UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In the Matter of the Search of the Real Property and Premises of Hannah Natanson	No. 1:26-sw-00054-AJT-WBP

UNITED STATES' SUPPLEMENTAL BRIEF
IN RESPONSE TO COURT'S PROPOSED REVIEW PROTOCOL

The United States of America, by counsel, hereby provides the supplemental brief ordered by Magistrate Judge Porter consistent with the Court's discussion with counsel at the status conference on March 4, 2026. *See* ECF No. 72. The government provides the following responses to the questions posed by the Court. It preserves for appeal all objections previously noted in its papers filed with the Magistrate Judge, at the status conference, and in its Objections to Magistrate Judge's Memorandum Opinion and Order on the Motion for Return of Property filed with the district court on March 10, 2026 (ECF No. 74).

I. RESPONSES TO QUESTIONS RELATED TO PREPARATION FOR REVIEW[1]

1. **What has been the chain of custody with respect to each of Ms. Natanson's devices that were seized by the government? Provide a summary of what extraction or imaging has been done with respect to each device, and by whom, and whether any information extracted or imaged from each device was reviewed or examined, and by whom, prior to the Standstill Order. Also verify that any information that has been extracted or imaged from any device will not be further reviewed or examined by anyone other than the Court in accordance with the Standstill Order. (Tr. 32:9-33:19.)**

The government verifies that no extraction, imaging, processing, or review of any of Ms. Natanson's devices seized by the government has taken place since the Court issued its Standstill

[1] These responses were prepared with the assistance of technical experts at FBI.

Order on January 21, 2026, and that the government will continue to abide by the Standstill Order.

Prior to the Standstill Order, the government took actions to extract, image, preserve, and process information from the devices. The chain of custody and history of those actions with respect to each device prior to the Standstill Order are detailed below.

(1) Personal Phone and Associated SIM Card

Federal Bureau of Investigation ("FBI") Special Agents investigating Aurelio Luis Perez-Lugones (the "Investigative Team") searched Ms. Hannah Natanson's person, residence, and vehicle on January 14, 2026, pursuant to a search warrant issued by this Court. *See* Decl. of FBI Asst. Dir. Roman Rozhavsky, filed Jan. 30, 2026 (ECF No. 35-1) ("Rozhavsky Decl.") ¶ 24. During the search, an Apple iPhone 13 ("Personal Phone") and its associated Subscriber Identity Module ("SIM") card was found upstairs in Ms. Natanson's office sitting on a charging stand with a cable. *Id.* ¶¶ 26-27. The phone was found powered on with a notification visible on its display indicating that it was in "Lockdown Mode."[2] *Id.* ¶ 27. The Investigative Team seized the Personal Phone and the associated SIM card.[3]

At the conclusion of the execution of the search warrants on January 14, 2026, the Investigative Team transported the Personal Phone and the SIM card to FBI's Northern Virginia Residence Agency (the "NVRA") in Manassas, Virginia,[4] where the items were checked in with

[2] Apple's support website explains that when an iPhone has "Lockdown Mode" enabled, "certain apps, websites, and features are strictly limited for security and some experiences might not be available at all." "About Lockdown Mode," https://support.apple.com/en-us/105120 (last visited Mar. 25, 2026).

[3] On February 25, 2026, attorneys for Ms. Natanson requested that the FBI return to Ms. Natanson the charging stand and cable that the FBI had seized along with the Personal Phone. The FBI is in communication with Ms. Natanson's attorneys and is in the process of returning these items.

[4] The NVRA is a subordinate component of the FBI's Washington Field Office, which is based in Washington, DC.

NVRA evidence control and transferred to the custody of FBI's Computer Analysis Response Team ("CART"), which has a forensic laboratory within the NVRA (the "CART Lab"). *Id.* ¶ 33.

CART attempted but was unable to extract or preserve any information from the Personal Phone because it was in "Lockdown Mode." *Id.* ¶ 33. CART has explained that FBI does not currently have the ability to access the Personal Phone and is currently unable to take the phone out of "Lockdown" mode without Ms. Natanson's access PIN number.

On January 14, 2026, CART extracted information from the SIM card using a tool that auto-generates a Hypertext Markup Language ("HTML") report that shows only the telephone number associated with the SIM card that was used with the Personal Phone. *Id.* ¶¶ 34-35. CART analysts reviewed this limited information (i.e., the telephone number shown on the HTML report). *Id.* ¶ 35.

After the above-described extraction and preservation actions were taken, CART moved the Personal Phone, which was presumed to contain classified information, into the Sensitive Compartmentalized Information Facility ("SCIF") located in the CART Lab in Manassas ("CART SCIF"). It remains in that location as of this date.

(2) Personal Computer

During the search of Ms. Natanson's residence on January 14, 2026, a silver MacBook Pro laptop computer ("Personal Computer") was found inside a black case upstairs in Ms. Natanson's office. *Id.* ¶¶ 26-27. The Personal Computer was found powered off and not plugged into any power source. *Id.* ¶ 27. The Investigative Team seized the Personal Computer.

At the conclusion of the execution of the search warrants on January 14, 2026, the Investigative Team transported the Personal Computer to the NVRA, where the item was checked in with NVRA evidence control and transferred to the custody of CART. *Id.* ¶ 33.

CART moved the Personal Computer, which was presumed to contain classified information, into the CART SCIF. It remains in that location as of this date.

Within the CART SCIF, CART attempted but was unable to image or preserve any information from the Personal Computer because it is password-protected. *Id.* ¶ 36. CART has explained that FBI does not currently have the ability to access the Personal Computer and is currently unable to image information from the computer without Ms. Natanson's password.

(3) Work Computer

During the search of Ms. Natanson's residence on January 14, 2026, another silver MacBook Pro laptop computer ("Work Computer") was found inside a red backpack in Ms. Natanson's kitchen. *Id.* ¶ 29. The computer was found powered on. *Id.* The Investigative Team seized the Work Computer.

Later that same day, the Investigative Team opened the laptop Work Computer and observed that the screen displayed an instruction to "Touch ID or Enter Password" to unlock the computer. *Id.* The Investigative Team presented Ms. Natanson with her open laptop Work Computer and reminded her that, in accordance with the authorization in the warrant, she must try to use her biometrics to unlock the laptop. *Id.* ¶¶ 31-32. The FBI assisted Ms. Natanson with applying her right index finger to the fingerprint reader, which immediately unlocked the laptop. *Id.* ¶ 32.

At the conclusion of the execution of the search warrants on January 14, 2026, the Investigative Team transported the Work Computer to the NVRA, where the item was checked in with NVRA evidence control and transferred to the custody of CART. *Id.* ¶ 33.

On January 14, 2026, CART identified that Ms. Natanson's user profile on the computer (which FBI could access after Ms. Natanson's fingerprint unlocked the computer) was logged in as a standard user without administrative privileges. As a result, CART was unable to fully image

information from the computer but was able to obtain a partial image of what was available to a standard user. *Id.* ¶ 38. This partial image included files native to the device—e.g., calendaring information, contact information, documents, downloads, browsing history, e-mail messages, and other messages native to Apple MacOS devices—but did not include information that was not native to the device—e.g., messages from third-party applications, like Signal, that are end-to-end encrypted where the decryption key is available only on the administrative side.

CART then processed the limited image of the Work Computer by running the image through the Axiom processing and review platform ("Axiom") (described in more detail below). As a part of this processing, CART used Axiom to break down any video file that had been imaged as part of the partial image into a set of separate frames to provide for a snapshot of the content of the videos during the review. CART also used Axiom to run Optical Character Recognition ("OCR") on imaged information that is OCR-readable.

CART then created a portable case within Axiom for the partial image from the Work Computer.[5] When creating the portable case, CART used Axiom to apply a date-range limiter to the data such that the portable case would include only files with time stamp metadata dated on or after October 1, 2025.[6]

[5] An Axiom "portable case" is a feature of Axiom that allows forensic examiners to export a subset of digital evidence into a free, self-contained, and lightweight viewer. It enables non-technical stakeholders—such as attorneys and investigators—to review, search, tag, and comment on evidence without needing a full Axiom license or software.

[6] The date-range limiting function available in Axiom analyzes any metadata associated with the files being processed that include a date stamp of any kind (e.g., creation date, sent date, etc.). When applying the date-range limiter, Axiom includes in the resulting set any file that has at least one metadata date stamp that falls within the date range specified. When applying the date-range limiter function to data in this matter, CART opted to treat files that had no time stamp metadata as falling within the specified date range and included those files in the resulting set.

After the above-described imaging and preservation actions were taken, CART moved the Work Computer, which was presumed to contain classified information, into the CART SCIF. *Id.* ¶ 39. It remains in that location as of this date.

In addition to and separate from the limited imaging described above, on January 14, 2026, after the Work Computer was moved inside the CART SCIF, FBI Special Agents who are not part of the Perez-Lugones Investigative Team (and are therefore not responsible for the Perez-Lugones investigation) (the "Filter Team") performed additional preservation actions on the contents of the Work Laptop stored in the CART SCIF due to the fact that CART was only able to partially image the computer and the image did not include the Signal chat messages that were known to be accessible on the device.[7] To preserve the chat messages found in the Signal application before any messages could auto-delete,[8] the Filter Team took photographs of Signal chat message conversations and video/audio-recorded audio files and attachments embedded within Signal chat conversations if any such conversations included one or more messages exchanged on or after October 1, 2025. *Id.* ¶¶ 41, 43-49. The Filter Team's manual process of photographing and/or recording the Signal chat message conversations on the Work Computer was necessary to preserve the information because, as noted above, CART was unable to image this data due to Ms. Natanson's user profile lacking administrative privileges and the data was potentially subject to auto-deletion. *Id.* ¶ 42. These manual preservation efforts resulted in the creation of thousands of

[7] One Special Agent who participated in these additional preservation efforts had previously assisted with the search of the Perez-Lugones office on January 8, 2026, but was not part of the Perez-Lugones Investigative Team and has had no substantive contact with the Investigation Team since the search of the Perez-Lugones residence.

[8] 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. Rozhavsky Decl. ¶ 40.

files, including photographs and video files, containing information preserved from the Signal application on the Work Computer, which the Filter Team transferred to the custody of CART. CART has not yet conducted any processing of these files, which have remained in CART's custody in the CART SCIF since January 14, 2026.

Neither the Filter Team nor any other government personnel conducted any substantive review of the Signal chat messages or any other information that had been imaged from the Work Computer. *Id.* ¶ 41.

(4) Audio Recorder and Associated SD Card

During the search of Ms. Natanson's residence on January 14, 2026, a "Handy" brand audio recording device ("Audio Recorder") and its associated Secure Digital ("SD") card was found upstairs in Ms. Natanson's office. *Id.* ¶¶ 26-27, 37. The Audio Recorder was found powered off and not plugged into any power source or other device. *Id.* ¶ 27. The Investigative Team seized the Audio Recorder and the associated SD card.

At the conclusion of the execution of the search warrants on January 14, 2026, the Investigative Team transported the Audio Recorder and Associated SD Card to the NVRA, where the items were checked in with NVRA evidence control and transferred to the custody of CART. *Id.* ¶ 33.

CART moved the Audio Recorder and SD card, which were presumed to contain classified information, into the CART SCIF. It remains in that location as of this date.

On or about January 17, 2026, CART preserved the information contained within the Audio Recorder and its associated SD card by imaging the SD card (the recorder itself did not contain data). *Id.* ¶ 37. This information included multiple audio files.[9]

CART then created a portable case within Axiom for the information imaged from the SD card. When creating the portable case, CART used Axiom to apply a date-range limiter to the data such that the portable case would include only files with time stamp metadata dated on or after October 1, 2025.

(5) Portable Hard Drive

During the search of Ms. Natanson's residence on January 14, 2026, a "Seagate" brand portable hard drive with a one-terabyte storage capacity ("Portable Hard Drive") was found upstairs in Ms. Natanson's office. *Id.* ¶¶ 26-27. The Portable Hard Drive was found powered off and not plugged into any power source or other device. *Id.* ¶ 27. The Investigative Team seized the Portable Hard Drive.

At the conclusion of the execution of the search warrants on January 14, 2026, the Investigative Team transported the Portable Hard Drive to the NVRA, where the item was checked in with NVRA evidence control and transferred to the custody of CART. *Id.* ¶ 33.

CART moved the Portable Hard Drive, which was presumed to contain classified information, into the CART SCIF. It remains in that location as of this date.

From within the CART SCIF, on or about January 16, 2026, CART preserved the information contained within the Portable Hard Drive by imaging the data in the device. *Id.* ¶ 37. This information included multiple, among other things, documents, photographs, and video files.

[9] CART will be able to more precisely quantify this and other imaged and extracted data after the Standstill Order is lifted or modified.

CART then began to process the information imaged from the Portable Hard Drive by running the image through Axiom. As a part of this processing, CART used Axiom to run OCR on a limited set of imaged files. CART was unable to complete the OCR process and other processing steps for all of the information on the Portable Hard Drive before the Standstill Order was issued.

(6) Running Watch

During the search of Ms. Natanson's residence on January 14, 2026, a "Garmin Forerunner" brand running watch ("Running Watch") was found in Ms. Natanson's dining room. *Id.* ¶ 28. The Running Watch was found powered on resting on a charging dock. *Id.* The Investigative Team seized the Running Watch and charging dock.[10]

At the conclusion of the execution of the search warrants on January 14, 2026, the Investigative Team transported the Running Watch to the NVRA, where the item was checked in with NVRA evidence control and transferred to the custody of CART. *Id.* ¶ 33.

CART moved the Running Watch, which was presumed to contain classified information, into the CART SCIF. It remains in that location as of this date.

CART had not yet imaged any information from the Running Watch before the Standstill Order was issued by the Court. *Id.* ¶ 37.

[10] On February 25, 2026, attorneys for Ms. Natanson requested that the FBI return to Ms. Natanson the Running Watch and the charging dock and cords that the FBI had seized. The government has not yet returned the Running Watch pending further analysis of the device. The FBI is in communication with Ms. Natanson's attorneys and is in the process of returning the charging dock and cords. FBI has advised that it is possible that the Running Watch potentially could store information responsive to the search warrant in addition to geolocation information that is standard for a running watch of its kind. If the Court lifts or modifies the Standstill Order and CART confirms that the Running Watch does not store information other than geolocation information, FBI will return the device to Ms. Natanson's attorneys per their request.

2. What more needs to be done to finish extracting or imaging information from the devices and process the information to prepare for Magistrate Judge Porter's review, and how long will that take? (Tr. 29:18-30:21, 41:6-10.)

Should the Court lift or modify the Standstill Order, CART could soon thereafter complete extraction and imaging information currently available on the devices and begin processing the devices to prepare the information for review. CART currently anticipates that, at such time, the following actions, in the following order consecutively, would need to take place before the Court could begin review:

(1) Image Information from the Running Watch

CART anticipates preserving information from the Running Watch by imaging any data that may be stored in the device or otherwise extracting a report that contains any information stored on the device. CART will then create a portable case for any information imaged or extracted from the Running Watch. CART anticipates that this will take approximately 1-2 days.

(2) Use Axiom to Process Videos of Signal Information

After all remaining imaging and extraction is complete, CART will complete processing. In order to process the video files taken of the audio files and attachments found within Signal chat message conversations, CART needs to put these files into containers that CART can forensically verify (i.e., authenticate, validate, and preserve to ensure it is reliable, unaltered, and admissible in legal proceedings). Then, CART needs to process the files through Axiom, which breaks down each video file into a set of separate frames to provide for a snapshot of the content of the videos during the review. CART will then create portable cases for the information. CART anticipates that this will take approximately 1-2 days.

(3) Use Axiom to Run OCR on Photos and Frames of Signal Information

After the above actions are complete, CART needs to use Axiom to run OCR on any remaining imaged or extracted information that is OCR-readable and appropriate for OCR[11] and has not yet had OCR run on it. This is estimated to be the most time-consuming part of processing the information in preparation for this review because of the expected large quantity of files that will require OCR, namely, the thousands of photographs of Signal chat messages from the Work Computer that are described above.

CART currently anticipates that OCR will need to be run on the following sets of information:

a. thousands of photographs and frames from videos taken of the Signal chat messages from the Work Computer; and

b. a majority of the files from the image taken from the Portable Hard Drive (OCR was previously run on only a subset of information).

Due to the quantity of data that requires OCR, especially the thousands of photographs of Signal chat messages, CART estimates that it will take 3-5 weeks to complete OCR.

(4) Finalize Portable Cases

Once all the above steps are complete, CART will need to create portable case files within Axiom for any information for which a portable case file has not already been created, which will

[11] CART has identified some information that will not require OCR processing, including (a) information extracted from the HTML report generated from the SIM card associated with the Personal Phone, (b) any audio files extracted from the Audio Recorder, (c) any audio files extracted from the Portable Hard Drive, and (d) information extracted from the Running Watch (assuming that the Running Watch does not contain information that can have OCR run on it). This information can be made available for manual review through Axiom.

include applying the date-range limiter described above to limit the data for the review to include only data with a date stamp on or after October 1, 2026.

(5) Set Up Hardware for Court Review (if not at CART SCIF)

As discussed at the status conference, and discussed further below, the government urges the Court to conduct its review at the CART SCIF in Manassas where CART currently has custody of the devices. Among other reasons, this would enable CART analysts with expertise in forensics and the Axiom review platform to aid the Court during its review.

Should the Court decide to review the information elsewhere, CART would need to take additional steps to prepare the information for review. CART would need to procure hardware cleared to store classified material to house the review platform and data (e.g., a laptop computer or a hard drive that can plug in with USB that is appropriately sized). CART would then need to set up a password-protected user profile for Magistrate Judge Porter and separate user profiles for any of his designees. CART would then need to baseline the system, install appropriate programs and drivers, including Axiom, and make sure any necessary applications are functional. CART would then need to load the portable cases for each device into Axiom. Finally, CART would need to customize Axiom per the Court's specifications, creating, for example, pre-set searches and any tags requested by the Court. CART estimates that this whole process would take approximately 2-3 days.

* * *

In sum, CART estimates that all information currently available to be imaged or extracted from the devices will be imaged or extracted and then processed such that it is ready for review approximately 4-6 weeks after the Standstill Order is lifted or modified. However, because the government was unable to complete imaging and extraction and processing prior to the issuance of the Standstill Order, the government has not yet determined what information, or how much

information, is on the devices. Consequently, the government's estimate on how long further processing will take is limited, and the government has no way to estimate how long actual *review* of the information would take.

3. **On which review platform would Magistrate Judge Porter and his designees be able to review the information from Ms. Natanson's devices? (Tr. 11:9-11.)**

As noted above, CART uses the Axiom processing and review platform, designed by Magnet Forensics, to conduct document reviews of this kind. Axiom is highly regarded in the digital forensics industry as a comprehensive and user-friendly tool for analyzing and reviewing digital evidence from computers, mobile devices, and the cloud due to its logical workflow, artifact parsing, and intuitive reporting. The tool has been validated and tested by FBI's Operational Technology Division, keeps up to date with the latest advances in technology, and is the industry standard.

4. **Is there some information that is not OCR-readable (e.g., video and audio files)? If so, how would Magistrate Judge Porter and his designees review this information? (Tr. 17:13-19.)**

As discussed above, CART has identified certain audio files from the devices that are not OCR-readable. Upon further processing, it is likely that CART will identify other information that will not be OCR-readable, such as large video files. All files that are not OCR-readable would be loaded in Axiom as they are found and would be available for review through Axiom's review platform.

5. **Would Magistrate Judge Porter and his designees be able to review the information from Ms. Natanson's devices on a computer in the SCIF at the courthouse in Alexandria? (Tr. 5:22-24, 10:7-14, 16:3-9.)**

As the government noted at the status conference, the FBI is treating all of the information from Ms. Natanson's devices as presumptively Top Secret with Sensitive Compartmentalized Information ("SCI"). CART is currently storing the information from Ms. Natanson's devices in

the CART SCIF. Within the CART SCIF, the information is being stored in a standalone, air-gapped computer—i.e., the computer is not networked with any other devices and is not connected to the Internet.

CART has the ability to create a copy of the information and transfer the copy to a separate standalone, air-gapped laptop computer or hard drive that can be securely transported to the SCIF located in the courthouse in Alexandria, Virginia ("Courthouse SCIF"). From within the Courthouse SCIF, Magistrate Judge Porter and his designees would be able to log on to the laptop computer, which would be set up with the Axiom review platform. As discussed above, the FBI would need to program the laptop computer to require each individual using the laptop to separately log on to that individual's user profile so that the individual's activity could be tracked. CART would need to coordinate with the Court prior to delivery of the laptop to the Courthouse SCIF to prepare such individual user accounts. As noted above, CART estimates that information will be ready for review approximately 4-6 weeks after the Standstill Order is lifted or modified.

6. **Would Magistrate Judge Porter and his designees be able to review the information from Ms. Natanson's devices in a SCIF controlled by the Department of Justice's Litigation Security Group? (Tr. 15:16-17:2, 39:24-41:13.)**

As an alternative to the CART SCIF and the Courthouse SCIF, a SCIF located at facilities controlled by the U.S. Department of Justice ("DOJ") Litigation Security Group (the "LSG") ("LSG SCIF") would also be available for the Court's review. However, for similar reasons as to why the government discourages use of the Courthouse SCIF for the review, the government would discourage use of the LSG SCIF, which was suggested by Movants' counsel.

For background, the LSG is comprised of a specialized team of Security Specialists whose mission is to prevent the unauthorized disclosure of classified information in the judicial process nationwide. LSG's primary facilities are located at a DOJ facility in Washington, DC. These facilities include SCIF spaces at which non-DOJ personnel, including cleared Court personnel and

parties' counsel, can be accompanied by LSG members for purposes of accessing classified information for a particular matter.

In this matter, the Court has appointed Jennifer Campbell from the LSG as the Classified Information Security Officer ("CISO") to provide security guidance and assistance to the Court and parties regarding the protection of classified information. In this role, Ms. Campbell is able to support the Court by, among other things, initiating background investigations and facilitating the security clearance process for members of the Court and for the parties, working with the Court to facilitate secure locations for storage of classified records, and providing specially configured computers and related devices to the Court for processing of classified information.

Although the LSG SCIF would be secure, conducting the review at this location would not enable the kind of technical support that could be easily offered at the CART SCIF. Members of LSG are able to facilitate basic hardware needs of the Court—for example, they could plug in a laptop or hard drive at the LSG SCIF or Courthouse SCIF. However, LSG members' ability to assist with technical issues is limited—for example, if a CART-issued laptop or hard drive were to malfunction, this would likely require support from CART directly. More significantly, LSG members are security specialists, not forensic experts like CART analysts. LSG members do not have specific expertise with respect to the Axiom processing and review platform and could not assist the Court in setting up more than basic searches or using the system to segregate data in the manner in which the Court has indicated it would like to do. Working to identify, isolate, and organize specific data from large datasets is what the forensic and technical experts at CART do routinely. LSG would only be able to help facilitate a conversation with CART analysts in these respects, which could cause significant delays and, potentially, miscommunications.

To be clear, LSG members would not be able to forensically image or extract information from Ms. Natanson's devices, nor would they be able to process any data to prepare it for review. They do not have the hardware or expertise necessary for those tasks. Their services in helping to safeguard classified information, while extremely valuable and necessary for this matter more generally, would not replace the technical expertise of CART experts, who could assist the Court with its proposed review, which would typically be conducted by experts in forensics and investigations with specialized knowledge.

7. What clearances would Magistrate Judge Porter and his designees need to have be able to review the information from Ms. Natanson's devices? (Tr. 9:25-10:6.)

Because all of the information from Ms. Natanson's devices is being treated as presumptively Top Secret with SCI, anyone reviewing the information, including Magistrate Judge Porter, his clerks, or other designees, would require a Top Secret with SCI clearance to start any review.

However, after the review begins, it is possible that reviewers would come across documents that include classified materials containing specific types of SCI that require specific clearances in *addition* to the general Top Secret with SCI clearance before being authorized to continue reviewing the SCI information. Ordinarily, when FBI personnel conduct a review and such SCI is discovered, the FBI personnel are required to immediately stop the review and contact FBI Headquarters liaisons with the relevant IC Community partners, or the relevant IC Community partners directly, to report the SCI. The FBI personnel cannot restart the review without first obtaining additional clearance (i.e., be "read in") to review that SCI, if appropriate and if the personnel is properly cleared. Here, Magistrate Judge Porter and his designees would be required to stop their review if they suspect they have identified classified information that contains SCI.

They would not be able to resume their review until it is determined by the government that the reviewers have the required clearances to proceed.

Based on the underlying criminal investigation, the government has reason to believe that there are classified documents as well as classified information or national defense information that has been extracted from classified documents, residing on Ms. Natanson's devices where the classification headers have been removed. As a result, the Magistrate Judge and his designees would be unable to identify classified information generally, including classified information that includes SCI, during their review without assistance from Executive Branch personnel trained to identify and deal with such classified information. While the Court-appointed CISO, Jennifer Campbell, would be able to provide assistance with classified information clearly marked as such, FBI Special Agents who work closely with classified information routinely and are able to identify classified information that is not clearly marked as such (e.g., Filter Team members), would need to be consulted when information is discovered that appears to be classified. The government notes, however, that although such consultations may assist the Court with the critical duty of identifying and segregating classified information, they would not remedy the larger issue that identifying classified information on devices requires specialized training that, respectfully, the Court does not have.

8. **Would the information to be reviewed be set up in such a way that it would mirror what it looks like on Ms. Natanson's devices, such that Magistrate Judge Porter and his designees could navigate through it with direction from Ms. Natanson? (Tr. 12:22-13:6.)**

Axiom is a pure forensic program that organizes information by categories. The program is not a "virtualized machine" that takes the image of the subject device and presents it like the device from which it was taken. The "virtualized machine" approach would be particularly difficult or impossible to implement here because of the irregular nature of the imaged or extracted

information. For example, CART was able to obtain only a limited image of the Work Computer, and the photographs taken of the Signal chat messages were organized within the Signal application and not on the Work Computer itself.

For this review, the information would be organized within Axiom in a folder system that should somewhat logically follow from, but would not mirror, the setup on Ms. Natanson's devices. CART would be able provide Magistrate Judge Porter and his designees a tutorial on how the folders are arranged in Axiom and how to navigate them prior to any review. Once the review has begun, CART analysts can be consulted by telephone to customize searches and troubleshoot any issues, but conducting the review at the CART SCIF where CART personnel are readily available would make such consultations as seamless as possible. The government notes, however, that although such consultations may assist the Court in its proposed review, they would not remedy the larger issue that identifying evidence of offenses and classified information on devices requires specialized training that, respectfully, the Court does not have.

II. RESPONSES TO QUESTIONS RELATED TO SUBSTANTIVE REVIEW

9. Does the government have a position regarding proposed "Step 1" of Magistrate Judge Porter's review protocol, specifically, to order Movants' counsel to (a) interview Movants regarding the "file architecture" on the devices and report back to the Court, and (b) provide the Court with a list of names of lawyers and people who conveyed information on behalf of lawyers so that the Court can conduct a privilege review. (Tr. 18:14-17, 19:8-20:4.)

a. Interviewing Ms. Natanson to Learn the "File Architecture"

The government has several concerns about the Court's proposal to learn about the "file architecture" of the devices from Ms. Natanson. Although such an approach might save some amount of time because Ms. Natanson could help steer the Court to caches of information that she had designed for organizational purposes that are most likely to contain responsive material, there are risks with that approach that significantly undermine the value of such time savings.

First, and most important, the government has concerns about the security risks involved with asking Ms. Natanson to discuss with other individuals where she stores classified and national defense information she retained on her devices or with whom and in which conversations she discussed such classified or national defense information. One of the primary reasons the government believes it is important that the Executive Branch conduct this review is to limit the further disclosure of such information, and this proposed approach could potentially facilitate further disclosure because, while describing the location of the information on her devices to counsel, Ms. Natanson may provide context of the nature of the information to counsel that is itself classified or highly sensitive. For example, Ms. Natanson potentially might describe to counsel folders on her devices that label or otherwise group documents, communications, or other information by specific sensitive subject matter or even by level of document classification.

Second, the security risks described above would not be worth taking given that the utility of the proposed approach would inherently be limited. Even if Ms. Natanson remembered and described where she put each piece of information on her devices, computers store information in multiple places, often in a fragmented manner. So there may be metadata associated with the files or deleted information or fragments that forensics experts would be able to retrieve. This is not based on how user viewed or organized files. Additionally, since Axiom would organize the information differently than how it appears on Ms. Natanson's devices (i.e., would not "mirror" her devices), even if Ms. Natanson provides what she believes to be accurate information about how the information appears on her devices, this might not help the review along. If it is the case that Ms. Natanson put all relevant material in one folder on her devices, and told the Court which folder that is, that could potentially be helpful. However, it seems more likely that Ms. Natanson stored relevant information—which may include a wide range of types of files, including emails,

chat messages, document drafts, PDFs, and others—in multiple locations and applications on her devices, which might not practically be identified with any precision by Ms. Natanson. Finally, an additional reason why such an approach would be unlikely to yield useful results in this matter is that a significant portion of the information to be reviewed is Signal chat messages captured by photographs. The photographs would have had OCR applied and so could be searched by keyword. However, the photographs would not be arranged in accordance with any file architecture that Ms. Natanson would be able to share. And since the scope of the search warrant would include chat messages not just between Perez-Lugones and Ms. Natanson, but also *about* Perez-Lugones, essentially all of the chat messages within the relevant date range would need to be reviewed by the Court to determine their responsiveness. Thus, Ms. Natanson's "file architecture" information would not be useful for this portion of the review.

Third, there is a not insignificant risk that the information Ms. Natanson would provide regarding her assessment of the "file architecture" could misdirect the Court to focus time and resources in the wrong places. Ms. Natanson has not, so far, been forthcoming with FBI about the devices. *See, e.g.*, Rozhavsky Decl. ¶¶ 25, 32 (describing how Ms. Natanson told the FBI Special Agents searching her residence that that the only devices she had in the residence were a laptop and a cell phone located upstairs (the Personal Computer and the Personal Phone), and that when FBI was leaving the residence with the Work Laptop found in her kitchen, she asked, "What laptop is that?"). There is the possibility that she could make false or inaccurate statements when describing the "file architecture" of her devices that could mislead the Court, rendering the whole exercise of very little value at the expense of the security and forensic risks described above.

b. List of Names for Privilege Review

Notwithstanding the government's strong objection to proceeding with the Court as a filter agent under the circumstances of this case, the government otherwise has no objection to the Court receiving a list of names from the Movants for its privilege review. The government would only caution that the Court's privilege review may very well involve classified information and that, if such circumstances were to arise, the Court and the government would need to work together to properly treat such information.

10. Does the government have a position regarding proposed "Step 2" of Magistrate Judge Porter's review protocol, specifically, to (a) segregate the information according to timestamp metadata and restrict the search to the window of time that's been authorized by the search warrant, and (b) run search terms proposed by the government. (Tr. 19:2-7, 20:5-12, 27:1-13.)

a. Segregate Information According to Timestamp Metadata

As a general matter, the government recognizes that filtering by date is a method that can be used as part of the review to identify data responsive to the warrant. However, the government notes that forensic review software may fail to identify, parse, or accurately display information based on timestamps and date ranges because of the way that digital information is formatted and stored. There would likely be information that is not timestamped at all or that has inaccurate date information. Some files, like the photographs and videos of the Signal chats, may have timestamp metadata reflecting the date on which the files were created rather than the date on which the content of the file was created, or may have date information that reflects an automated process on the computer. And some files may simply have not been timestamped correctly by the computer or the system, or had their labels manually altered. The government proposes that, for any file that lacks timestamp metadata or that has metadata that appears inconsistent or inconclusive, the Court *not* exclude the file from the review by segregating it. In order to identify such files, the government proposes that the Court work closely with CART members, who are forensic experts

skilled in determining which types of metadata are reliable, to determine the parameters for segregating information based on timestamp metadata.

b. Run Search Terms Proposed by the Government

The government does not object to the Court working with the government to identify search terms to apply against the information in Axiom in order to assist in finding responsive material. The government notes, however, that data—including data from messaging applications—often is encoded and stored in formats or databases that interfere with the accuracy of keyword searches. A reviewer who lacks specialized digital forensic training may incorrectly conclude that relevant information is absent when, in fact, it is merely unparsed, unindexed, or not presented by the software in a manner the reviewer recognizes. The search terms in the Filter Team Review Memorandum that the government submitted to the Court on January 30, 2026, could be used initially, but the government would request that it be able to offer additional terms after having an opportunity to review documents identified by the Court as responsive during the course of the Court's review.

* * *

With respect to the Court's proposed "Step 2" more generally, the government notes the following: Identifying evidence of offenses and classified information on devices requires specialized training that, respectfully, the Court does not have. Although Axiom forensic review software is a valuable tool and can identify a substantial portion of data stored on digital devices, the software does not eliminate the need for a fully qualified digital investigative analyst. Only a trained and experienced examiner, such as a CART analyst, has the expertise necessary to recognize, interpret, and account for categories of digital evidence that forensic software may fail to identify, parse, or display accurately. Qualified digital investigative analysts understand that

date filters, keyword searches, and other review limitations can miss both inculpatory and exculpatory evidence because digital information is frequently stored in formats or locations that are not fully indexed or reconstructed by forensic tools. For that reason, filtering decisions made without the involvement of a qualified digital investigative analyst are inherently vulnerable to error. These difficulties are compounded by the need to identify classified information on the devices.

While modern forensic tools such as Axiom provide a user-friendly interface, that ease of use can create a false impression of completeness in the hands of an untrained reviewer. A non-expert may incorrectly assume that the software is displaying all relevant data on the device and that the absence of a keyword hit or results from other search methods means the absence of the underlying information. Experienced digital investigative analysts, like those at CART, know otherwise. They understand that no forensic tool identifies, interprets, or presents all digital evidence perfectly, and they rely on specialized training, technical experience, and artifact-level analysis to recognize the limitations of each tool, identify relevant data, and assign proper meaning to the data. Accordingly, any effort by a non-expert reviewer to identify relevant information, or to apply filtering criteria such as date ranges, keywords, or other search limitations, is likely to produce inaccurate and incomplete results.

11. Does the government have a position regarding proposed "Step 3" of Magistrate Judge Porter's review protocol, specifically, to return to Movants information that the Court finds is not responsive to the search warrant. (Tr. 20:13-21:1. 23:23-24-3.)

While the government appreciates the Court's focus on finding ways to structure the Court's review so as to get information that is not responsive to the search warrant and potentially protected back to the Movants as expeditiously as possible, the government would strongly object to the Court returning any information from the seized devices back to the Movants until such

information is cleared as not containing classified or national defense information by government specialists who have authority to make such determinations.

As discussed above, all of the information on Ms. Natanson's devices is presumed by the government to be Top Secret with SCI and is being treated as such from a security perspective. This is because the government has reason to believe that Ms. Natanson was passed information at that high classification by Perez-Lugones. Respectfully, Magistrate Judge Porter and his designees do not possess that expertise nor the authority to determine what material is classified or constitutes national defense information. *See* Objections to Magistrate Judge's Memorandum Opinion and Order on the Motion for Return of Property filed with the district court on March 10, 2026 (ECF No. 74), at 13.

To the extent information reviewed includes obvious classification markings, the Court could flag such documents for review by government specialists who could confirm whether the information is classified and at what level. However, information on Ms. Natanson's devices may not include such markings because the markings may not have been included in the classified information that was passed to Ms. Natanson or the markings may have been deleted or modified before the information was passed. For such information, the Court could, at best, attempt to make educated guesses on whether the information is classified based on context clues about what information might be of a classified nature. Such an approach, while good-intentioned, would be prone to inadvertent mistake or misunderstanding, and the government has serious security concerns about potentially releasing highly sensitive national security information based on such a review. Therefore, the government asserts that information cannot be returned to Movants until an Executive Branch official with training on how to identify classified information (e.g., an FBI Special Agent) reviews and clears the information.

The government is open to discussing with the Court a system by which information that clearly appears on its face to be unclassified may be prioritized by government specialists for potential eventual release.

12. Does the government have a position regarding whether the parties' communications with the Court in relation to the Court's review should be *ex parte*, *in camera*, under seal, or otherwise? (Tr. 21:21-22:3, 27:18-29:13.)

As discussed during the status conference, the government's position is that it is fair and appropriate for the parties to be aware of submissions any party is providing to the Court, with the exception of classified information and information required by the Court to locate classified information. Such classified information may need to be filed with Court *ex parte*, under seal, and, if necessary, subject to the rules governing classified submissions to a Court. The government, for example, submitted its proposed review protocol not only to the Court but also to the Movants with minor redactions of information that was related to classified information.

The government also recognizes that certain information that the Court may require may involve law enforcement sensitives or other factors where filing under seal or *ex parte* may be appropriate, and it reserves the right to do so if necessary.

13. Does the government have a position regarding whether the Privacy Protection Act of 1980 ("PPA") provides different levels of protection to work-product materials versus documentary materials? (Tr. 22:18-23.)

With respect to PPA-protected information, the government's analysis of the two types of protection and their applicability in this review are articulated in the government's proposed review protocol. After defining both types of PPA protection, the proposed protocol provides direction to the Filter Team about how to treat PPA-protected information encountered during a review, stating:

> To the extent that a search of the Approved Devices uncovers unclassified materials intended for publication that are unrelated to this matter or any criminal conduct and discrete from evidence of the offenses under investigation, such material would

> be protected by the PPA, even if it is not covered by 28 C.F.R. § 50.10 (the Department's Media Regulations). And, as a result, it may not be searched for or seized. If these materials are encountered during a search, they should be segregated. The protocol described below establishes a methodology for such segregation of materials.

The proposed protocol therefore does not provide more or less protection to either work-product materials or documentary materials that are unrelated to this matter or any criminal conduct; rather, the level of protection afforded to both types of materials should be the same: segregation of such materials such that they will not be produced to the prosecution team.

14. Does the government have a position regarding whether Movants' counsel should be provided security clearances? (Tr. 24:16-25:7.)

As a threshold matter, individuals may only have access to classified information if they have a "need to know the information." *See* Exec. Order No. 13526, § 4.1(a)(3) (Dec. 29, 2009). Here, Movants' counsel have no need to know the substance of any classified information in the holdings seized pursuant valid search warrants. Movants' counsel, therefore, should not be provided security clearances.

Dated: March 25, 2026

Respectfully submitted,

BRETT A. SHUMATE
Assistant Attorney General
Civil Division

JOHN A. EISENBERG
Assistant Attorney General
National Security Division

ERIC J. HAMILTON
Deputy Assistant Attorney General
Civil Division, Federal Programs Branch

/s/ Joseph E. Borson
JOSEPH E. BORSON (Va. Bar No. 85519)
Assistant Branch Director
Civil Division, Federal Programs Branch

CHRISTIAN DIBBLEE
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W.
Washington, D.C. 20005
Tel: (202) 514-1944
Email: Joseph.Borson@usdoj.gov

DAVID R. COURCHAINE
Trial Attorney
National Security Division

Counsel for the United States