

Exhibit 1

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA**

IN THE MATTER OF THE SEARCH OF
THE REAL PROPERTY AND PREMISES
OF HANNAH NATANSON

)
)
)
)
)

No. 1:26-sw-54

**DECLARATION OF FEDERAL BUREAU OF INVESTIGATION
ASSISTANT DIRECTOR ROMAN ROZHAVSKY**

I, Roman Rozhavsky, on this 30th day of January 2026, declare and state:

1. I am over the age of 18 years old, sound of mind and otherwise competent to make this Declaration.

2. I am the Assistant Director of the Counterintelligence and Espionage Division, Federal Bureau of Investigation ("FBI"), United States Department of Justice ("DOJ"), a component of an Executive Department of the United States Government. I am responsible for, among other things, directing the conduct of FBI counterintelligence and espionage investigations. As the Assistant Director of the Counterintelligence and Espionage Division, I have official supervision and control over the files and records of the Counterintelligence and Espionage Division, FBI, Washington, DC. This Declaration is submitted in support of the Government's Opposition to the Motion to Intervene and for Return of Property.

3. The matters stated herein are based on my personal knowledge, my review and consideration of documents and information available to me in my official capacity, and information furnished by Special Agents ("SA") and other employees of the FBI and the Department of Justice. My conclusions have been reached in accordance therewith.

4. In my capacity as the Assistant Director of the FBI's Counterintelligence and Espionage Division, I have been delegated original classification authority by the Attorney

General of the United States. See Executive Order 13526, Section 1.3(c). As a result, and pursuant to all applicable Executive Orders, I am responsible for the protection of classified information within the FBI, including counterintelligence and espionage information relating to the sources, methods, and techniques used by the FBI in the collection of that information. Thus, I have been authorized, pursuant to the responsibilities and obligations defined in Executive Orders and through the delegation from the Attorney General, to execute declarations and other affidavits to protect such classified information.

I. Genesis of Investigation

5. In November 2025, the FBI opened an investigation to identify and stop the unlawful dissemination of classified and national defense information which had been published in an article in the Washington Post on October 31, 2025.

II. Identification of Perez-Lugones

6. Through the course of the investigation, Aurelio Perez-Lugones was identified as having accessed and printed the classified information which was published on October 31, 2025. Additionally, he was identified as accessing and printing more classified information which was subsequently published in other Washington Post articles. Hannah Natanson was the only reporter who authored, co-authored, or contributed to all of the relevant published articles.

III. Investigation of Perez-Lugones

7. Aurelio Luis Perez-Lugones resides in Howard County, Maryland, and has held a TOP SECRET security clearance since at least 1995. From 1982 to 2002, Perez-Lugones served in the U.S. Navy. Since that time, more than two decades, Perez-Lugones has worked as a government contractor.

8. Perez-Lugones worked as a systems engineer and information technology specialist

for a government contractor. To perform his duties as a systems administrator, Perez-Lugones had access to classified systems and networks and worked inside a sensitive compartmented information facility (“SCIF”).

9. As a security clearance holder, Perez-Lugones received instruction and training on the proper handling of classified information, including the proper storage of classified material. As part of his employment, Perez-Lugones was required to complete regular, annual training relating to the proper marking and handling of classified information. As recently as September 2025, Perez-Lugones completed web-based training on the proper handling of classified information and the unauthorized disclosure of classified information.

10. Between in or around at least October 2025 and January 2026, Perez-Lugones repeatedly accessed classified reports, printed or otherwise copied the information in these classified reports, removed the printouts and information from the SCIF, then transmitted this classified national defense information to Natanson.

11. On or around October 28, 2025, Perez-Lugones searched for, accessed, and viewed a TOP SECRET//SCI//NOFORN classified intelligence report relating to a foreign country (“Country 1”). Perez-Lugones took a screenshot of the intelligence report and pasted the screenshot into a Microsoft Word document (hereinafter “Classified Document A”). One of the screenshots taken by Perez-Lugones rendered a portion of the intelligence report unreadable due to how the screenshot was cropped. Perez-Lugones also opened an attachment to the intelligence report, took screenshots of that attachment, and pasted those screenshots into Classified Document A. Shortly thereafter, Perez-Lugones printed Classified Document A.

12. On or around October 31, 2025—three days after Perez-Lugones accessed and took screenshots of the intelligence report—Natanson co-authored an article that contained much

of the classified information that was set forth in Classified Document A. The article omitted the information contained in the portion of the intelligence report that had been rendered unreadable in the screenshots taken by Perez-Lugones.

13. On or around November 5, 2025, Perez-Lugones accessed classified summaries of intelligence reports related to Country 1. Some of these summaries were classified as SECRET//NOFORN. Perez-Lugones took a screenshot of these summaries and pasted the screenshot into a Microsoft Word document (hereinafter "Classified Document B"). Perez-Lugones subsequently took additional screenshots, including information relating to Country 1, and pasted these screenshots into Classified Document B. Later the same day, Perez-Lugones printed Classified Document B. On or around November 11, 2025, Natanson co-authored an article that contained portions of the classified information contained in Classified Document B.

14. On or around December 4, 2025, Perez-Lugones accessed a different intelligence report related to Country 1. This report was classified as CONFIDENTIAL//NOFORN. Perez-Lugones took a screenshot of the report and pasted the screenshot into a blank Microsoft Word document (hereinafter "Classified Document C"). Shortly thereafter, Perez-Lugones printed Classified Document C and departed the SCIF.

15. On or around December 8, 2025, Natanson co-authored an article that contained portions of the classified information set forth in Classified Document C.

16. On or around January 5, 2026, Perez-Lugones accessed another intelligence report related to Country 1. This report was classified at the SECRET level. The following day, Perez-Lugones took handwritten notes in a yellow notepad while viewing classified intelligence reports on his work computer. Subsequently, Perez-Lugones removed approximately three pages from the yellow notepad, folded the pages in half, and, several hours later, removed them from the SCIF.

17. On or around January 6, 2026, Natanson contributed to a published article that contained classified information that appeared in the same intelligence report that Perez-Lugones viewed on January 5, 2026.

18. Two days later, on or around January 8, 2026, Perez-Lugones accessed a classified report relating to Country 1. This report was classified as SECRET//NOFORN. Perez-Lugones copied information from the report, pasted it into another application, and printed it out (hereinafter "Classified Document D"). Perez-Lugones cut off header information from Classified Document D, thereby removing his name from the document. Additionally, also on January 8, 2026, Perez-Lugones copied and printed information from another report classified as SECRET//REL TO USA, NATO (hereinafter "Classified Document E").

IV. Perez-Lugones is Arrested, and Search Warrants Executed on His House, Car, and Person

19. Perez-Lugones was arrested on January 8, 2026. Prior to his arrest, 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. The FBI reviewed messages between Perez-Lugones and Natanson sent via Signal, an encrypted messaging application, on or around January 7 and 8, 2026. The messages discussed the classification level of certain documents, set forth details about which U.S. government agencies had produced different reports, and explained how certain documents would be referenced in forthcoming news articles. As part of these messages, Perez-Lugones also sent audio messages to Natanson where he provided additional details about the information that he had transmitted.

20. The search also revealed that Perez-Lugones had transmitted photographs of classified documents to Natanson, including Classified Document D and Classified Document E,

on or around January 8, 2026. After transmitting one such document, Perez-Lugones wrote, "I'm going quiet for a bit . . . just to see if anyone starts asking questions."

21. Around this same time, a court-authorized search revealed a hard copy printout of Classified Document D with the header information removed in Perez-Lugones's lunchbox. The removed header information was later located at Perez-Lugones's workplace, in a trash basket.

22. On or around January 9, 2026, Natanson co-authored an article that contained classified information set forth in Classified Document D.

V. Arrest/Search and Indictment of Perez-Lugones

23. On January 8, 2026, the FBI arrested Perez-Lugones and executed search warrants for Perez-Lugones's person, mobile phone, residence, and vehicle. On January 9, 2026, Perez-Lugones was charged with the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e). On January 15, 2026, Perez-Lugones consented to detention. On January 22, 2026, a federal grand jury in the District of Maryland indicted Perez-Lugones on five counts of unlawfully transmitting, and one count of unlawfully retaining, national defense information, in violation of 18 U.S.C. § 793(e).

VI. Searches of Natanson's Person, Residence and Vehicle (All Items Seized Were from Her Residence)

24. On January 14, 2026, the FBI executed search warrants on Hannah Natanson's person, on Natanson's residence, and on Natanson's vehicle.

25. Prior to the execution of the search warrant, Agents rang the doorbell and identified themselves as FBI Agents while presenting their FBI-issued credentials and stated they were there to execute a residential search warrant. During the execution of the search warrants, Agents asked Natanson what electronics she had in the residence. Natanson stated that the only devices she had in the residence were a laptop and a cell phone located upstairs. Natanson asked the FBI whether

she was required by the warrant to provide her passcode to her devices. FBI advised Natanson that the FBI could not compel her to provide her passcodes, but she could consent to provide them. Natanson said she would not provide the FBI with such consent. It was further explained that although she was not compelled to provide her passcodes, the warrant did give the FBI authority to use Natanson's biometrics, such as facial recognition or fingerprints, to open her devices. Natanson stated that she did not use biometrics on her devices.

26. Natanson's laptop, a silver MacBook Pro with a black case, and Natanson's cell phone, an Apple iPhone 13, were both found upstairs in Natanson's office, along with a Handy branded audio recording device and a Seagate portable hard drive.

27. The iPhone was found powered on, sitting on a charging stand with a cable, and a notification visible on its display indicated the iPhone was in "Lockdown" mode. The MacBook Pro in a black case was found powered off and not plugged into any power source. The Handy recorder and Seagate portable hard drive were similarly found powered off and not plugged into any power source or other device.

28. As Natanson was preparing to take a walk outside, Natanson asked whether she could take her Garmin watch and pointed towards the dining room. Natanson was advised that she could not take it because it is an electronic device covered by the search warrant. Natanson said she liked to count her steps, and Natanson was further advised she could not take her watch. The Garmin Forerunner watch was found powered on resting on a charging dock on a side table in the dining room.

29. Another silver MacBook Pro without a case was found powered on inside a red backpack in the kitchen. Opening the laptop displayed an instruction to "Touch ID or Enter Password" to unlock the laptop.

30. As the FBI was concluding its searches, the FBI attempted to contact Natanson through her fiancé's cell phone number, but it went straight to voicemail. A few minutes later, the fiancé's number was called again and Natanson answered. Natanson was advised that the FBI was close to completing the searches and would leave a receipt listing the property that had been seized by the FBI. Natanson was asked whether she would be returning to the residence. Natanson said she would not be returning.

31. FBI Agents then departed the residence and returned to their vehicles located in a nearby parking lot. Agents waited until they observed Natanson returning to her residence and followed her back to her front door. When Agents approached, Natanson was outside of her front door while on a cellphone. The FBI presented Natanson with her open laptop which had been found in the red backpack located in the kitchen. Natanson was reminded the FBI has authority to use her biometrics to unlock the laptop and Natanson repeated that she does not use biometrics on her devices.

32. Natanson was told she must try, in accordance with the authorization in the warrant. The FBI assisted Natanson with applying her right index finger to the fingerprint reader which immediately unlocked the laptop. As the FBI left the front of her residence, Natanson asked, "what laptop is that?"

VII. Law Enforcement Preservation of Evidence

33. At the conclusion of the execution of the search warrants, evidence items were transported to FBI's WFO and were checked into evidence. The following items were seized pursuant to the warrant and subsequently brought to the FBI's Computer Analysis Response Team ("CART") for processing:

1. iPhone 13 (found powered on and in Lockdown Mode);

2. Work MacBook Pro (found powered on and locked; biometrically unlocked with Natanson's fingerprint on 1/14/2026);
3. Personal MacBook Pro (found powered off during search);
4. Handy Recorder;
5. 1TB Seagate Portable Drive; and
6. Garmin Forerunner Watch.

34. On the afternoon of January 14, 2026, DOJ informed the FBI that items seized during the execution of the Natanson warrants were required to undergo a scoping process (to comply with Attachment B of the search warrant) and a filter review (to protect against disclosure of attorney-client protected materials). This review would be guided by a Scoping/Filter Protocol authored by the Department of Justice. The processing of all electronic devices seized from Natanson's home was conducted by CART and filter Special Agents who are not part of the case team and are therefore not responsible for the Perez-Lugones investigation.

35. Because the iPhone 13 was in Lockdown Mode, there was no extraction of the device at that time. FBI has paused any further efforts to extract this device because of the Court's Standstill Order. The SIM card was extracted with an auto-generated HTML report created by the tool utilized by CART. As a matter of standard practice, and prior to the standstill order, the HTML report of this SIM was reviewed by CART and the data contained in the HTML was limited to the telephone number.

36. Natanson's personal MacBook Pro is password protected and encrypted and therefore no imaging was effected. The FBI paused any further efforts because of Court's Standstill Order. No review has occurred.

37. Data from the Handy recorder (including its SD card) and the 1TB Seagate Portable drive were processed. No review has occurred. Natanson's Garmin Forerunner was not processed

prior to the issuance of the Standstill Order and, therefore, no processing will occur until further order of the Court.

38. Upon initial CART preservation efforts of the Work MacBook Pro, it was identified Natanson's user profile lacked administrative privileges. Therefore, a full physical image was unavailable. A limited partial live logical image was processed but was not reviewed due to the court order.

39. Due to the possible classification of materials on the Work MacBook Pro, upon forensic processing by CART, the Work MacBook Pro was placed inside an FBI SCIF for storage and further preservation.

40. Signal is a messaging application that, in addition to end-to-end encryption, allows users to add a custom timeframe in which messages "disappear" or "delete." This feature can be enabled or disabled at any time through a conversation stream with a specific user, and users can at any time change the frequency to which messages in a specific conversation thread are deleted. Filter Special Agents noted that several of Natanson's Signal chat messages were, in fact, set for auto-deletion, with different timeframes depending on the conversation.

41. Hence, that same day, filter Special Agents began taking photographs and, where necessary, audio/video recording of the contents of the various conversations within Signal application on the Work MacBook Pro, for preservation purposes only. No substantive review of these messages has occurred. The filter Special Agents preserving the Signal conversations in this manner have been walled off from the case team.

42. This manual process of photographing and/or videotaping portions of the Signal chats was necessary in part because CART was unable to forensically place the data from Signal into a human readable format.

43. Due to the above, and at the direction of DOJ to preserve the messages by photographing them, photographs of the Work MacBook Pro were taken using a Nikon D780 camera and were stored on Secure Digital (SD) Memory Cards. Each SD Memory Card was “wiped” clean of data before use.

44. Each SD Memory Card was also formatted before any data was stored. The Work MacBook Pro was placed into airplane mode and the WiFi disabled. The device remained in this state for the entirety of the process described below.

45. Signal appeared to log chat conversations “newest to oldest” and logged conversations in the order in which a last message, attachment, notification, conversation setting change, etc. was sent or received by the account owner. Agents therefore began preserving the Signal messages by working in a reverse chronological order. Agents took photographs of the entire content of all Signal messages for only those conversations in which the display date of the last message, attachment, notification, conversation setting change, etc. was on or after October 1, 2025. During this step, Special Agents only took pictures of the chat contents, and did not initially attempt to download, open, or otherwise expand, any attachment or message within the chat conversations. Hence, this process preserved the entirety of all Signal conversations, in which there was a new message or alert on or after October 1, regardless of the date of the message, notification, or attachment.

46. Once this process was complete, Agents repeated the same for four “pinned” conversations, which all had at least one of the above listed characteristics (such as a message or notification) that fell on or after October 1, 2025.

47. Once the conversations were photographed in their entirety, as they appeared on screen, Agents then attempted to manually click on and open every attachment and file contained


within each one of the above-described conversations. This attempt was made regardless of file type and of the currently downloaded state of an attachment. If an attachment was able to be viewed, a photograph of that file in its location was taken, as was a photograph of the item itself. Each photograph taken of the Work MacBook Pro was memorialized in a photographic log.

48. Of note, at least one conversation thread contained various recorded audio files. These audio files were preserved by using the video recording function of the Nikon D780 camera, which captures both audio and video. Where this process was utilized, it was also memorialized on the FBI FD-674 (a photographic evidence log sheet used to document crime scene or investigation photos). Additionally, at least some files within conversations could only be viewed by downloading the file to the evidence item itself. In these cases, the item was downloaded from within the Signal application by the Agent, saved directly to the Work MacBook Pro, and opened for viewing. This process was, when utilized, captured using the video recording function of the Nikon D780 camera and memorialized in the FBI FD-674. Once opened, the item was then preserved by the Nikon D780 camera. After preservation of the downloaded file was complete, the downloaded file was left stored on the Work MacBook Pro and not deleted by the Agent.

49. This entire process utilized five separate SD memory cards of various storage sizes. The data from those memory cards was transferred to a staging drive for storage. Each time the files were transferred from one storage device to another, Agents verified the hash values of the files to ensure that no corruption or degradation of the data had occurred. The verified hash values were also stored on the staging media and included in the transferred data.

50. On January 21, 2026, this Court granted a motion for a Standstill Order. ECF 18. No further preservation efforts were pursued following the granting of the Standstill Order.

51. The facts and information contained in this Declaration are true and correct according to the best of my knowledge, information, and belief.


FBI Assistant Director Roman Rozhavsky