

FILED

UNITED STATES DISTRICT COURT NOV 02 2022

for the District of Nevada

US DISTRICT COURT DISTRICT OF NEVADA

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
ALAMO, NEVADA 89001)
(Attachment A-2))

Case No.

Sp. Atty. Blevins

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 District of Nevada (identify the person or describe the property to be searched and give its location):

See Attachment A-2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before November 16, 2022 (not to exceed 14 days) in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good 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 Honorable Nancy J. Koppe (United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), 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: 11/2/2022 4:15pm

NANCY J. KOPPE Judge's signature

City and state: Las Vegas, Nevada

Hon. Nancy J. Koppe, U.S. Magistrate Judge Printed name and title

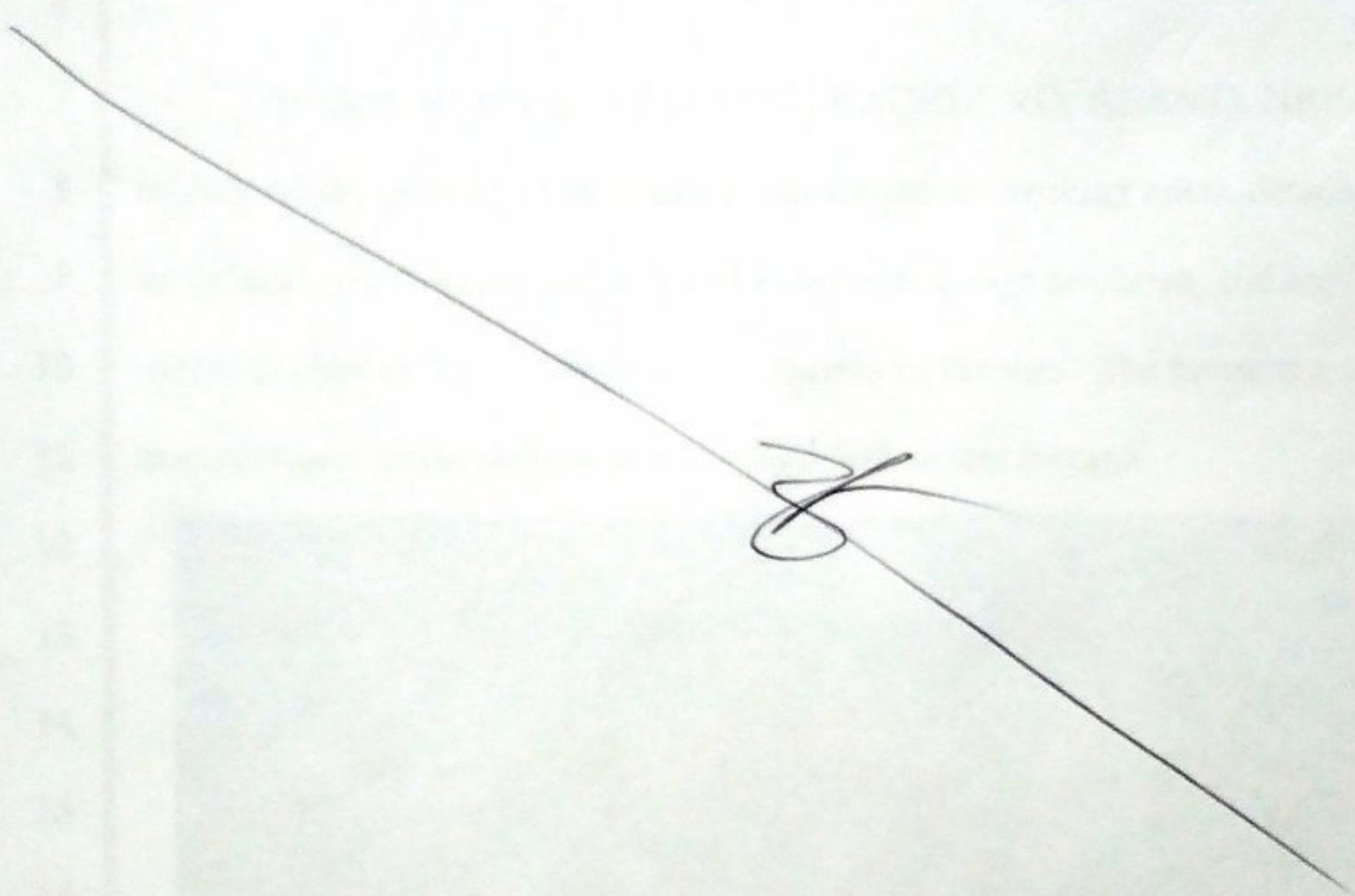
Return

Case No.:	Date and time warrant executed: 11-3-22 9:10 am	Copy of warrant and inventory left with: owner of residence Joerg Arnu
-----------	--	--

Inventory made in the presence of: Brown McAllister

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

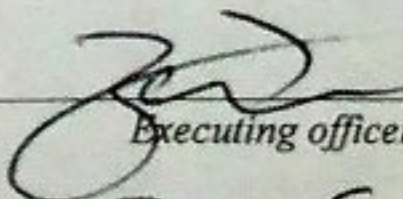
See FD-597



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: 11-3-22


Executing officer's signature
Zach Franklin, FBI Special Agent
Printed name and title

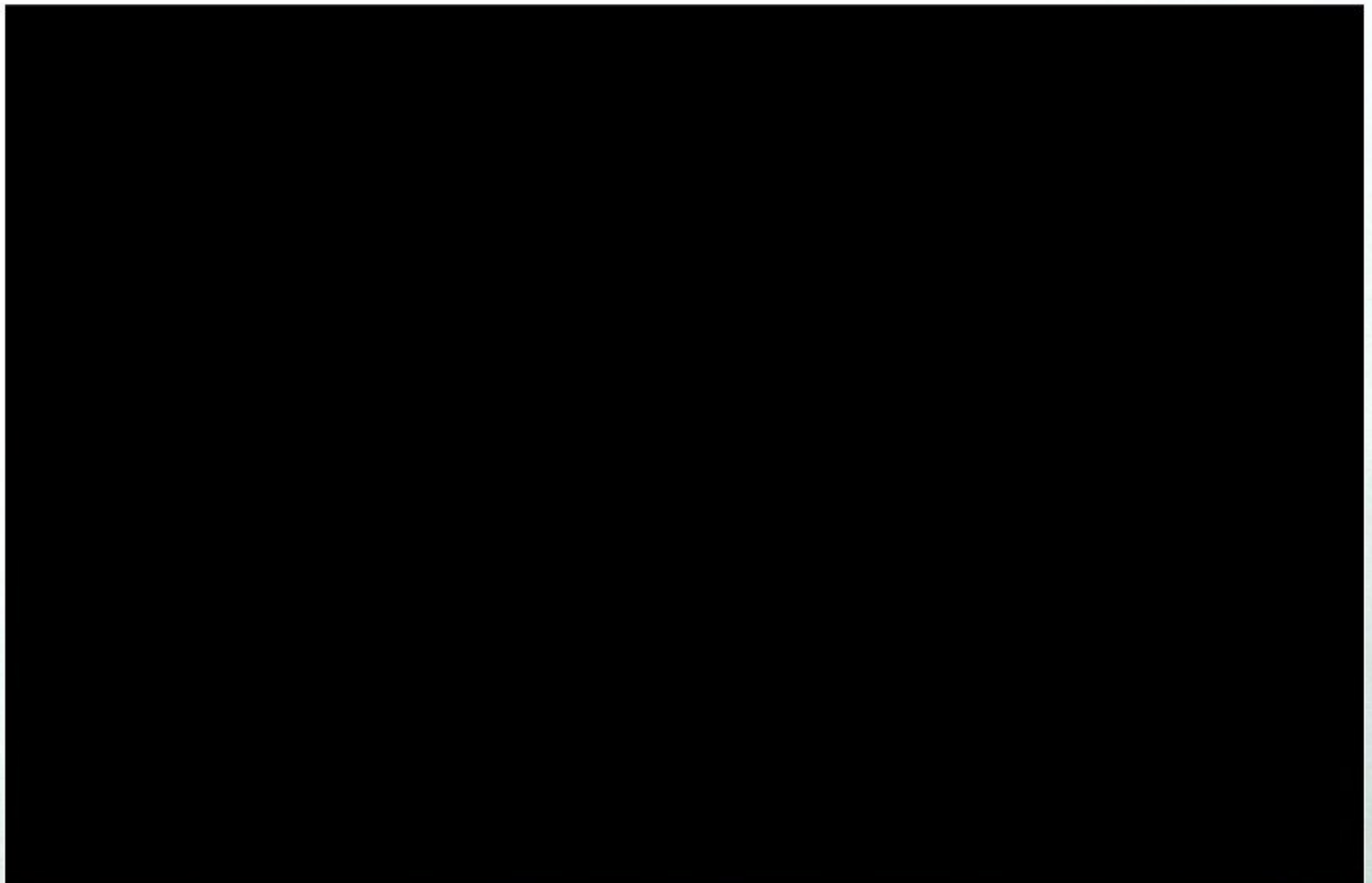
Attachment "A-2"

Page 1 of 2

Description of Property/Premise to be Searched

ALAMO, NEVADA 89001
COUNTY OF LINCOLN,
STATE OF NEVADA

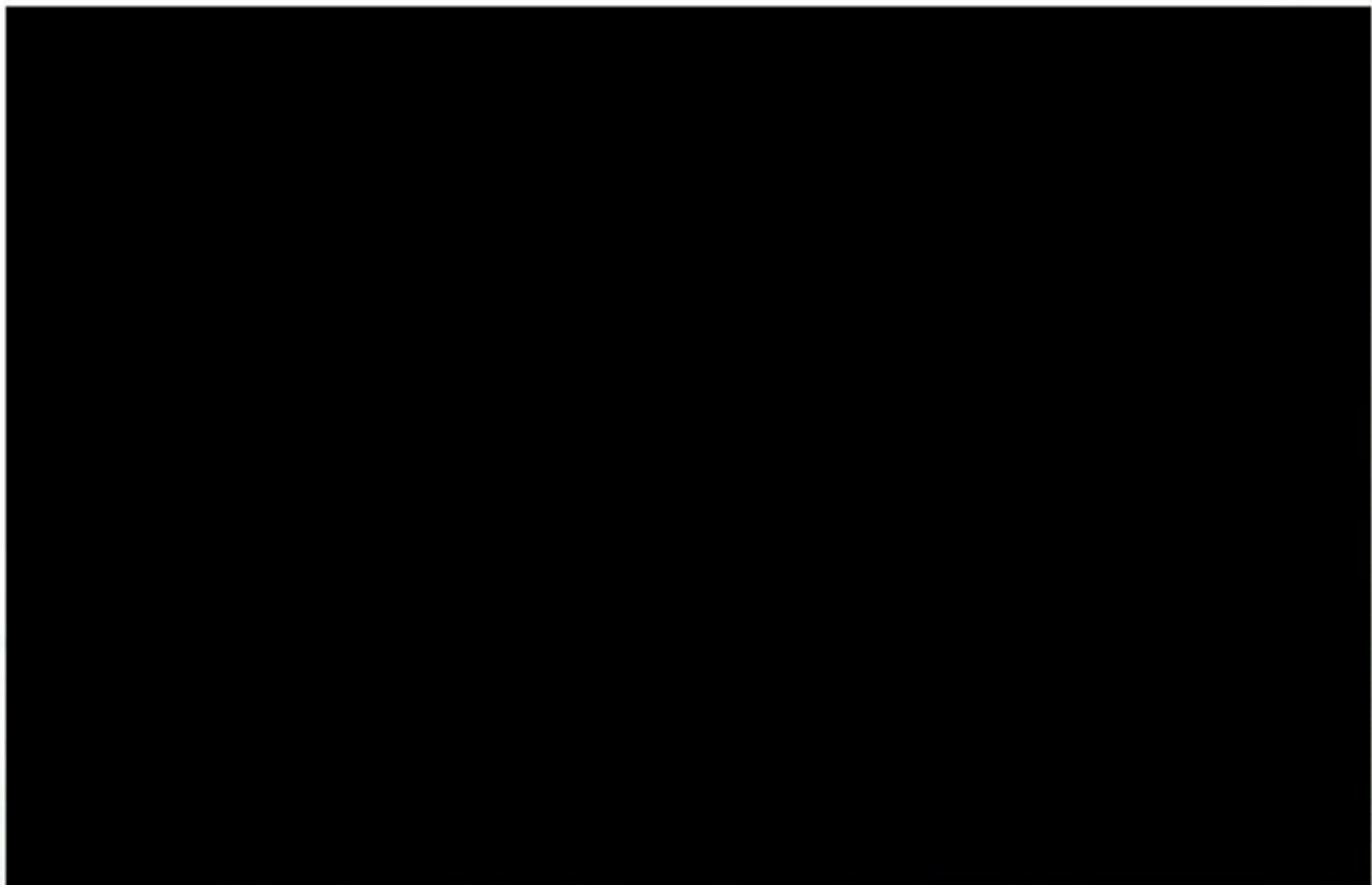
The premise to be searched is ALAMO, NEVADA 89001, to include all its appurtenances, parking areas, outdoor working areas, detached buildings, including and any computing related digital devices or digital media located therein or thereon. The house is a single-family manufactured home with approximately square footage.



Attachment "A-2"

Page 2 of 2

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

Attachment "B"

Particular Things to be Seized

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, 371 (Conspiracy), 18 U.S.C. § 795 (Photographing and Sketching Defense Installations), 18 U.S.C. § 796 (Use of an Aircraft for Photographing Defense Installations), and 18 U.S.C. § 797 (Publication and Sale of Photographs of Defense Installations) (collectively, the "Subject Offenses"), namely:

1. Records and information relating to any military installations in the United States.
2. Records, materials, and documents relating to the operation of military installations, national defense information, and/or classified or unclassified military programs;
3. Records and documents relating to the identity or location of any other known and unknown co-conspirators; and
4. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
5. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;
 - b. evidence of the presence or absence of software that would allow others to control the device, 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 attachment of other devices;
 - d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

1 e. evidence of the times the device was used;

2 f. applications, programs, software, documentation, manuals, passwords,
3 keys, and other access devices that may be necessary to access the device or data stored on the
4 device, to run software contained on the device, or to conduct a forensic examination of the
5 device;

6 g. records of or information about Internet Protocol addresses used by the
7 device.

8 h. As used herein, the terms "records," "information," "documents,"
9 "programs," "applications," and "materials" include records, information, documents,
10 programs, applications, and materials created, modified, or stored in any form, including in
11 digital form on any digital device and any forensic copies thereof.

12 i. As used herein, the term "digital device" includes any electronic system
13 or device capable of storing or processing data in digital form, including central processing
14 units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless
15 communication devices, such as telephone paging devices, beepers, mobile telephones, and
16 smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft
17 Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters,
18 monitors, and drives intended for removable media; related communications devices, such as
19 modems, routers, cables, and connections; storage media, such as hard disk drives, floppy
20 disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding
21 analog tapes such as VHS); and security devices.
22
23
24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment "B". The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment "B". Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out

1 in this protocol beyond those required by binding law. To the extent evidence of crimes not
2 within the scope of this warrant appear in plain view during this review, a supplemental or
3 "piggyback" warrant will be applied for in order to further search that document, data, or
4 other item.

5 4. Once the Search Warrant Data Copy has been thoroughly and completely
6 examined for any document, data, or other items identified in Attachment "B-2" as
7 Information to be Seized, and, if the United States pursues a criminal prosecution in this
8 matter, all litigation including any appeal or collateral attack has been completed, the Search
9 Warrant Data Copy will be sealed and not subject to any further search or examination unless
10 authorized by another search warrant or other appropriate court order. The Search Warrant
11 Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

12 5. The search procedures utilized for this review are at the sole discretion of the
13 investigating and prosecuting authorities, and may include the following techniques (the
14 following is a non-exclusive list, as other search procedures may be used):

15 a. examination of all of the data contained in the Search Warrant Data to view the
16 data and determine whether that data falls within the items to be seized as set forth herein;

17 b. searching for and attempting to recover from the Search Warrant Data any
18 deleted, hidden, or encrypted data to determine whether that data falls within the list of items
19 to be seized as set forth herein (any data that is encrypted and unreadable will not be returned
20 unless law enforcement personnel have determined that the data is not (1) an instrumentality
21 of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully
22 possessed, or (5) evidence of the offenses specified above);

23 c. surveying various file directories and the individual files they contain;

24 d. opening files in order to determine their contents;

- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
- f. scanning storage areas;
- g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment "B"; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment "B."

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than fourteen (14) days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

1 (1) Warrant to Search for and Seize a Person or Property.

2 (B) Inventory. An officer present during the execution of the warrant must prepare and
3 verify an inventory of any property seized. In a case involving the seizure of electronic storage
4 media or the seizure or copying of electronically stored information, the inventory may be
5 limited to describing the physical storage media that were seized or copied. The officer may
6 retain a copy of the electronically stored information that was seized or copied.

7 7. Pursuant to this Rule, the government understands and will act in accordance
8 with the following:

9 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of
10 the warrant, an agent is required to file an inventory return with the Court, that is, to file an
11 itemized list of the property seized. Execution of the warrant begins when the United States
12 serves the warrant on the named custodian; execution is complete when the custodian provides
13 all Search Warrant Data to the United States. Within fourteen (14) days of completion of the
14 execution of the warrant, the inventory will be filed.

15 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which
16 the electronically stored information must be seized after the issuance of the warrant and
17 copied after the execution of the warrant, not the "later review of the media or information"
18 seized, or the later off-site digital copying of that media.

19 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
20 may be limited to a description of the "physical storage media" into which the Search Warrant
21 Data that was seized was placed, not an itemization of the information or data stored on the
22 "physical storage media" into which the Search Warrant Data was placed;

23 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
24 for purposes of the investigation. The government proposes that the original storage media on

1 which the Search Warrant Data was placed plus a full image copy of the seized Search
2 Warrant Data be retained by the government.

3 e. If the person from whom any Search Warrant Data was seized requests the
4 return of any information in the Search Warrant Data that is not set forth in Attachment "B-
5 2", that information will be copied onto appropriate media and returned to the person from
6 whom the information was seized.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

