AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	
2003 Silver Subaru Forester 4D, TXLP: RMK7178, VIN: JF1SG63643G757363, currently located at located at the Alvarado Police Department	)	Case No. 4:25-MJ-460
	)	FILED UNDER SEAL

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 Northern District of Texas
(identify the person or describe the property to be searched and give its location):
2003 Silver Subaru Forester 4D, TXLP: RMK7178, VIN: JF1SG63643G757363, currently located at located at the, as further described in 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 7/22/25 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ 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 United States Magistrate Judge Jeffrey L. Cureton.
(name)

N/A 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 *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/8/25 @ 1:29pm

Judge's signature

City and state: Fort Worth, Texas

United States Magistrate Judge Jeffrey L. Cureton
Printed name and title

Return

Case No.: 4:25-MJ-460	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

The property to be searched is **2003 SILVER SUBARU FORESTER 4D, TXLP: RMK7178, VIN: JF1SG63643G757363 which is located at the Alvarado Police Department, 600 South Parkway Drive, Alvarado, Texas which is located in the Northern District of Texas and shown below.**

Attachment A

ATTACHMENT B

Property to be seized

1. All records relating to violations of the following: 18 U.S.C. § 111 (Assault on f a Federal Agent); 18 U.S.C. § 1114 (Protection of Officers and Employees of the United States, and Officers Assisting Such an Officer); 18 U.S.C. § 1361 (Damage to Government Property); and 18 U.S.C. § 371 (Conspiracy), those violations involving the following known individuals: Bradford Winston Morris aka Meagan Morris ("MORRIS"); Ines Soto ("I SOTO"), Nathan Josiah Baumann ("BAUMANN"), Elizabeth Soto ("E. SOTO"), Maricela Rueda ("RUEDA"), Seth Edison Sikes ("SIKES"), Joy Abigail Gibson ("GIBSON"), Savanna Batten ("BATTEN"); and Zachary Jared EVETTS, **and other unknown individuals** and occurring on or about July 4, 2025, including:

   a. Any and all firearms, ammunition, fireworks, weapons, and ballistic vests;

   b. Any and all flyers, printed materials, social media posts, and communications concerning: anti-government ideology; over throwing the U.S. Government; anti-law enforcement; interfering with Immigration and Customs Enforcement and/or other law enforcement or government functions;

   c. Any and all notes, plans, training materials, manifestos, and drawings;

   d. Any and all spray paint or other paint material;

e. Any and all receipts, bills, invoices, or similar documents showing the purchase of any of the above items;

f. Any and all contact lists;

g. Any and all text messages, phone logs, instant messages, private messages, emails, voicemails and other forms of electronic communication using a cellular telephone or electronic device;

h. Any and all photographs including still photos, negatives, videos, showing evidence of the aforementioned offenses and that will help identify others involved in the offenses;

i. Any and all location information on the electronic devices and GARMIN SOLAR WATCH;

j. Any and all cellular telephones, laptops, radios, and other communication devices;

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disk drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied 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 FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2003 Silver Subaru Forester 4D, TXLP: RMK7178, VIN: JF1SG63643G757363, currently located at located at the Alvarado Police Department

Case No. 4:25-MJ-460

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

2003 Silver Subaru Forester 4D, TXLP: RMK7178, VIN: JF1SG63643G757363, currently located at located at the, as further described in Attachment A.

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 111	Assault on a Federal Officer
18 U.S.C. §§ 924(c)	Possession of a Firearm in Furtherance of a Crime of Violence

The application is based on these facts:

See attached Affidavit of FBI Task Force Officer Stanley Scott Mitchell

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Task Force Officer Stanley Scott Mitchell, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/8/25

Judge's signature

City and state: Fort Worth, Texas

United States Magistrate Judge Jeffrey L. Cureton
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

IN THE MATTER OF THE SEARCH OF:

2003 SUBARU TXLP: RMK7178 VIN: JF1SG63643G757363

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

I, Stanley Mitchell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of three applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the three items listed below, which includes a vehicle, a cellular telephone, and a Garmin watch, described below hereinafter "PREMISES," further described as:

2003 SILVER SUBARU TXLP: RMK7178 VIN: JF1SG63643G757363;

more particularly described in Attachment A, for the things described in Attachment B.

2. I am a Task Force Officer with the Federal Bureau of Investigation (FBI) duly appointed and acting according to law. I have been assigned as an FBI Task Force Officer since February 2019. I have been assigned to the Dallas Division of the FBI, where I have been assigned to investigate violations of federal law including violations involving terrorism. As a federal agent, I am authorized to investigate violations of

United States laws and to execute warrants issued under the authority of the United States. I have been employed with the Fort Worth Police Department since 1998 and have served in several roles to include Patrol, Emergency Preparedness and Incident Command, Hostage Negotiation Team and the Homeland Security Unit. In addition to my law enforcement background, I hold a Bachelor of Science degree from Texas Tech University in Biology

PROBABLE CAUSE

3. As will be explained below on the evening of July 4, 2025, there was a concerted attack on the Federal Immigration and Customs Enforcement Detention Facility known as Prairieland Detention Center ("Prairieland") located 1209 Sunflower Lane, Alvarado, Texas. This affidavit is being submitted in support of one Applications for Search Warrant pursuant to Federal Rule of Criminal Procedure 41. The violations of law under investigation, include but are not limited to the following: 18 U.S.C. § 111 (Assault on a Federal Officer); 18 U.S.C. § 1114 (Protection of Officers and Employees of the United States, and Officers Assisting Such an Officer); 18 U.S.C. § 1361 (Damage to Government Property); and 18 U.S.C. § 371 (Conspiracy).

4. On July 4, 2025, at approximately 10:37 PM Central Standard Time (CST), Prairieland Detention Center, located at 1209 Sunflower Lane, Alvarado, Texas, became concerned that a group of unidentified subjects were breaking into the facility. Prairieland Detention Center is a Department of Homeland Security ("DHS")

detention facility which holds persons related to immigration violations or are awaiting deportation hearings.

5. At approximately 10:42 PM CST, the group was observed on CCTV spraying graffiti, firing fireworks towards the facility, and using high powered flashlights. DHS Officers manning the facility then called 9-1-1, prompting a response from Alvarado Police Department ("PD").

6. At approximately 10:59 PM CST, an Alvarado Police Department ("APD") officer was dispatched to the Prairieland Detention Center to make contact with the unidentified subjects. The APD officer was engaged with gunfire and was shot in the neck and/or upper back area. DHS Correctional Officers within Prairieland Detention Center also reported they were being engaged by gunfire and were observed on CCTV ducking for cover.

7. Shortly thereafter, Bradford Winston Morris aka Meagan Morris (MORRIS), was traffic stopped after fleeing the scene in a red/maroon 2007 Hyundai bearing Texas License Plate: CLP-3588 and was taken into custody by the Johnson County Sheriff's Office ("JCSO") detective. That is, the detective with JCSO was enroute to Sunflower Lane when he was radioed and told that a red/maroon Hyundai was observed fleeing the scene and that it was headed in the detective's direction. During the traffic stop, a black pistol was observed in plain view in the vehicle and the occupant was asked if there were any other firearms in the vehicle. The sole occupant, MORRIS, told the JCSO officers that there was another firearm in the backseat. At that time the officers

observed an AR-15 style rifle in the backseat of the car. MORRIS was removed from the vehicle and detained. The JCSO officers observed two Kevlar ballistic style vests, one of which was in the backseat and the other was in the back of the van. There was also a ballistic helmet in the vehicle. MORRIS had a loaded magazine in his pocket that matched the pistol and a radio in his possession. MORRIS was Mirandized and waived his rights. MORRIS said that he met these people online and that he transported some of them down from Dallas. MORRIS said the plan was to go to the location to make some noise. MORRIS claimed ownership of all the firearms in the vehicle. As a part of the investigation, FBI has been able to determine that MORRIS's residence is 2452 56th Street, Dallas, Texas (.

8. Further, during the course of the investigation, MORRIS was interviewed by a Special Agent with the FBI and a Ranger with Texas Department of Public Safety. MORRIS was *Mirandized* and waived his rights. MORRIS told the FBI that he was at home in Oak Cliff and he heard about an event on a Signal Group Chat that he was a part of. MORRIS told the FBI that that he had been a part of the group chat for a while and that he had been invited to the group chat years ago after attending a protest. MORRIS explained he drove himself, his girlfriend (Autumn Hill), and two people he knew by nicknames, Champagne and Rowan. (During the course of the investigation, MORRIS identified Joy Abigail GIBSON as the individual he knew as Rowan.) MORRIS said that Champagne and Rowan were strangers, but he invited them to his home in Oak Cliff to ride together to the event at Prairieland Detention Center. MORRIS said he drove the

four of them there and parked in a nearby area. MORRIS said he took his handgun, his AR-15 style rifle, and a bullet proof vest. MORRIS said he brought those for his own protection and that he also brought four handheld radios. MORRIS said he gave three of the radios to Hill, Champagne, and Rowan and they decided that MORRIS would stay in the car to protect the vehicle to make sure no one broke into the vehicle. While MORRIS was in the car, he saw multiple other vehicles parked in the area to include a red car parked in front of his and a white SUV. (During the course of the investigation, the red car MORRIS described was determined to be 2016 Red Mazda CX5 TXLP: NRJ7521 registered to Zachary Jared EVETTS. Further, during the course of the investigation, the white SUV was determined to be 2017 White Nissan Rogue TXLP: TXM9235 that was driven by Nathan Josiah Baumann, who resides in College Station, Texas). MORRIS explained that he observed a male get out of the front driver's seat of the red car and pull out a cart/wagon and load the cart/wagon with fireworks and a case of water. MORRIS denied seeing any firearms being loaded into the cart/wagon, and he stayed in the car. MORRIS said that at some point he heard gun shots and waited for his friends for approximately two minutes and then decided that was long enough and he left. Shortly after leaving, MORRIS was stopped by JCSO as referenced above.

9. At approximately 11:10 PM CST, JCSO Deputies made contact with seven additional subjects at the intersection of Tanglewood Dr and Burnett Blvd, approximately 300 yards east of the engagement of the APD officer. The subjects were dressed in black, military-style clothing, body armor, and covered in mud. Some of the subjects were

armed and others had radios. Additional firearms, magazines containing ammunition, and body armor were found during a search of the area between this encounter and the Prairieland Detention Center.

10. The following subjects were taken into custody by law enforcement: Ines Soto ("I SOTO"), Nathan Josiah Baumann ("BAUMANN"), Elizabeth Soto ("E. SOTO"), Maricela Rueda ("RUEDA"), Seth Edison Sikes ("SIKES"), Joy Abigail Gibson ("GIBSON"), and Savanna Batten ("BATTEN").

11. When SIKES was arrested, he had a handgun in his waist band and an AR-15 style rifle broken down in the backpack he was wearing. During the course of the investigation SIKES was interviewed by the FBI and a Texas Ranger. SIKES was Mirandized and he waived his rights. During the interview, SIKES said that he saw a flyer on a Discord chat. As a result of seeing the flyer, he drove to Prairieland Detention Center by himself. (During the investigation, it was determined that SIKES drove his 2009 Black Honda CRV TXLP: BY4G657). SIKES said he did not know anyone else there before he got there. SIKES said he met with the group of people that were there and that he thought that it was just going to be fireworks that were set off. The group of people then walked over to the detention facility and while the fireworks were going off, he heard gunfire behind him, and then he went back toward the vehicles with the other people. It was as he was going back to the vehicles that he was apprehended by police. SIKES stated that the guns were for his protection and that he never pulled one out and never intended to use one of them.

12. During the course of the investigation, it has been determined that Nathan Josiah Baumann ("BAUMANN"), one of the seven arrested in the group referenced above, resides in College Station, Texas and the 2017 White Nissan Rogue TXLP: TXM9235 which was parked in the same area. That is, according to a records check the Nissan Rogue is registered to Joyce Renee Bessent (year of birth 1972) which is an address affiliated with BAUMANN. Bessent is believed to be a relative of BAUMANN. At the time BAUMANN was arrested he appeared to be heading back to his vehicle. According to the Alvarado Police Officer who arrested BAUMANN, he was soaking wet and his clothing was covered with burs (commonly referred to as hitchhikers). It appeared as though BAUMANN had been crawling around in the woods prior to his arrest. (It should be noted that there are wooded areas in and about the area where the shots may have come from.) At the time BAUMANN was booked into the Johnson County Jail, he was in possession of a backpack. An Alvarado Police Officer searched BAUMANN's backpack incident to his arrest. During a search of the backpack, multiple pieces of paper, some of which included what appeared to be flyers were recovered. Additionally, the following items were observed in the backpack: a can of spray paint; pajamas; and a water bottle. BAUMANN said in the back of the patrol car after he was detained that he saw information about the protest on Facebook and that he was there as a part of a "loud protest" and that he did not have any intentions of participating in violence, that he did not know there was going to be any violence, and that he has friends

who are police officers. BAUMANN said he was from College Station, and that was verified from his driver's license information

13. On July 5, 2025, at approximately 2:00 AM CST, Zachary Jared Evetts (EVETTS) was encountered by law enforcement and taken into custody while walking along Highway 67 near Venus, Texas. EVETTS was dressed in black, military style clothing and was a person of interest because he was the registered owner of a red 2016 Mazda CX-5 bearing Texas license plate: NRJ-7521, which was parked at Prairieland Detention Center during and after the encounter. EVETTS was arrested by a Lieutenant with the Venus Police Department. The Lt. with the Venus Police Department stopped EVETTS because he was walking facing the wrong direction which is a violation of Texas transportation code. A high-risk stop was conducted due to the nature of the information received by the Lieutenant and EVETTS complied. Thereafter, another officer arrived, and he was taken into custody by both officers. EVETTS was inventoried incident to arrest for the Texas transportation code violation at which time the officers recovered a black balaclava mask, a pair of tactical style gloves, and a pair of safety goggles. When EVETTS was initially encountered he had a black tactical style shirt around his waste that was also recovered by the officers. An officer asked EVETTS where he was coming from and he said, I do not know, and that he had an identification card in his back pocket. EVETTS address on his identification card was listed on the Texas identification card as in Waxahachie, which was the direction he was walking. In addition, the black GARMIN SOLAR WATCH, SERIAL NUMBER 73H062455,

identified in Attachment A-3, was located on Zachary Jared EVETTS upon his arrest. The GARMIN SOLAR WATCH is now located at the Federal Bureau of Investigation located at One Justice Way, Dallas, Texas, which is located in the Northern District of Texas.

14. The 2003 Silver Subaru Forester, TX license plate RMK7178 with VIN JF1SG63643G757363 (Attachment A-1) shows through TCIC/NCIC checks to be owned and registered to Elizabeth Andrea Soto at 5621 Cowden St., Fort Worth, TX 76114. The vehicle identified in Attachment A-1 was seized from the area of the Prairieland Detention Center and towed to the Alvarado Police Department storage lot, which is located at 600 South Parkway Drive, Alvarado, Texas and is located in the Northern District of Texas.

15. The SAMSUNG CELL PHONE WITH OTTERBOX CASE, IMEI 358163261588218, identified in Attachment A-2, was located on the person of Ines SOTO by Johnson County Sheriff's Department Sergeant Justin Smith on July 5, 2025 at approximately 0030 hours upon his arrest referenced above. The SAMSUNG CELL PHONE is now located at the Federal Bureau of Investigation located at One Justice Way, Dallas, Texas, which is located in the Northern District of Texas.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Internet Protocol Address: An Internet Protocol address ("IP address") is a unique numeric address used by devices on the Internet. Every device attached to the Internet must be assigned a public IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables devices connected to the Internet to properly route traffic to each other. Devices connected to the Internet are assigned public IP addresses by Internet service providers ("ISPs"). There are two types of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). An IPv4 address has four sets ("octets") of numbers, each ranging from 0 to 255, separated by periods (e.g., 149.101.82.209). An IPv6 address has eight groups ("segments") of hexadecimal numbers, each ranging from 0 to FFFF, separated by colons (e.g., 2607:f330:5fa1:1020:0000:0000:0000:00d1).

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

18. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file

does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files and information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic

evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of 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. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies,

transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not

always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

20. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the

loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the

storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

22. I submit that this affidavit supports probable cause for a warrant to search the VEHICLE described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

23. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation

into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Stanley Scott Mitchell
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me on this 8th day of July 2025 at 1:29 a.m./p.m., in Fort Worth, Texas.

JEFFREY L. CURETON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is **2003 SILVER SUBARU FORESTER 4D, TXLP: RMK7178, VIN: JF1SG63643G757363 which is located at the Alvarado Police Department, 600 South Parkway Drive, Alvarado, Texas which is located in the Northern District of Texas and shown below.**

Attachment A

ATTACHMENT B

Property to be seized

1. All records relating to violations of the following: 18 U.S.C. § 111 (Assault on f a Federal Agent); 18 U.S.C. § 1114 (Protection of Officers and Employees of the United States, and Officers Assisting Such an Officer); 18 U.S.C. § 1361 (Damage to Government Property); and 18 U.S.C. § 371 (Conspiracy), those violations involving the following known individuals: Bradford Winston Morris aka Meagan Morris ("MORRIS"); Ines Soto ("I SOTO"), Nathan Josiah Baumann ("BAUMANN"), Elizabeth Soto ("E. SOTO"), Maricela Rueda ("RUEDA"), Seth Edison Sikes ("SIKES"), Joy Abigail Gibson ("GIBSON"), Savanna Batten ("BATTEN"); and Zachary Jared EVETTS, **and other unknown individuals** and occurring on or about July 4, 2025, including:

   a. Any and all firearms, ammunition, fireworks, weapons, and ballistic vests;

   b. Any and all flyers, printed materials, social media posts, and communications concerning: anti-government ideology; over throwing the U.S. Government; anti-law enforcement; interfering with Immigration and Customs Enforcement and/or other law enforcement or government functions;

   c. Any and all notes, plans, training materials, manifestos, and drawings;

   d. Any and all spray paint or other paint material;

e. Any and all receipts, bills, invoices, or similar documents showing the purchase of any of the above items;

f. Any and all contact lists;

g. Any and all text messages, phone logs, instant messages, private messages, emails, voicemails and other forms of electronic communication using a cellular telephone or electronic device;

h. Any and all photographs including still photos, negatives, videos, showing evidence of the aforementioned offenses and that will help identify others involved in the offenses;

i. Any and all location information on the electronic devices and GARMIN SOLAR WATCH;

j. Any and all cellular telephones, laptops, radios, and other communication devices;

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disk drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied 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 FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.