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

Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT MARINE1VANE@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 1:24-sw-356

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Steven Nestoryak, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a Special Agent with the Federal Bureau of Investigation ("FBI") since March 2017 and am currently assigned to the Counterterrorism Division. While

employed by the FBI, I have investigated federal criminal violations related to matters of domestic terrorism, child exploitation, and cybercrime. I have gained experience through training at the FBI's Basic Field Training Course and everyday work relating to these types of investigations. Prior to my employment with the FBI, I was a sworn Police Officer with the Norfolk Police Department in Norfolk, Virginia, from September 2008 until February 2017. During that time, I was assigned to various investigative units. I am currently a federal law enforcement officer who is engaged in enforcing federal criminal laws, and I am authorized by law to request a search warrant.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 175(a) (Production of Ricin for Use as a Weapon), 18 U.S.C. § 175(b) (Possession of Ricin for Non-Peaceful Purpose), 18 U.S.C. § 175b(c)(1) (Possession of a Select Agent by an Unregistered Person), and 18 U.S.C § 842(p) (Distribution of Information Relating to Explosives, Destructive Devices, and Weapons of Mass Destruction) have been committed by RUSSELL RICHARDSON VANE, IV. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

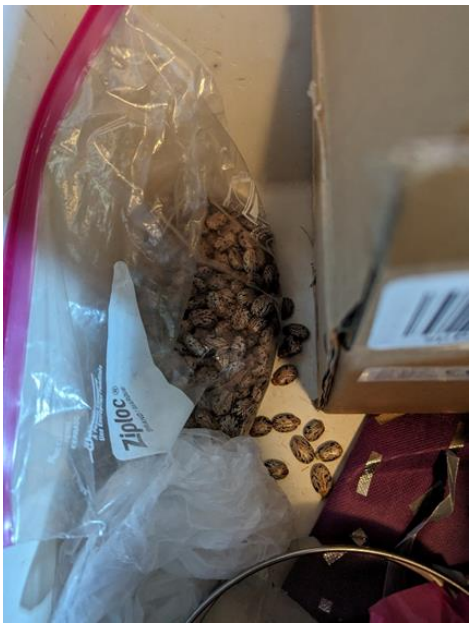
PROBABLE CAUSE

6. RUSSELL RICHARDSON VANE, IV, is a 42-year-old male residing in Vienna, Virginia.

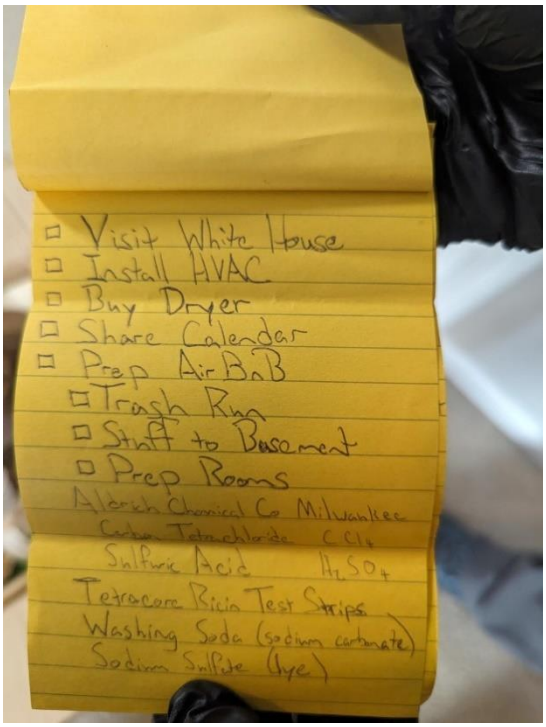
7. VANE came to the attention of the FBI in late March 2024 when members of a Virginia based militia, "The Virginia KEKOAS," released a YouTube video depicting the reasons they kicked VANE out of their organization. The most concerning reasons for VANE's dismissal was VANE's consistent talk of the production of homemade explosives ("HME"), which the militia had no interest in. In the YouTube video, militia members stated that VANE worked in some capacity for the United States Government, had printed off explosives-making instructions from his government network account, and had passed physical copies of that information to one of their members. In an interview with FBI Task Force Officers in early April 2024, one of the militia members turned over an explosives precursor report generated by the Defense Intelligence Agency that VANE had given to them.

8. On April 10, 2024, the FBI executed a search warrant, 1:24-sw-258, on VANE's residence, authorized by the Honorable United States Magistrate Judge William E. Fitzpatrick, for evidence of violations of 18 U.S.C. § 842(p), distribution of information about destructive devices.

9. During the execution of that warrant, FBI Special Agents searched a laundry room in VANE's residence. On a high shelf in that laundry room, the agents discovered a gallon-size Ziplock bag containing beans that appear to be castor beans. No other foodstuffs were stored in the laundry room.



9. Also on the high shelf was a cardboard box containing laboratory equipment, including beakers, a graduated cylinder, funnels, and a rack with test tubes, along with cleaning rags. There appeared to be powdery chemical residue in some of the test tubes. In or near the box, agents also found a handwritten recipe for synthesizing ricin from castor beans. In my training and experience, I know that ricin is highly lethal toxin that is naturally present in castor beans. Using certain chemicals in a laboratory setting, it is possible to isolate the ricin toxin from the castor beans. With the recipe, agents found a handwritten checklist that includes a what appears to be a "To-Do" list and what appears to be a shopping list of items to purchase. The shopping list included "Tetracore Ricin Test Strips."



10. After discovering these items, the FBI obtained a second search warrant (1:24-sw-264) for the ricin-related materials in VANE's residence. Since then, preliminary laboratory testing has confirmed the presence of ricin toxin in and on some of the laboratory equipment seized from the laundry room VANE's home.

10. During the investigation leading up to the execution of the search warrant of VANE's residence on April 10, 2024, Google provided subscriber records concerning e-mail address marine1vane@gmail.com. The name associated with the account's creation was "DUKE VANE" and that the email account had a recovery telephone number of +1 703-774-6725.

11. During the investigation, law enforcement confirmed that VANE was also known as "DUKE" and/or "DUKE VANE." Additionally, in or around early April 2024, VANE attempted to legally change his name to "Duke Russ Hampel."

12. T-Mobile, a cellular telephone service provider, provided subscriber and call detail records for cellular telephone number +1 703-774-6725, the recovery number for

marine1vane@gmail.com. The records provided by T-Mobile showed that the telephone number had a subscriber name of VANE BROTHERS FINANCE LLC, with a subscriber address that corresponded to VANE's residence. A records check of the State Corporation Commission for the Commonwealth of Virginia confirmed that the principal office address for VANE BROTHERS FINANCE LLC was the same address as VANE's residence, and an active Registered Agent listed as RUSSELL VANE IV as of May 10, 2024.

13. The FBI also confirmed that beginning on or about December 29, 2022, and continuing through on or about February 5, 2024, VANE had periodically conducted detailed research on his work computer relating to the making of explosives, explosives precursors and chemical compounds, ricin, sarin, and the manufacture and offensive use of poisons. VANE had also printed over a dozen articles, reports, and/or publications related to his searches for these materials.

BACKGROUND CONCERNING GOOGLE[1]

14. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

15. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

16. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

17. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

18. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

19. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events

or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

20. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

21. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and

documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

22. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

23. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

24. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are

enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

25. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

26. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

27. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed),

the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

28. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

29. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. With the specific Google search history data this warrant seeks, this writer will be able to determine the method in which VANE sought to produce ricin, possible suppliers of the raw materials used in ricin production, when VANE's production of ricin began, the identity of possible targets or co-conspirators, and why VANE produced ricin.

30. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored

communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

31. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

32. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

33. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity,

documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

34. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

35. Based on the forgoing, I request that the Court issue the proposed search warrant.

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Steven T. Nestoryak
Special Agent
Federal Bureau of Investigation

Respectfully submitted and attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on May 15, 2024.

Digitally signed by Ivan Davis
Date: 2024.05.15 14:06:25 -04'00'

Honorable Ivan D. Davis
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with marine1vane@gmail.com ("the Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC AND/OR Google Payment Corporation ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on April 4, 2024, with the Google Reference Number 57201695, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from **December 29, 2022**, to **April 1, 2024**, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
6. Length of service (including start date and creation IP) and types of service utilized;
7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

e. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

f. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

g. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record; and

h. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google

Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

Google is hereby ordered to disclose the above information to the government within **fourteen (14) days** of issuance of this warrant.

II. Information to be seized by the Government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations 18 U.S.C. § 175(a) (Production of Ricin for Use as a Weapon), 18 U.S.C. § 175(b) (Possession of Ricin for Non-Peaceful Purpose), 18 U.S.C. § 175b(c)(1) (Possession of a Select Agent by an Unregistered Person), and 18 U.S.C. § 842(p) (Distribution of Information Relating to Explosives, Destructive Devices, and Weapons of Mass Destruction) involving RUSSELL RICHARDSON VANE IV and occurring after December 29, 2022, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

a. The production, storage, use, and/or distribution of ricin;

b. Communications with individuals providing VANE with instructions or advice on how to produce, store, use, or distribute ricin;

c. Homemade explosives, explosives precursors, and the production, construction, or use of explosive devices;

d. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

e. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation; and

f. The identity of the person(s) who created or used the Account.

General Government Review Procedures

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in

addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Federal Bureau of Investigation may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Filter Review Notice Procedures

If the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e., communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team, and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. This investigation is presently covert, and the government believes that the subject of the search is not aware of this warrant.