UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

IN THE MATTER OF THE SEARCH OF SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH MOOBOT MALWARE	)	Case No. 24-MJ-129

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania and elsewhere:

SEE ATTACHMENT A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before February 9, 2024
(not to exceed 14 days)

❒ In the daytime 6:00 a.m. to 10 p.m. **X** at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Richard A. Lloret.
(name)

X I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized for 30 days.

Date and time issued: 1/26/2024 3:31 pm

/s/ The Honorable Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

HON. RICHARD A. LLORET, USMJ
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to be Searched

This warrant applies to U.S.-based routers manufactured by Ubiquiti and infected with Moobot malware ("Subject Devices") [redacted]

[redacted]

ATTACHMENT B

Particular Things to be Seized

This warrant authorizes the remote access and search of the Subject Devices identified using the method in Attachment A, and the seizure of data from the Subject Devices, as the evidence and instrumentality of computer fraud and conspiracy in violation of Title 18, United States Code, Sections 1030(a)(2)(C) (unauthorized access to a protected computer and obtaining information), 1030(a)(5)(A) (damage to a protected computer), and 371 (conspiracy). This warrant authorizes the government to remotely access the Subject Devices and issue commands to:

a. copy stolen data, malicious files and scripts, and directory and file listings;

b. remove stolen data and malicious files;

c. block access [redacted]

d. change the firewall rules to block [redacted] to block remote access [redacted] and to block communication with known malicious [redacted] and

e. enable the subsequent collection and transmission of non-content information about attempts to remotely access the Subject Devices [redacted]

This warrant does not authorize the seizure of any tangible property. Except as provided above, this warrant does not authorize the seizure or copying of any content from the Subject Devices identified using the method in Attachment A.

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

IN THE MATTER OF THE SEARCH OF SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH MOOBOT MALWARE	Mag No. 24-129 **(UNDER SEAL)**

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41(b)(6)(B) FOR A SEARCH AND SEIZURE WARRANT

I [redacted] a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. The United States is investigating unauthorized computer intrusions being perpetrated by a group known to private cybersecurity investigators as APT28 (also known as the "Sofacy Group," "Forest Blizzard," "Pawn Storm," "Fancy Bear," and "Sednit"). Operating since at least 2007, the group is known to target U.S. persons, government, military, and security organizations, corporate entities, international organizations, and their respective employees. In 2018, the Department of Justice and the FBI, publicly attributed APT28 to Unit 26165 of the Main Intelligence Directorate of the General Staff ("GRU"), which is a military intelligence agency in the Russian Federation. Relevant to this application, the FBI is investigating APT28 actors' unauthorized access to routers manufactured by a U.S.-based company known as Ubiquiti Inc. ("Ubiquiti"). The APT28 actors leverage the routers as proxy computers to conceal their true

location and identity while committing other federal crimes,[1] including harvesting credentials, collecting NTLMv2 digests,[2] as well as hosting spearphishing[3] landing pages and custom tools.[4]

2. FBI agents, analysts, and computer scientists have identified victim-owned Ubiquiti routers worldwide, including U.S.-based routers (the "Subject Devices") identified in Attachment A, infected with "Moobot," a Mirai-based malware developed by suspected criminal cyber actors (as opposed to APT28) that turns network devices running Linux into remotely controllable bots. During the course of the investigation, the FBI has developed evidence that APT28 is using Moobot to access and control numerous Ubiquiti routers, including the Subject Devices. The owners of multiple infected routers consented to the FBI accessing and analyzing their routers, allowing the FBI to develop the technical ability to remotely access compromised Ubiquiti routers accessible to APT28 actors, collect evidence of federal crimes, and to prevent

---

1 A proxy, often referred to as a proxy server, is a computer that acts as a relay, separating the user from the website that the user is browsing. There are several reasons to use a proxy server. It can provide privacy by shielding a user's IP address from websites they visit and can provide access to geographically-locked content or servers.

2 NTLMv2, or New Technology LAN Manager version 2, is a suite of security protocols that Windows-based computers can use to authenticate users' identities. This protocol is used to implement single-sign-on so that a user's identity can be confirmed without submitting a password. During the authentication process, an alphanumeric string, called a digest, is calculated based on the password, and that digest can then be used to authenticate a user's identity. An NTLMv2 digest is a representation of a user's password. By collecting such information, a hacker can access the underlying computer as though they were a legitimate user.

3 Spearphishing is a method of targeting specific individuals or groups using emails, social media, or other communication platforms to get a user to divulge sensitive information, oftentimes login credentials. Spearphishing messages are often designed to deceive the recipient into believing the message has come from a legitimate source.

4 A landing page is the web page that appears in an Internet browser in response to clicking an Internet link. A landing page, like any web page, can have spaces for user input (such as login credentials), and clickable links or icons that redirect user inputs to another web page. The purpose of a malicious landing page can be to obtain user data (*e.g.*, some mimic webmail login pages to trick the user into entering their username and password) and send it to an actor-controlled web page or server.

further access and related crimes by malicious actors. The FBI now seeks authorization to use the technical capability it has developed to remotely search the Subject Devices and to interfere with APT28's ability to use the property in committing federal crimes. The FBI will leverage [redacted] installed on the routers by criminal hackers to electronically connect to the Subject Devices identified in Attachment A and issue commands to: (1) retrieve data from the router relating to malicious activity; (2) remove malicious files; (3) remove APT28's access to [redacted] the routers; (4) block remote access to the devices via [redacted] (until reversed, if desired, by the device owner); and (5) enable the subsequent collection and transmission of non-content information about remote login attempts, pursuant to a separate Pen Register/Trap and Trace Order. These actions, further described below and in Attachment B, will allow the FBI to neutralize the APT28 actors' illegal access to these routers for criminal conduct until the victims can take further steps to mitigate the compromises and reassert full control over their routers.

3. Therefore, I submit this affidavit in support of an application for a warrant under Federal Rule of Criminal Procedure 41(b)(6)(B) to remotely search those routers, further identified in Attachment A, and to seize and copy electronically stored information that constitutes evidence and seize property designed for use, intended for use, or used in committing a crime, pursuant to Federal Rule of Criminal Procedure 41(c)(3), further described in Attachment B.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other witnesses and agents. 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.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(2)(C)

(accessing a protected computer without authorization and obtaining information), 1030(a)(5)(A) (intentional damage to a protected computer) and 371 (conspiracy) ("Subject Offenses") have been committed in the Eastern District of Pennsylvania and elsewhere. There is also probable cause to remotely search the routers identified in Attachment A and seize the evidence, contraband, fruits, and/or instrumentalities of the Subject Offenses further described in Attachment B.

AGENT BACKGROUND

6. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been [redacted] I am currently assigned to the [redacted] Division of the FBI and work on the national security cyber squad. In this capacity, I am charged with investigating possible violations of federal criminal law, specifically those involved with cybercrimes. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including functioning as a case agent on computer crime cases. I have received training in the conduct of computer crime investigations. I have also received training and gained experience in interviewing and interrogation techniques, the execution of legal process such as preservation requests, 2703(d) orders, and subpoenas, and the identification and collection of computer-related evidence.

STATUTORY AUTHORITY

7. Federal Rule of Criminal Procedure 41(b)(6) provides that "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."

8. Title 18, United States Code, Section 1030(a)(5)(A) provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished[.]" Section 1030(e)(2)(B) defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" Section 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information[.]" Title 18, United States Code, Section 1030(a)(2)(C) provides that whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished[.]"

9. Title 18, United States Code, Section 371 provides: "If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both."

PROBABLE CAUSE

A. APT28 Use of Compromised Routers

10. The FBI has been monitoring APT28's use of compromised Ubiquiti routers as part of this investigation. In particular, APT28 has been utilizing these compromised routers to proxy browsing traffic, harvest credentials and collect NTLMv2 digests, as well as to host spearphishing landing pages and custom tools.

11. APT28 utilizes a variety of malware to gain unauthorized access to and control victim computers. The malware historically involved varying capabilities, including spying

functionalities, such as keystroke logging, and file exfiltration. In compromising the Ubiquiti routers specifically, APT28 is leveraging existing SSH malware,[5] implanted by the Moobot actors, as an initial access vector onto the routers. The Moobot actors have installed a suite of malware ("Moobot malware"), including the SSH malware, to create and maintain a botnet that infects Internet of Things (IoT) and other devices, using remotely exploitable vulnerabilities or weak passwords. Relevant to this affidavit, Moobot exploits vulnerable Ubiquiti routers by using default credentials – *i.e.*, generic, publicly known login credentials used to access devices during initial setup – and are accessible remotely through the Internet, and then implants malware. One of these implants is an SSH malware [redacted] permits administrator access to anyone [redacted] This implant displays a specific OpenSSH version number in its public-facing software banner that does not correspond to a legitimate version of OpenSSH.[7] Based on the FBI's review of the contents of numerous Moobot-infected Ubiquiti routers, the FBI assesses that the APT28 actors likely find and illegally access compromised Ubiquiti routers by conducting public scans of the Internet using the specific OpenSSH version number as a search parameter, and then using Moobot [redacted] to access the compromised Ubiquiti routers.

---

5 SSH stands for the secure shell and is a protocol, or method, for securely sending commands to a computer over an unsecured network.

[redacted]

7 OpenSSH is the open-source suite of tools widely used to remotely access computers using the SSH protocol.

12. The Ubiquiti routers have a robust operating system and are popular with users because they are user friendly but nevertheless offer greater capabilities than most consumer-level routers. Accordingly, these devices are attractive targets for malicious actors because they can repurpose these routers as capable platforms to conduct illegal activity. While reviewing compromised Ubiquiti routers obtained through consent, FBI identified several bespoke scripts and files that contained details of APT28 and Moobot computer intrusion campaigns (*e.g.*, custom Python scripts to collect webmail credentials, instances of programs used to collect NTLMv2 digests, and routing rules to designed to redirect phishing traffic to dedicated infrastructure). Across several routers, the FBI found numerous overlapping tactics, techniques, and procedures (commonly referred to as "TTPs") associated with APT28.

13. For example, APT28 actors have used compromised Ubiquiti routers to facilitate spearphishing campaigns. In some instances, the actors sent specially-crafted spearphishing emails to Microsoft Outlook users, exploiting a zero-day vulnerability (*i.e.*, one that was previously unknown, and therefore unpatched), to transmit victims' login credentials back to the compromised Ubiquiti routers. APT28 actors also used compromised Ubiquiti routers to receive and store the stolen credentials received from unwitting victims of APT28's spearphishing attempts. In another identified campaign, APT28 actors designed a fake Yahoo! landing page to send credentials entered on the false page to a compromised Ubiquiti router to be collected by APT28 actors at their convenience. Based on FBI's analysis, APT28 typically creates and modifies files in the /home/ and /root/ directories on the device.

14. In addition to files associated with APT28 actors, the compromised Ubiquiti routers analyzed by the FBI contain several directories and files created and installed by Moobot. These directories and files are associated with Moobot malware and are not created by legitimate users or by normal system processes. These files typically include stolen user credentials and files and

scripts that provide Moobot with additional functionality, including a script allowing communication back to the Moobot command-and-control ("C2") infrastructure, tools for brute-forcing passwords and propagating the Moobot malware, and malware designed to steal legitimate router user credentials.

15. Compromised Ubiquiti routers also contain Moobot files listing several malicious domains and IP addresses. In some instances, compromised Ubiquiti routers have been observed creating VPN tunnels to communicate with these IP addresses, which appear to be Moobot C2 servers.

B. FBI's Ability to Disrupt Malicious Activity

16. Based on a detailed review of several compromised Ubiquiti routers, the FBI [redacted] has allowed it to identify hundreds of Moobot-infected devices in more than five federal judicial districts in the United States, including at least one device in the Eastern District of Pennsylvania. These Ubiquiti devices appear to be compromised by Moobot and are thus likely accessible to APT28 actors. Specifically, as of January 23, 2024, IP addresses for three compromised devices geolocate to Philadelphia, Pennsylvania and are serviced by Verizon Business or Comcast Cable Communications, LLC.

17. The FBI has also developed a series of commands to be sent to the Subject Devices, via the Moobot [redacted] that will disrupt Moobot and APT28 from using the compromised routers in committing federal crimes. These commands [redacted] retrieve data from the Subject Devices, delete known malicious files, and make reversible changes to the Subject Devices that would prevent malicious actors from remotely accessing the Subject Devices and committing federal crimes on or with the Subject Devices. The commands to be delivered to the Subject Devices pursuant to this warrant would specifically accomplish the following tasks:

a. copy the following data from the Subject Devices:

   i. malicious Moobot files and other actor-created files, as discussed in paragraphs 14 and 15;

   ii. stolen data stored by malicious actors, as discussed in paragraphs 13 and 14; and

   iii. a list of directories and files within the /home/ and /root/ directories;[8]

b. remove malicious files discussed in paragraph 17(a)(i)-(ii) [redacted];

c. remove APT28's access [redacted][9]

d. make reversible changes to the firewall rules on each device to block remote access [redacted] to block remote access [redacted] and to block

---

[8] As discussed in paragraph 13, APT28 typically creates and modifies files in the /home/ and /root/ directories on the device. The commands issued by FBI will instruct the Subject Devices to transmit the names of subdirectories and files in these particular directories to the FBI [redacted] This process will terminate at the end of the warrant period. These commands will not provide the FBI with the contents of these directories or files. Other than files and directories created or changed by malicious actors, these directories should only contain default files and files related to the router's operating system because the Subject devices are routers, and not personal computers or mobile devices. If malicious actors regain access to one of the Subject Devices during the warrant period, changes to the directories and files may alert the FBI to the malicious actors' attempts to troubleshoot their loss of access.

[9] The FBI will block APT28's remote access [redacted], thereby preventing the router's use as an instrumentality of further crime. FBI's command will also [redacted] preventing APT28 from [redacted] compromised the Subject Devices [redacted]

communication with known [redacted] as discussed in paragraph 15;[10] and

e. enable the collection and transmission of non-content (*i.e.*, IP addresses) about attempts to remotely access the Subject Devices [redacted]

18. The commands issued from an FBI-controlled server will only affect Subject Devices [redacted] In the event [redacted] not work on a Subject Device, communication with that Subject Device will fail, and the Subject Device will not be affected by the actions authorized by this warrant.

C. Request for Anticipatory Search

19. Based on [redacted] there were approximately [redacted] IP addresses associated with Subject Devices in the United States as of January 22, 2024. The FBI's current visibility is [redacted] Over the course [redacted] the list of IP addresses has

---

[10] The firewall rules will block remote access [redacted] by blocking incoming traffic on the ports solely used by these services. This will not interrupt any other services accessible from the outside Internet that victims may have running on the Subject Devices. The FBI commands will also prevent communication to and from [redacted] In my training and experience, because the [redacted] assigned to servers solely used to communicate with [redacted] malware, it is highly unlikely that a victim would be attempting to communicate with [redacted] voluntarily. The new firewall rules will be visible and accessible to any users accessing their Web UI locally, that is, from the same network as the router. In the event the Subject Devices' owners want to revert the firewall rules to those in place prior to the FBI's seizure of the Subject Devices, the owners will be able to easily access the routers from their local network and undo the firewall changes via the Web UI or by factory-resetting the device.

[11] Based on my training and experience, I expect that malicious actors will attempt to use [redacted] to access the Subject Devices after execution of the commands in paragraph 17(a)-(d). [redacted] The government will request a separate pen register/trap and trace court order authorizing the collection and review of data sent to the FBI-controlled server. This process will terminate at the end of the warrant period.

fluctuated [redacted] It is therefore likely that the FBI's list of IP addresses associated with Subject Devices can change quickly. Accordingly, the FBI seeks to deliver the same commands described in paragraph 17 to additional IP addresses that FBI discovers [redacted] at any point during the execution of this warrant. Thus, this application seeks approval to execute the search described herein on the lists of IP addresses identified [redacted] described in Attachment A during the time period of execution of the warrant.

D. Remote Access, Search, and Seizure

20. As described above, the FBI has identified approximately [redacted] IP addresses associated with Subject Devices in the United States. These devices are infected with Moobot malware, are likely being used as criminal instrumentalities as described herein, and are capable of being exploited for yet-to-be-identified ends. Through this application, the FBI seeks authority to remotely access the Subject Devices, search those devices for malicious files and other evidence of APT28 and Moobot malicious activity, and seize such files and data. The FBI also seeks authority to, through the modification of the Subject Devices' firewall rules, temporarily seize the routers to prevent further access and related crimes by malicious actors until the Subject Device's legitimate owners have the opportunity to regain full control of such devices.

21. Based on the FBI's analysis of Ubiquiti router functions, conversations the FBI has had with Ubiquiti, and the historical actions of the malicious actors, the steps described in paragraph 17 of this affidavit are a reasonable way to neutralize the APT28 actors' ability to further access the routers.

22. The FBI has tested its technical ability to send the aforementioned commands to compromised Ubiquiti routers and those commands achieved the intended results as described in

paragraph 17 of this affidavit. During extensive testing, the commands successfully copied, deleted, and otherwise effectuated the desired changes. This testing showed that no other legitimate functionality of the devices was impacted. To ensure that the operation is conducted as intended, the FBI commands will cause the Subject Devices to relay a confirmation that it has received the commands back to the FBI-controlled server. This will ensure the search described herein is being carried out, and that the commands operate, as intended. The FBI-controlled server will not maintain a communications channel with the Subject Devices after the execution of this warrant.

23. The changes made to the firewall rules will appear to the owner of any Ubiquiti router in the Web UI, along with all the firewall rules the user has implemented. This means that any device owner can modify the new firewall rules. Additionally, the FBI intends to publicly explain (in connection with the announcement of the execution of this search warrant) that a device owner can change these rules to their preferred configuration.

24. Subject Devices located in the United States constitute "protected computers" within the meaning of Rule 41(b)(6)(B) and § 1030(e)(2)(B) because they are used in or affecting interstate or foreign commerce or communication, based on their connection to the Internet. The routers have been "damaged" within the meaning of Rule 41(b)(6)(B) and § 1030(e)(8) because the installation of malware has impaired the integrity and availability of data, programs, systems, and information on the devices.

25. The FBI [redacted] to date has identified Subject Devices in almost every state, including portions of Pennsylvania that are in the Eastern District of Pennsylvania. Thus, the Subject Devices are located in five or more judicial districts.

TIME AND MANNER OF EXECUTION

26. The FBI requests that the Court authorize the government to access the relevant victim computers located in the United States for a period of 14 days, beginning on or about January 26, 2024.

27. The FBI requests that the Court authorize the government to execute the warrant at any time in the day or night. There is good cause to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to legitimate users.

[redacted]

REQUEST FOR SEALING AND DELAYED NOTICE

28. Based on my training and experience and my investigation of this matter, I believe that reasonable cause exists to seal this application and warrant, as well as the return to the warrant, and to delay the service of the warrant for up to 30 days after execution of the warrant. Pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), delayed notice of the execution of a search warrant is permitted if three requirements are satisfied: (1) the Court finds reasonable cause to believe that providing immediate notification may have an adverse result, as defined in 18 U.S.C. § 2705; (2) the warrant does not allow the seizure of tangible property, wire or electronic communication, or stored wire or electronic information (unless the Court finds reasonable necessity for the seizure); and (3) the warrant provides for the giving of such notice within a reasonable period after execution, not to exceed 30 days unless the facts of the case justify a longer period. 18 U.S.C. § 3103a(b)(1)-(3). An "adverse result" includes a list of factors including "seriously jeopardizing an investigation." 18 U.S.C. § 2705(a)(2).

29. Here, allowing premature disclosure to the public at large or to individual owners of the Subject Devices would seriously jeopardize the investigation and the effort to remediate the

infected routers. Premature disclosure could give state-sponsored and criminal hackers the opportunity to destroy the evidence on the victim devices or make changes to the malware enabling continued or additional damage to victims' devices or that otherwise thwart the successful execution of the operation described in this affidavit.

30. When notice is no longer delayed, the United States intends, pursuant to Rule 41(f)(1)(C), to provide notice through public announcement and via third parties. Federal Rule of Criminal Procedure 41(f)(1)(C) provides the following regarding the means of providing notice of the warrant and receipt:

> For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.

31. The FBI will provide notice to the Internet Service Provider (ISP) that hosts the IP address for the victim asking the ISP to provide notice to its client. For each such notification, the FBI will attach a copy of the requested warrant and receipt. Additionally, the FBI will issue a public notice on its official website (www.fbi.gov) that the FBI conducted the operation to alert the victims and notify them of their ability to reverse the FBI's above-described seizures. The FBI, along with partner agencies will also publish a cybersecurity advisory providing further details of the operation and the malicious threat actors. The Department of Justice will issue a similar notice on its official website (www.justice.gov). I believe that this combination of methods is reasonably calculated to reach those persons entitled to service of a copy of the warrant and receipts.

CONCLUSION

32. I submit that this affidavit supports probable cause for a warrant to use remote access to search electronic storage media described in Attachment A and to seize and copy the information described in Attachment B.

Respectfully submitted,

[redacted]

Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me by telephone on January 26, 2024, and I find that sufficient probable cause exists.

/s/ The Honorable Richard A. Lloret
HON. RICHARD A. LLORET
UNITED STATES MAGISTRATE JUDGE