AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

MARCO ANTONIO AGUAYO,

Defendant(s)

Case No. 2:26-mj-00201-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 12, 2025, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 871	Threat Against the President and Successors to the Presidency

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Marjorie L. Edens, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: January 14, 2026

Judge's signature

City and state: Los Angeles, California

Hon. Alka Sagar, U.S. Magistrate Judge
Printed name and title

AUSA: Robert K. Quealy

AFFIDAVIT

I, MARJORIE EDENS, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Secret Service ("USSS"), and have been so employed since July 2019. I completed the Uniformed Police Training Program (UPTP) at the Federal Law Enforcement Training Center (FLETC) in Artesia, New Mexico, where I received training in Federal Law Enforcement procedures, including interviewing techniques, behavioral analysis, threat assessment, cyber investigations and legal considerations. Following this, I was a Uniformed Division Officer stationed in Washington, D.C. from July 2019 through May 2024. I also completed a 24-week USSS Criminal Investigator Training Course at the James J. Rowley Training Center in Laurel, Maryland, further enhancing my expertise in investigation techniques and federal law enforcement operations, and was appointed as a Special Agent. During my tenure with the U.S. Secret Service as a Special Agent, I served as a member of the Protective Intelligence (PI) squad in the Los Angeles Field Office. In this capacity, I was responsible for identifying, investigating, and assessing potential threats to USSS protectees. My duties included conducting interviews with individuals who had made threatening statements or exhibited concerning behavior toward protectees, as well as evaluating whether such threats meet the threshold for further

investigative or preventive action. As part of my role, I utilized specialized training in threat assessment and behavioral analysis to determine the credibility, intent, and capability of individuals to carry out threats. My work required a thorough understanding of federal laws, investigative procedures, and protective intelligence methodologies

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against, and arrest warrant for, MARCO ANTONIO AGUAYO for a violation of 18 U.S.C 871 (Threat against President and Successors to the Presidency). This affidavit is also made in support of a search warrant for 603 W. Bellevue Drive, Apartment D in Anaheim, California (the "SUBJECT PREMISES") described further in Attachment A-1, and the person of MARCO ANTONIO AGUAYO described further in Attachment A-2, for the items to be seized described in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates and times are on or about those indicated.

III. STATEMENT OF PROBABLE CAUSE

A. Investigators Identify AGUAYO After Pipe Bomb Threat is Posted on Disney's Official Instagram

4. On July 12, 2025, J.D. Vance, the Vice-President of the United States of America, was visiting and staying at the Disneyland Resort in Anaheim, CA.

5. On July 12, 2025, at approximately 6:14 p.m., an Instagram account with the username "@jesses_andamy" posted the following public comments on the official Instagram page for Disney, Inc.:

a. the first comment stated "Pipe bombs have been placed in preparation for J.D. Vance's arrival";

b. a subsequent comment stated "It's time for us to rise up and you will be a witness to it"; and

c. a third comment stated "Good luck finding all of them on time there will be bloodshed tonight and we will bathe in the blood of corrupt politicians".

6. I know from review of subscriber records from META, Inc. ("META"), that Instagram account "@jesses_andamy" is registered to the email address "dumblilboi28@gmail.com." I know from review of subscriber records from Google, Inc. ("Google") that this email address is registered to AGUAYO. Google records further show two phone numbers associated with the account.

7. Review of California Department of Motor Vehicle records for AGUAYO returned the address of the SUBJECT PREMISES.

8. META records show that the Instagram account was registered using an IP address ending in "a83d." I know from open-source information that this IP address is located in Anaheim, California and is operated by T-Mobile USA. META records further show that the Instagram posts were made from an IP address ending "114.50," which I know from open-source records is located in Anaheim, California and operated by Spectrum.

B. Investigators Interview AGUAYO at the SUBJECT PREMISES

9. On July 12, 2025, at approximately 10:54 p.m., I went to the SUBJECT PREMISES with USSS Technical Special Agent David Kim and Sergeant John McClintlock with the Anaheim Police Department.

10. After knocking on the front door, a woman later determined to be AGUAYO's sister, D.P., answered. We requested to speak with AGUAYO who agreed to come to the door and answer questions about threatening statements directed at the Vice President.

11. I questioned AGUAYO outside of the SUBJECT PREMISES regarding the specific Instagram posts. AGUAYO initially denied knowledge of the posts and claimed that his account had been hacked; however, AGUAYO ultimately admitted to making the threatening statements. He claimed that he intended it merely as a joke to provoke attention and laughter. AGUAYO stated he contemplated deleting the post but ultimately forgot to do so.

12. AGUAYO provided verbal and written consent to me to search his mobile device. I reviewed the Instagram application

on this mobile device, which showed AGUAYO logged into four different Instagram accounts, including "@jesses_andamy." I also observed the three threatening Instagram posts on this device. AGUAYO stated his only active social media platforms are Instagram and WhatsApp.

13. AGUAYO provided consent to search his bedroom and closet located within the SUBJECT PREMISES and specifically, his mobile device and a laptop that AGUAYO claimed he shared with his mother.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

14. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the

[1] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures

are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

15. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

16. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress AGUAYO's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of AGUAYO's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

V. CONCLUSION

17. For all the reasons described above, there is probable cause to believe that AGUAYO violated 18 U.S.C. § 871 (Threat against President and Successors to the Presidency).

18. Further, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offense will be found at the SUBJECT PREMISES, as described in Attachment A-1, and on the person of AGUAYO, as described in Attachment A-2.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 14th day of January, 2026.

HONORABLE ALKA SAGAR
UNITED STATES MAGISTRATE JUDGE