplace. The following facts are drawn from the criminal complaint charging Perez-Lugones:

(a) Perez-Lugones is a United States citizen born in Miami, Florida. At the time of his arrest, he lived in Laurel, Maryland. Perez-Lugones had been a Government contractor in various capacities since 2002.

(b) At the time of the events described in the criminal complaint, Perez-Lugones worked as a systems engineer and information technology specialist for a Government contracting company whose primary customer was a Government agency. Perez- Lugones was a system administrator with access classified systems, networks, databases, and repositories as required for his job. Perez-Lugones's desk was in a SCIF.

(c) As detailed in the criminal complaint, on multiple occasions since at least October 2025, while having authorized access to classified systems, Perez-Lugones navigated to and searched databases or repositories containing classified information without authorization. There, Perez-Lugones accessed and viewed classified intelligence reports or

summaries of classified intelligence reports. Those reports or report summaries were produced, created, or maintained by several Government agencies.

(d) On October 28, 2025, Perez-Lugones searched for, accessed, and viewed a classified intelligence report related to a foreign country. ("Country 1"). That report was classified TOP SECRET. Perez-Lugones took a screenshot of the report and pasted that screenshot in an unmarked Microsoft Word document. The screenshot of that report rendered one of the four bullet points listed at the end of the report illegible due to how the screenshot was cropped. Perez-Lugones also opened an attachment to that report, took screenshots of the attachment, and pasted those screenshots into the same Microsoft Word document. After this, Perez-Lugones printed the Microsoft Word document hours before logging off the system for the day.

(e) The classified national defense information contained in the Microsoft Word document printed by Perez-Lugones on October 28, 2025, subsequently appeared in a news article published by the Washington Post on October 31, 2025. This article was authored by Natanson and others.

(f) On January 6, 2026, Perez-Lugones logged onto the classified system shortly after arriving at his workplace. That afternoon, he picked up a yellow notepad, examined and removed approximately three pages, folded those pages in half, and set those pages on his desk. Perez-

Lugones then gathered his things, picked up the pages he had removed from the notepad, and left his desk area with the pages in hand.

(g) The following day, January 7, 2026, Perez-Lugones again logged onto the classified system shortly after arriving at his workplace. Perez-Lugones again took notes on a yellow notepad. Throughout the morning, he was observed looking back and forth between the screen corresponding to the classified system and the notepad, all the while writing on the notepad. At around 10:52 a.m., Perez-Lugones was observed leaving his desk with a yellow notepad page, leaving his workplace, getting into his vehicle, and driving to his residence. Less than an hour later, Perez-Lugones was observed driving his vehicle back to his workplace and entering the workplace carrying his mobile phone.

PEREZ-LUGONES'S ARREST

14. On January 8, 2026, FBI agents initiated a *Terry* stop on Perez-Lugones upon his arrival home after work. As a result of the *Terry* stop, Perez-Lugones agreed to participate in a voluntary interview, consented to a search of his cell phone, and unlocked his cell phone for agents to search.

15. During the search of Perez-Lugones's mobile phone, the FBI observed that the Signal application was being used to communicate with Natanson, the user of the Natanson Electronics. Specifically, the FBI reviewed and photographed Signal messages between Perez-Lugones and Natanson (who was identified in the chat by her initials and whose contact card explicitly said that she was a Washington Post reporter), and noted that the messages were set to auto-delete after one day. Those messages discussed classified information, the classification

level of that information, and contained Portable Document Format ("PDF") and JPEG files uploaded and sent to Natanson by Perez-Lugones. Both files contained information marked as classified. As discussed below, the following day, some of that information appeared in a Washington Post article authored by Natanson and others. The FBI did not identify any other PDF documents containing classified information on Perez-Lugones's mobile phone, suggesting that Perez-Lugones had deleted any messages or files previously sent to Natanson.

16. Review of the Signal chat between Perez-Lugones and Natanson revealed their use of Signal as a means to obfuscate and conceal their actions. It also revealed Natanson's knowledge of the classified nature of the information she was receiving as well as her direct request for specific follow-up information related to the classified reporting Perez-Lugones was providing. For example, after Perez-Lugones provided the above-referenced PDF through Signal, Natanson requested, "if there is any way to get more detail on that [Government Agency] report and the [Country 1] safely that would be a top priority for us."

17. Later on January 8, 2026, a United States Magistrate Judge in the District of Maryland issued a warrant authorizing the search of Perez-Lugones's mobile phone, residence, vehicle, workplace, and person. The FBI executed the search warrant that same day. Inside a lunch box contained within Perez-Lugones's vehicle, the FBI identified a classified intelligence report. As a result of the search warrant and the interview in which he voluntary participated, Perez-Lugones was placed under arrest.

Five Washington Post Articles Contain Classified Information Provided by Perez-Lugones

18. From October 2025 to January 2026, the Washington Post published at least five articles containing classified information and national defense information provided by Perez-Lugones, as described below. As alleged in the criminal complaint charging Perez-Lugones,

during this same period Perez-Lugones was seen at his workplace viewing, copying, printing, and removing classified records and notes that contained the same information published by the Washington Post. *See generally* Ex. 1 at ¶¶ 15-32, 35.

19. On October 31, 2025, the Washington Post published an article containing direct quotes from an intelligence report that Perez-Lugones printed on October 28, 2025. The intelligence report was marked as classified up to the TOP SECRET level. The byline for the corresponding Washington Post article was shared by four individuals, including Natanson. The article quoted, among other things, three of the four bullet points in the report, omitting the same bullet point that was illegible in Perez-Lugones's screenshot of the report. The article expressly stated that the information it set forth was based on "internal U.S. government documents obtained by the Washington Post."

20. On November 11, 2025, the Washington Post published an article containing direct quotes from a summary of a different intelligence reports that Perez-Lugones printed on November 5, 2025. The intelligence report was marked as classified up to the SECRET//NOFORN level. The corresponding Washington Post article did not contain any classified information outside of the summary printed by Perez-Lugones. The byline for this article was shared by five individuals, including Natanson.

21. On December 8, 2025, the Washington Post published an article containing direct quotes from an intelligence report that Perez-Lugones printed on December 4, 2025. The classified intelligence report was marked up to the CONFIDENTIAL//NOFORN level. The corresponding Washington Post article also summarized other portions of the report. The byline for this article was also shared by five individuals, again including Natanson.

22. On January 6, 2026, at around 7:30 p.m., the Washington Post published an article containing specific numbers corresponding to information in a classified intelligence report that Perez-Lugones accessed and viewed on January 5, 2026. The intelligence report was marked as classified up to the SECRET//FGI//NOFORN level. The byline for the corresponding Washington Post article was shared by three individuals, including Natanson.

23. On January 9, 2026, the Washington Post published an article containing information from a classified intelligence report that Perez-Lugones accessed on January 8, 2026. The intelligence report was marked as classified up to the SECRET//NOFORN level. This is the same classified intelligence report that was found inside his lunch box during the FBI's search of his vehicle on January 8, 2026. The corresponding Washington Post article summarized portions of the report. The byline for this article was also shared by eleven individuals, again including Natanson. The article contains information that Perez-Lugones sent to Natanson on January 8, 2026, as revealed by the FBI's search of his mobile phone on that date.

Natanson Details Her Use of the Natanson Electronics to Receive Information, Including From Perez-Lugones

24. In addition to the temporal relationship between Perez-Lugones' unauthorized printing, copying, and removal of classified information and the publication of these Washington Post stories authored by Natanson, Natanson has also publicly written about her use of the Natanson Electronics to receive information, including (implicitly) from Perez-Lugones. On December 24, 2025, the Washington Post published an article authored by Natanson that detailed her efforts to find and recruit Government employees and contractors as sources using Reddit and Signal. Natanson stated, in the article, that she used Signal on her "iPhone." Based on my

training and experience, I also know that users can access Signal using personal computers. In the article, Natanson also stated that she "bought a privacy screen for my iPhone and computer. I carried both with me at all times, even walking between rooms in my house." The reference to her iPhone and computer is a reference to the Natanson Electronics.

25. In the article published on December 24, 2025, Natanson describes using Reddit[2] to ask Government employees and contractors to contact her using Signal. Natanson provided her Signal contact information (*i.e.*, a phone number) on Reddit.[3] Accessing messages on Signal can be done through one's phone or computer. Natanson's December 24, 2025, article indicates that she used the Natanson Electronics to access the Signal messages she received as part of listing her contact information on Reddit.

26. Natanson quoted, in the article, Signal messages from Government employees and contractors from various agencies going back to at least February 4, 2025. Natanson also states in the article that among the many tips she was receiving, they related to topics she does not cover, including national security: "[p]eople were saying our national security was at risk, but i didn't know how to write about these things, or even who in our newsroom did." Natanson did not have authorization at any time to access, retain, or use classified information or materials relating to the national defense.

27. Natanson describes in the article how hundreds of Government employees and contractors reached out to her using Signal. Toward the end of the article, Natanson wrote that

---

[2] Specifically, the author posted on Reddit asking Government employees and contractors to reach out regarding Government employment issues.

[3] The author also posts her Signal contact information on the Washington Post's website.

she still received messages on Signal, and "[s]ome become stories[.]" After that statement, the article contains a link to the article published on October 31, 2025, which contains direct quotes from the classified intelligence report from which Perez-Lugones captured only three of four bullets from and printed on October 28, 2025.

28. Natanson described developing the "safest possible sourcing system." This system involved asking Government employees and contractors to "send [her] a picture of their government ID," "keep[ing] notes from reporting conversations in an encrypted drive, never writing down anyone's name," and "us[ing] a private browser with no search history." She also "retitled every Signal chat by agency" and "bought a privacy screen for [her] iPhone and [her] computer."

29. Natanson stated, in the article, that she shared some of the Signal messages with her fiancé, a Government security clearance holder.

30. Towards the end of the article, Natanson states that she "still wake[s] up to between 30 and 100 Signal notifications."

31. Signal is a web-based and mobile application that can be downloaded and accessed using a mobile phone, tablet, or desktop computer. Signal can be downloaded through the Google Play Store on mobile phones with an Android operating system[4] or through the Apple App Store on mobile phones with an iPhone operating system.[5] To sign up for Signal, a user must provide a phone number.

---

[4] Google owns the Android operating system. The Android operating system is used on most non-Apple mobile phones.

[5] Apple owns the iPhone operating system. The iPhone operating system is used on Apple mobile phones.

32. According to FBI open-source research, a Signal account exists for Natanson's known mobile phone number. In fact, Natanson has publicly identified her Signal account through the Washington Post and on Reddit. The FBI confirmed Natanson's mobile phone number through queries of both Government and publicly available commercial databases in January 2026.

33. Signal, as a secure messaging service, provides end-to-end encryption for user messages. This means that the messages are not in a readable format while in transit, not even to Signal, including when the messages are passing through Signal's servers. The only places where the Signal messages are stored in unencrypted form are in the sender's and receiver's Signal application, as well as possibly in a personal data storage cloud if the sender or receiver utilizes back-up services hosted by providers such as Google (*i.e.*, Google Drive).

34. Based on my training and experience, individuals who receive unlawfully transmitted classified or national defense information will often receive the same electronically using services provided by Google or services enabled by Google such as Google Drive, and encrypted messaging applications like Signal.[6] This may, in some cases, simply involve the receipt of information as text messages in the Signal application. In other cases, this may involve receiving documents containing classified information, such as photographed documents taken with a mobile phone's camera function, and then receiving the resulting digital files through Signal. Additionally, the images and messages stored in unencrypted form in the mobile phone's Signal application, may be backed up to cloud storage as part of default settings in the phone or other cloud service.

[6] Individuals use Signal because of the application's end-to-end encryption, which limits the ability to intercept the content of communications.

35. Alternatively, my training and experience has included witnessing or learning of hand delivery of paper documents by individuals who are involved in the unlawful transmission of classified information. From December 12, 2025, until January 8, 2026, the FBI maintained physical surveillance of Perez-Lugones to observe any potential in-person meetings between Perez-Lugones and Natanson. The FBI physical surveillance provided coverage every day from 6:00 a.m. to 10:00 p.m., including holidays and weekends. Additionally, since December 17, 2025, the FBI maintained closed-circuit television ("CCTV") surveillance of Perez-Lugones' residence for around the clock coverage of any comings and goings by Perez-Lugones. Neither FBI physical surveillance nor CCTV surveillance have observed any meetings between Natanson and Perez-Lugones. Hence, it is my professional assessment that Perez-Lugones transmitted classified information to Natanson exclusively via electronic means.

36. Based on the results of the FBI's physical surveillance, evidence seized pursuant to the search warrants, and Natanson's explicit description of using Signal to communicate with her government sources, the FBI believes that Natanson is using Signal to receive the content of the original classified and sensitive reports from Perez-Lugones, either in the form of text messages or digital images. The FBI further believes that evidence of Perez-Lugones's unauthorized gathering, retention, and transmission of classified and national defense information may be found in the Natanson Electronics based on Natanson's own identification of the use of these devices in her December 24, 2025, Washington Post Article. In addition to the use of her mobile phone and laptop computer, Natanson also indicates that she, "kept notes from reporting conversations in an encrypted drive." This evidence may include the actual unencrypted messages within the Signal application itself, saved documents previously

transmitted by Perez-Lugones, and additional data related to the transmission that may be stored elsewhere within the Natanson Electronics or metadata (*e.g.*, log files).

PROBABLE CAUSE TO SEARCH THE NATANSON RESIDENCE, NATANSON VEHICLE, AND NATANSON'S PERSON

37. There is probable cause to believe that evidence, fruits, instrumentalities, or contraband of the Target Offense will be found in the Natanson Electronics because Natanson has been observed carrying a mobile phone during work hours. Further, Natanson appears to have used an Apple iPhone associated with the phone number 202.580.5477 to receive classified information and to communicate with individuals about the same using Signal or some other mobile phone-based application. This is based not only on my training and experience, but also on Natanson's acknowledgement in the December 24, 2025, article that she uses Signal to receive sensitive national security information, likely to include the classified information at issue in this investigation. Signal is tied to a phone number, which further evinces that there is probable cause to believe that Natanson's Electronics will contain evidence of a crime, contraband, and property used to commit a crime (i.e., the information transmitted by Perez-Lugones and communications regarding the same). At approximately 8:40 a.m. yesterday morning, the FBI observed Natanson using an Apple iPhone while walking from her residence to the King Street Metro Station.

38. During the search of Perez-Lugones's mobile phone on January 8, 2026, law enforcement identified the above-described Signal chat between Perez-Lugones and Natanson. Law enforcement further observed that messages in this chat were set to auto-delete after one day.

39. Based on my training and experience, there is probable cause to believe that Natanson saved evidence, fruits, contraband or instrumentalities of crime she received from Perez-Lugones because Natanson took longer than the one-day auto-delete period to write an article and because journalists are generally required to preserve their source material.

40. Based on my training and experience, I understand that individuals may store sensitive records on electronic devices or electronic storage media located in their residences or vehicles. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that if evidence, fruits, contraband or instrumentalities of crime originally resided on Natanson's mobile phone, it may also be saved to other digital devices within the Natanson Residence or Natanson Vehicle.

41. A review of open-source databases revealed that Natanson resides at the Natanson Residence, 313 S. Royal Street, Alexandria, Virginia 22314-3715. As of January 10, 2026, FBI physical surveillance observed Natanson entering and exiting the Natanson Residence. A review of Virginia Department of Motor Vehicle records revealed that the Natanson Vehicle, a maroon 2013 Ford Fusion with Virginia license plate TRD 2309, is registered to Natanson at the Natanson Residence.

42. The classified and national defense information that may be found pursuant to the requested warrants includes information relating to Country 1. According to

and the Department of War, given (i) the recent U.S. military operations in Country 1, (ii) the ongoing activities and operations thereafter, and (iii)

, further disclosure and dissemination of the information that may be found on the subject premises risks causing exceptionally grave and irreparable harm to U.S. national security.

43. Moreover, even if the information is not disseminated by the individual with control over the Natanson Residence or Natanson Vehicle or Natanson herself, according to the U.S. Intelligence Community and the Department of Justice, such information is targeted by foreign adversaries and other criminals, who attempt to obtain such classified or other sensitive information through unauthorized accesses, including cyber intrusions. Such adversaries seek to obtain from all sources, especially sources that do not have the sorts of protections the United States uses to protect such information.

44. In light of the arrest of Perez-Lugones, the government anticipates disclosing in discovery specific information about his transmission of classified information to Natanson before the impending discovery deadline later this month. Therefore, the fact that classified information will likely be present on any devices (belonging to Natanson) to be found on Natanson's person or in the Natanson Residence or Natanson Vehicle may become public information. Moreover, if Natanson were to become aware of the government's investigation and gain knowledge of this matter, she may attempt to create additional copies or back-ups of the information or to share the information with other associates, which can further exacerbate the risk of foreign adversaries or other criminals obtaining the classified and national defense information.

FORENSIC ANAYLSIS OF ELECTRONIC COMMUNICATION DEVICES

45. Based on my training and experience, I know that electronic devices such as mobile phones and computers can store information for long periods of time. Similarly, things that have

been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

46. As further described in Attachment B, this application seeks permission to locate, not only electronically stored information that might serve as direct evidence of the crimes described on the warrant.

47. There is probable cause to believe that this forensic electronic evidence might be on the Natanson Electronics because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about when the data files were created and the sequence in which they were created.

48. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

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

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

51. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

UNLOCKING BIOMETRICALLY SECURED DEVICES

52. These warrants would also permit law enforcement to obtain from Natanson the display of physical biometric characteristics (*e.g.*, fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to the above-referenced warrants. I seek this authority based on the following:

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

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

55. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints.

56. 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.

57. 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 have a heightened concern about securing the contents of a device.

58. I also know from my training and experience, as well as from information found in publicly available materials, including those published by device manufacturers, that biometric features will not unlock a device in some circumstances, even if such features are enabled. These circumstances might, or might not, include: (1) when more than 48 hours has passed since the last time the device was unlocked, (2) when the device has not been unlocked for eight hours and the passcode or password has not been entered in the last six days, (3) when the device has just been restarted or powered on, (4) when attempts to unlock via fingerprint have failed a specified number of times, (5) when the device has received a remote lock command. Thus, in the event that law enforcement encounters a locked device, the opportunity to unlock the device via fingerprint may exist only for a short time.

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

60. Accordingly, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to the requested warrants and may be unlocked using one of the aforementioned biometric features, the requested warrants would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of the Subject to the fingerprint scanner of the device(s); or (2) hold the devices in front the Subject's face for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by the warrants.

CONCLUSION

61. Based on the foregoing information, I request that the Court issue the proposed warrants authorizing the search of the locations identified in Attachments A-1, A-2, and A-3) (i.e., Natanson Residence, Natanson Vehicle, and Natanson's person) for the purpose of seizing the items and records further described in Attachment B (i.e., records relating to the unlawful retention and transmission of classified information and records relating to Perez-Lugones).

<<

<<

<<

<<

<<

<<

Type text here

62. Since this investigation is continuing, disclosure of this affidavit will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order that this affidavit in support of application for search warrants be filed under seal.

FURTHER THIS AFFIANT SAYETH NOT.

Matthew Johnson
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to, in accordance with Fed. R. Crim. P. 4.1, by telephone on this 13th day of January 2026.

William B. Porter
United States Magistrate Judge

Criminal Complaint

U.S. v. Perez-Lugones

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Maryland

United States of America
v.
Aurelio Luis Perez-Lugones

Case No. 1:26-mj-00045-CJC

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 8, 2026 in the county of Howard County in the _____ District of Maryland, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §793(e)	Unlawful retention of national defense information

This criminal complaint is based on these facts:

See affidavit.

☑ Continued on the attached sheet.

Complainant's signature

SA Keith Starr, FBI
Printed name and title

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d).

Date: January 9, 2026

Judge's signature

City and state: Baltimore, Maryland

Chelsea J. Crawford, US Magistrate Judge
Printed name and title

PCM/TMS: USAO 2025R00683

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
	*	
v.	*	**CASE NO.** 1:26-mj-00045-CJC
	*	
AURELIO LUIS PEREZ-LUGONES,	*	
	*	
Defendant	*	
	*	
	*******	

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Keith Starr, being duly sworn, declare and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since 2021. I am currently assigned to the FBI Washington Field Office. I have spent most of my time as an FBI Special Agent working national security investigations, including the mishandling of classified information. I am assigned to the Counterintelligence Division at the FBI's Washington Field Office. I investigate, among other things, offenses involving the unauthorized disclosure of classified information to those not entitled to receive the same, including members of the media. I use a variety of techniques to conduct these investigations, including writing and executing search warrants, interviewing witnesses, victims, and subjects, and conducting 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 that, on or about January 8, 2026, in the District of Maryland and elsewhere, the Defendant, **AURELIO LUIS PEREZ-LUGONES ("PEREZ-LUGONES")**, committed the offense of unlawful retention of national defense information, in violation of 18 U.S.C. § 793(e).

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 AUTHORITY AND DEFINITIONS

4. Under 18 U.S.C. § 793(e), "[w]hoever 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 [commits a federal offense.]"

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 to access such classified national security information. For a foreign government to receive access to 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.

PROBABLE CAUSE

PEREZ-LUGONES' U.S. Government Employment and Access to Classified Information

8. **PEREZ-LUGONES** is a United States citizen born in Miami, Florida, and now lives in Laurel, Maryland. **PEREZ-LUGONES** was a member of the United States Navy from 1982 to 2002. From 1995 to 2002, as a member of the United States Navy, **PEREZ-LUGONES** held a Top Secret security clearance. **PEREZ-LUGONES** has been a Government contractor in various capacities since 2002.

9. Currently, **PEREZ-LUGONES** works as a systems engineer and information technology specialist for a Government contracting company whose primary customer is a Government agency. **PEREZ-LUGONES'** workplace is in Annapolis Junction, Maryland. **PEREZ-LUGONES'** workplace is owned and operated by another Government contracting company. **PEREZ-LUGONES'** role is administrative. **PEREZ-LUGONES** has access to classified systems so that he can maintain, support, and optimize various computer systems, networks, and software. **PEREZ-LUGONES** is a system administrator with heightened access to classified systems, networks, databases, and repositories as required for his job.

10. Due to his employment, **PEREZ-LUGONES'** possesses a Top Secret security clearance with access to SCI.

11. **PEREZ-LUGONES** has had access to SCI since at least 2000. As a security clearance holder, **PEREZ-LUGONES** has received instruction on the proper handling of classified information, including the proper storage of classified information. As part of his employment, **PEREZ-LUGONES** was also required to take regular, annual training that included refresher training on the proper marking and handling of classified information.

12. In September 2025, **PEREZ-LUGONES** took and passed a web-based training on handling classified information and a web-based training on the unauthorized disclosure of classified information.

13. Because **PEREZ-LUGONES** held a security clearance in the United States Navy and as a Government contractor, the Government entrusted **PEREZ-LUGONES** with access to classified information and national defense information so long as he needed to know that information to perform his job.

14. Absent a work-related reason to access those systems, **PEREZ-LUGONES** is not authorized to access classified systems, networks, databases, or repositories, nor is he permitted to view or print the classified information from classified systems.

PEREZ-LUGONES' Printing of Classified Materials

15. On several occasions since at least October 2025, while having authorized access to classified systems, **PEREZ-LUGONES** navigated to and searched databases or repositories containing classified information without authorization. There, **PEREZ-LUGONES** accessed and viewed classified intelligence reports or summaries of classified intelligence reports. Those reports or report summaries were produced, created, or maintained by several Government agencies.

16. On October 28, 2025, **PEREZ-LUGONES** used databases or repositories to search for, access, and view a classified intelligence report related to a foreign country ("Country 1"). That report was classified Top Secret. **PEREZ-LUGONES** took a screenshot of the report and pasted that screenshot in a Microsoft Word document titled "Microsoft Word – Document1."

17. Notably, **PEREZ-LUGONES'** screenshot of the report rendered one of the four bullet points at the end of the report illegible due to how the screenshot was cropped.

18. **PEREZ-LUGONES** also opened an attachment to that report, took screenshots of the attachment, and pasted those screenshots into the same Microsoft Word document.

19. Afterward, **PEREZ-LUGONES** printed the Microsoft Word document hours before logging off the system for the day. The illegible bullet point referenced above is also illegible in the printed version of the Microsoft Word document.

20. **PEREZ-LUGONES** had no need to know and was not authorized to search for, access, view, screenshot, or print any of this information.

21. **PEREZ-LUGONES** should be aware, based on his training and experience as a security clearance holder, that he cannot remove classified information from a SCIF without authorization, proper packaging, and a government-issued courier card.

22. **PEREZ-LUGONES** did not have authority to remove any classified or sensitive information. **PEREZ-LUGONES** did not receive specific requests to search for, access, view, screenshot, or print the classified or sensitive reports referenced above, nor did he have a need to conduct those searches.

23. **PEREZ-LUGONES'** job duties do not include accessing, viewing, printing, or manipulating classified information or defense information of any kind related to Country 1. **PEREZ-LUGONES'** job duties are limited to administrative tasks, which were described above.

24. Government security clearance holders are aware, often through mandatory in-person or web-based training, that Government classified systems are or can be monitored by the sponsoring agency, which can include monitoring printing activity.

25. An individual may try to avoid creating an obvious record of printing activity (*e.g.*, avoid printing a document with classification markings in the file name, which would reflect that the document being printed is classified) by taking screenshots of classified information and printing those screenshots or pasting those screenshots in a text document. This type of activity

would obfuscate the title of the printed document, making it seemingly innocuous, but it would not necessarily obfuscate the content of the printed document.

26. **PEREZ-LUGONES'** employer can retrieve records of print activity on classified systems, including copies of printed documents.

27. **PEREZ-LUGONES** printed on classified systems during the times described above.

28. **PEREZ-LUGONES'** employer retrieved copies of the documents **PEREZ-LUGONES** printed on October 28, 2025.

29. As described above, a review of **PEREZ-LUGONES'** printing activity on that dates showed that he had printed innocuous sounding documents (i.e., Microsoft Word – Document 1) that really contained classified and sensitive reports.

NOTETAKING

30. On January 5, 2026, **PEREZ-LUGONES** accessed and viewed a classified intelligence report related to Government operational activity. The report was classified up to Secret, and was maintained on databases or repositories.

31. On January 6, 2025, **PEREZ-LUGONES** left his residence for his workplace in his vehicle at about 8:00 a.m. He arrived at and entered the workplace at around 8:15 a.m. Shortly thereafter, **PEREZ-LUGONES** logged onto the classified system.

32. At around 4:00 p.m., **PEREZ-LUGONES** left the SCIF and then returned to the SCIF a short time later. At around 4:10 p.m., **PEREZ-LUGONES** picked up a yellow notepad, examined and removed approximately three pages, folded those pages in half, and set those pages on his desk. **PEREZ-LUGONES** then gathered his things, picked up the pages he had removed from the notepad, and left his desk area with the pages in hand. **PEREZ-LUGONES** left the

workplace at around 4:25 p.m., with a black bag. **PEREZ-LUGONES** was observed looking around the workplace parking garage before entering his vehicle and driving to his residence.

33. After leaving the workplace on January 6, 2026, **PEREZ-LUGONES** arrived at his residence at around 4:41 p.m. **PEREZ-LUGONES** did not leave his residence the rest of the night.

34. The following day, January 7, 2026, **PEREZ-LUGONES** left his residence for the workplace in his vehicle at around 8:00 a.m., arriving at around 8:11 a.m. Shortly thereafter, **PEREZ-LUGONES** logged on to the classified system.

35. At around 9:00 a.m., **PEREZ-LUGONES** took notes on a yellow notepad. Throughout the morning, **PEREZ-LUGONES** looked back and forth between the screen corresponding the classified system and the notepad, all the while writing on the notepad.

36. At around 10:52 a.m., on January 7, 2026, **PEREZ-LUGONES** left his desk with a yellow notepad page, leaving the workplace, getting into his vehicle, and driving to his residence.

A Search of PEREZ-LUGONES' Car and Residence Revealed Documents Marked as Classified

37. On January 8, 2026, a federal court issued search warrants authorizing the search of **PEREZ-LUGONES**'s residence in Laurel, Maryland, as well as his vehicle, and other locations. The searches were conducted the same day.

38. While searching the authorized areas listed above, investigators located multiple documents that were marked as SECRET.

39. While searching **PEREZ-LUGONES**'s car, investigators located a lunch box in which a document was marked as SECRET. Prior video surveillance observed **PEREZ-LUGONES** at his cubicle in the SCIF at his workplace looking at this same document on January 8, 2026. Additional prior investigation of **PEREZ-LUGONES** in the SCIF at his workplace also identified him removing the classification header/footer markings from this document prior to leaving his workplace. The document identified in the lunch box by investigators during the authorized search of **PEREZ-LUGONES**'s car was the same classified document without the classification header/footer markings that **PEREZ-LUGONES** was seen handling in the SCIF at his workplace.

40. While searching **PEREZ-LUGONES**'s residence, investigators located a document in the basement of the residence marked as SECRET.

41. One or more of these documents are related to national defense.

CONCLUSION

42. I submit that this affidavit establishes probable cause in support of a criminal complaint charging **PEREZ-LUGONES** with the unlawful retention of national defense

information, in violation of 18 U.S.C. § 793(e), and thus respectfully request that the Court issue a complaint charging **PEREZ-LUGONES** with that offense.

Respectfully submitted,

Keith Starr
Special Agent
Federal Bureau of Investigation

Affidavit submitted by e-mail and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 9th day of January, 2026.

HONORABLE CHELSEA J. CRAWFORD
UNITED STATES MAGISTRATE JUDGE