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.

SARFRAZ YOUSUF, and
MARC CHAVEZ,

Defendants

Case No. **8:21-mj-00321-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 and between the dates of June 1, 2020, and June 30, 2020, in the county of Orange, in the Central District of California, the defendants violated:

Code Section	*Offense Description*
18 U.S.C. § 641, 2(a)	Theft of Government Property; Aiding and Abetting

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Marc Nelson, 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: May 7, 2021

Karen E. Scott
Judge's signature

City and state: Santa Ana, California

Hon. Karen E. Scott, U.S. Magistrate Judge
Printed name and title

AUSA: Keith D. Ellison (6920)

AFFIDAVIT

I, Marc Nelson, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrants against SARFRAZ YOUSUF ("S. YOUSUF") and MARC CHAVEZ ("CHAVEZ") for a violation of Title 18, United States Code, Sections 641, 2(a) (Theft of Government Property; Aiding and Abetting).

2. This affidavit is also made in support of an application for a warrant to search [redacted], Trabuco Canyon, CA 92679 (the "SUBJECT PREMISES") as described more fully in Attachment A.

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 641 (Theft of Government Property), 1832 (Theft of Trade Secrets), and 1343 (Wire Fraud) (collectively, the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrant, 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.

II. BACKGROUND OF AFFIANT

5. I am a Special Agent with the United States Department of Defense ("DOD"), Office of the Inspector General ("OIG"), Defense Criminal Investigative Service ("DCIS"), in Valencia, California, and have been so employed since April 2019. Prior to my employment at DCIS, I worked as a Special Agent for the Office of Personnel Management, OIG for approximately five years, and as a Senior Investigator with the United States Department of Labor, Employee Benefits Security Administration. I am a graduate of the Criminal Investigator Training Program and the Inspector General Academy at the Federal Law Enforcement Training Center in Glynco, Georgia. I have received specialized training in the investigation of various financial and white collar crimes and I have personally conducted or assisted in the investigation of violations of U.S. law to include conspiracy, theft, mail fraud, wire fraud, health care fraud, and identity theft. In addition, I have received both formal and informal training regarding computer-related investigations and computer technology.

III. SUMMARY OF PROBABLE CAUSE

6. During an investigation into a U.S. Navy employee's unlawful sale of government-controlled technical drawings to a Newport Beach company, Newport Aeronautical Sales Corporation ("NASC"), agents discovered that NASC was also unlawfully obtaining government-controlled technical data -- specifically,

U.S. Air Force Technical Orders -- from the users of a Yahoo e-mail account, S. YOUSUF and INDERA YOUSUF ("I. YOUSUF" and collectively, the "YOUSUFs"). As part of their investigation, agents obtained and reviewed emails sent to and from the YOUSUFs' Yahoo e-mail account. During their review, agents discovered CHAVEZ was also unlawfully acquiring Air Force Technical Orders from the YOUSUFs on behalf of LTC Products, Inc. ("LTC Products") in Trabuco Canyon, California. Between January 2015 and July 2020, CHAVEZ unlawfully acquired at least 1,875 Air Force Technical Orders from the YOUSUFs in exchange for at least $132,280. The YOUSUFs were not authorized to sell the Technical Orders and CHAVEZ was not authorized to receive the Technical Orders.

7. In June 2020, YOUSUF sold 34 Air Force Technical Orders to CHAVEZ, including one marked with Distribution Statement E containing overhaul instructions related to a "Rate Gyro Assembly Flight Control", for $2,170. Knowing the Technical Orders were unlawfully procured outside of official government channels, CHAVEZ paid YOUSUF for the Technical Orders and resold them to customers for a profit.

8. As described herein, LTC Products conducts business at SUBJECT PREMISES, which is also CHAVEZ's primary residence. There is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses will be found within SUBJECT PREMISES.

IV. BACKGROUND ON U.S. AIR FORCE TECHNICAL ORDERS

9. Because public disclosure of technical data is tantamount to providing uncontrolled foreign access, in accordance with 10 U.S.C. § 130, the Secretary of Defense may withhold from public disclosure any technical data with military or space application in the possession of, or under the control of, the DOD, if such data may not be exported lawfully without an approval, authorization, or license. It is DOD policy to provide technical data to qualified U.S. contractors when such data relates to a legitimate business purpose for which the contractor is certified, so long as the provision does not jeopardize an important U.S. technological or operational advantage.

10. Requests for technical data are processed in accordance with DOD Directives and Instructions. FOIA requests are handled in accordance with the procedures set forth in DOD Directives and FOIA requests for technical data determined to be subject to the withholding authority are denied (notwithstanding permitted access by qualified U.S. contractors).

11. Upon receipt of a request for technical data in the possession of, or under the control of, the DOD, the controlling DOD office first determines whether such data is governed by the withholding authority. If so, the controlling DOD office may only authorize release to currently qualified U.S. contractors. Qualified U.S. contractors who receive technical data may only disseminate such data for purposes consistent with their

certification. Accordingly, even qualified contractors who receive such data may not further disseminate such data.

12. The Joint Certification Program ("JCP") certifies Canadian and U.S. contractors for access to unclassified military technical data belonging to Canada's Department of National Defence and to the DOD. This Program helps to protect controlled Unclassified Militarily Critical Technical Data and technology from common adversaries, but allows it to flow to certified Canadian and U.S. companies that have a legitimate need-to-know for business purposes. This program is effective in protecting the competitive edge of North American companies by ensuring that only eligible companies are provided with this data.

13. Based on my investigation into this case and information I have received from the U.S. Air Force, I am aware of the following:

a. U.S. Air Force Technical Orders ("TOs"), also referred to as Technical Order Manuals, are documents which cover installation, operation, maintenance, and handling of Air Force equipment and material.

b. The U.S. Air Force maintains TOs that are not publicly available in the Enhanced Technical Information Management System ("ETIMS") online storage portal.

c. Access to ETIMS is restricted to authorized users for official purposes only. An Air Force Portal account is generally required for ETIMS access.[1]

d. The Air Force Public Sales Office coordinates the release and/or sale of Air Force TOs to qualified defense contractors with legitimate business needs. Qualified defense contractors requesting Air Force TOs must inquire with the Air Force Public Sales Office and explain the specific need in support of the solicitation. Before releasing an Air Force TO, the Air Force Public Sales Office confirms that the requesting defense contractor has an approved DD Form 2345 (Militarily Critical Technical Data Agreement) and a legitimate business need. Subsequent sale of TOs to other defense contractors, whether or not they are qualified, is not a legitimate business need.

e. The DOD uses a document classification system outlined in DOD Instruction 5230.24 (Distribution Statements on Technical Documents) to indicate how broadly technical documents, such as U.S. Air Force TOs, may be distributed based on defined criteria. Pursuant to the instruction, classified and unclassified DOD technical documents are assigned Distribution Statement A, B, C, D, E, or F. Distribution Statement A is assigned to unclassified technical documents that have been cleared for public release. Distribution Statements

[1] Unrelated to the investigation described herein, the Air Force also offers authorized users access to TOs within the ETIMS library through eTools, a software program that can be installed and run on digital devices, such as iPads, to access electronically formatted TOs downloaded to the device. eTools does not require device users to have an Air Force Portal account.

B, C, D, E, and F are assigned to technical documents with distribution restrictions. The applicable restrictions increase with each subsequent letter, with Distribution Statement F -- applied under rare and exceptional circumstances -- providing for the most restrictions ("Further dissemination only as directed by [the controlling DoD office] or higher DoD authority").

V. STATEMENT OF PROBABLE CAUSE

A. Background of Investigation

14. After discovering that a U.S. Navy civilian engineer was emailing government-controlled technical drawings related to military weapons systems to his prior cohabitant's Gmail account, agents investigated further and discovered the civilian engineer was unlawfully selling the technical drawings to NASC, an international supplier of aerospace technical data located in Newport Beach, California. NASC then sold the stolen drawings to customers inside and outside of the United States.

15. As a result of that investigation, on October 2, 2020, the government charged four individuals -- including NASC employees George MacArthur Posey IV ("Posey") and Dean Mirabal ("Mirabal") -- with one count of conspiracy to steal government property and receive stolen government property, in violation of Title 18, United States Code, Section 641, and to commit bribery of a federal public official, in violation of Title 18, United States Code, Section 201(b)(1)(C) and (b)(2)(C), as well as with three counts of receiving stolen government property. United

States v. Fitting, et al., No. 8:20-CR-591-DOC, ECF No. 48 (C.D. Cal. Oct. 2, 2020).

B. Identification of mroadvisor@yahoo.com

16. As part of the investigation described above, on February 10, 2020, the Honorable Jacqueline Chooljian, United States Magistrate Judge, Central District of California, authorized a warrant pursuant to 18 U.S.C. § 2703 for information associated with certain NASC email accounts, including the NASC email accounts of Posey (mac@newportaero.com) and Mirabal (dean@newportaero.com), in case number 2:20-MJ-00590. Of particular note, the warrant authorized the seizure of information related to the acquisition, transfer, or sale of U.S. Government technical drawings or manuals.

17. During a review of information obtained pursuant to the warrant, agents discovered that the Yahoo e-mail account mroadvisor@yahoo.com[2] was being used for the sale of U.S. Air Force TOs to NASC.

18. The earliest observed e-mail from mroadvisor@yahoo.com was to Mirabal on approximately February 2, 2015, and read: "Hello, Yousuf just spoke to me and say you might be interested in new source for T.O….Thank you Mandy". Mirabal forwarded the email to Posey the next day.

19. On February 3, 2015, Posey replied to mroadvisor@yahoo.com: "Mandy, Dean informed me you may have

[2] I believe that the letters "mro" in the email address are an acronym commonly used in the aerospace industry for maintenance, repair, and overhaul.

access to TOs. Can you please elaborate on what you have available? Delivery and cost? Thank you"

20. That same day, the user of mroadvisor@yahoo.com replied: "Hi Mac, Thank you for your interest. I have direct access to the Air Force Portal to which I get the absolute latest revisions to T.O.'s!! I GUARANTEE you the latest revision sent electronically at the time of request once it is not a restricted one!...95 for oh/ipl 80 for oh only 50 for ipl only…Give me a try!! Hope to hear from you soon. Mandy"

a. Based on my background, training, experience, and investigation in this case, I believe the YOUSUFs, using the alias "Mandy," informed Posey that they had access to U.S. Air Force TOs maintained within ETIMS ("I have direct access to the Air Force Portal") and offered to sell NASC TOs for $95, $80, or $50 depending on overhaul ("oh") and illustrated parts lists ("ipl") ("95 for oh/ipl 80 for oh only 50 for ipl only").

C. Identification of S. YOUSUF and I. YOUSUF as the Users of mroadvisor@yahoo.com

21. During my review of emails sent from mroadvisor@yahoo.com to NASC employees, I observed that the sending name[3] associated with the account was Taradai Arjune ("T. Arjune"). I queried the name T. Arjune in CLEAR[4] and learned that T. Arjune is a sixty-eight year old female who resides in

[3] Based on internet queries, I am aware that a sending name is the name a recipient sees when an email is sent from a Yahoo email, rather than displaying the actual email address.

[4] Thomson Reuters' CLEAR software provides law enforcement with the ability to search numerous public information databases for records associated with names, addresses, telephone numbers, and other identifying information.

Miramar, Florida, at [redacted] (the "Miramar residence"). Further queries also associated Surjmohan Arjune ("S. Arjune"), a sixty-nine year old male, S. YOUSUF, and I. YOUSUF with the Miramar residence. I queried the Miramar residence in Google Maps and observed that it appears to be a single-family home in a residential neighborhood.

22. I reviewed Florida Division of Corporations online records and learned that the Miramar residence is listed as the principal address for Aerospace Parts Source, LLC. S. YOUSUF is listed as the registered agent for the company. The Miramar residence is also listed as the principal address for Corporate Sanitation, LLC and United Sanitation, LLC. S. YOUSUF is listed as the registered agent for both companies.

23. I also reviewed e-mails between mroadvisor@yahoo.com and NASC employees that included references to PayPal and attached invoices related to the sale of TOs. I reviewed PayPal records for a PayPal account associated with mroadvisor@yahoo.com. The records list the accountholder as I. YOUSUF and the Miramar residence as an address affiliated with the account.

24. I reviewed Florida Department of Highway Safety and Motor Vehicle records for I. YOUSUF and S. YOUSUF, which reflect that I. YOUSUF is a 40-year-old female, S. YOUSUF is a 43-year-old male, and both reside at the Miramar residence.

25. Based on my review of the PayPal records, I learned that funds received into the PayPal account were transferred into two Chase Bank accounts. I reviewed records for those

accounts, which identified the account holders as I. YOUSUF (for one of the accounts) and S. YOUSUF (for the other). The address of record for both accounts is the Miramar residence.

26. During my review of the Chase Bank records for S. YOUSUF's account, I noticed that S. YOUSUF received regular deposits -- consistent with payroll deposits -- from Summit Aerospace, Inc. During my review of NASC employee emails discussed above, I discovered an email from sarfraz.yousuf@summitmro.com to Mirabal dated August 18, 2014, reading: "Hi Dean, I'm working at Avionics International now. Would you have the subject T.O.? Thank (sic) Sean". The signature block lists "Sarfraz Yousuf, Quality Control Manager" and both Summit Aerospace and Avionics International.[5]

27. On October 11, 2017, the user of mroadvisor@yahoo.com e-mailed both Mirabal and Posey: "Good morning, 6J3-4-24-13: 14 Mar 2017. Available… 6J3-4-24-14: 01 Apr 2009. Available…" The email contained an attached Microsoft Excel file titled "Copy of MANDY TO List.xlsx". The document properties for the file reflect that "Sarfraz Yousuf" was the last person to save the file.

28. Based on my investigation, I believe S. YOUSUF and I. YOUSUF are the users of mroadvisor@yahoo.com.

[5] Based on my review of the first email sent from mroadvisor@yahoo.com to Mirabal, as discussed in paragraph 18 above, I suspect that Mirabal had a pre-existing relationship with S. YOUSUF ("Yousuf just spoke to me and say you might be interested in new source for T.O….Thank you Mandy") that may have facilitated the unlawful business relationship with NASC.

D. S. YOUSUF used ETIMS to Unlawfully Access TOs

29. I reviewed a DD Form 2345 (Militarily Critical Technical Data Agreement) for Summit Aerospace, Inc. on file with the Defense Logistics Agency ("DLA").

30. The form was signed by the contractor on approximately June 23, 2017, and accepted by the DOD on approximately July 13, 2017. The form lists S. YOUSUF as the Data Custodian for Summit Aerospace, Inc. According to the instructions for filling out a DD Form 2345, the Data Custodian is a representative for the contractor who receives military technical data and assumes responsibility for its further dissemination. The form also describes the relevant business activity of Summit Aerospace, Inc. as follows: "Specializing in the repair of CSD, IDG, Generators, Hydraulic, Pneumatic, APU's, Landing Gears, Avionics, Instruments, Rewind of Electrical mechanical parts such as Rotors, Stators, and exciters."

31. Based on my review of Air Force records, I am aware that the Air Force issued S. YOUSUF accounts to access the Air Force Portal and ETIMS for authorized purposes pursuant to his employment for Summit Aerospace, Inc. Based on information I have received from Air Force personnel, I am aware that S. YOUSUF would first have to log in to the Air Force Portal prior to logging in to ETIMS. Each time S. YOUSUF logged in to the Air Force Portal, he was required to acknowledge a warning banner advising, in part, "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only."

32. During my review of DLA and DOD records, I was unable to locate any accounts or records associated with I. YOUSUF.

33. As previously discussed, I reviewed e-mails between mroadvisor@yahoo.com and NASC employees that included references to PayPal and attached invoices related to the sale of TOs. I also reviewed e-mails between mroadvisor@yahoo.com and CHAVEZ's email, mchavez@ltc-products.com, as discussed further below, and another suspected customer, that also contained references to PayPal and attached invoices related to the sale of TOs. Those invoices listed TO numbers and the prices charged for the TOs by the YOUSUFs.

34. Agents provided Air Force personnel with a list of 51 Air Force TO numbers identified in invoices the YOUSUFs sent to their customers in or around June 2020. Air Force personnel responded with accessibility information for 50 of the TOs -- one of the TOs was not active (superseded status). Specifically, Air Force personnel provided agents with an Excel spreadsheet that included the ETIMS account number for all accounts that had access to each of the 50 TOs. ETIMS account number "E*05KM" had access to all 50 of the active TOs. No other ETIMS account had access to all 50.

35. To receive access to Air Force TOs, a contractor must complete and submit an Air Force Technical Order ("AFTO") Form 43. I reviewed an AFTO Form 43 for ETIMS account number "E*05KM", and discovered the account belongs to S. YOUSUF. The form indicated that S. YOUSUF requested access in March 2013 related to his employment with Kellstrom Repair Services, Inc.,

a U.S. contractor with a government contract. On April 28, 2017, S. YOUSUF requested a revision to his account updating his employer to Summit Aerospace, Inc. S. YOUSUF's ETIMS account is subscribed to approximately 10,870 TOs.

36. According to Air Force personnel, when access to a TO requires sponsor approval, the TO Manager ("TOMA") must first approve a request from the ETIMS user account before access is granted. Once the TOMA approves access, the ETIMS user receives instant access to the digital version of the TO as well as notifications whenever the TO is updated. Of the 51 TOs that were provided to the Air Force for verification, 46 required sponsor approval.[6]

37. Because S. YOUSUF accessed the 51 TOs after inquiries for those TOs from customers, including CHAVEZ, I do not believe that S. YOUSUF accessed the TOs as part of his job at Summit Aerospace, Inc. Based on my review of Air Force records and my investigation in this case, I believe S. YOUSUF used his access to ETIMS to access Air Force TOs, converted the TOs to his own use, and then sold the TOs to various entities, including NASC and LTC Products.

E. CHAVEZ Purchases Stolen TOs from the YOUSUFs

1. Identification of CHAVEZ and LTC Products

38. On October 15, 2020, the Honorable Alexander F. MacKinnon, United States Magistrate Judge, Central District of California, authorized a warrant pursuant to 18 U.S.C. § 2703

[6] It is possible that S. YOUSUF subscribed to some of the TOs requiring sponsor approval at a time when they did not require sponsor approval.

for information associated with the YOUSUFs' Yahoo e-mail account (mroadvisor@yahoo.com), in case number 2:20-MJ-04987.

39. During a review of the information obtained pursuant to the warrant, agents identified at least 897 e-mails sent from mchavez@ltc-products.com to mroadvisor@yahoo.com. In general, those e-mails related to the availability and currency of TOs. mchavez@ltc-products.com also received at least 372 e-mails from mroadvisor@yahoo.com, some of which contained TOs that were not releasable outside of the DOD.

40. The signature line included in emails from mchavez@ltc-products.com listed "LTC Products, Inc." and the address [redacted] Trabuco Canyon, California 92679 (the SUBJECT PREMISES). In their emails, the YOUSUFs addressed the user of mchavez@ltc-products.com as "Marc".

41. I reviewed California Secretary of State records for LTC Products, Inc. The records indicate that the company was incorporated in August 2005 and list the business address as the SUBJECT PREMISES. CHAVEZ is named as the company's Chief Executive Officer and Chief Financial Officer.

42. I reviewed documents from Proofpoint, Inc. ("Proofpoint")[7] indicating that Proofpoint provided services related to the web address http://ltc-products.com, and the subscriber address was the SUBJECT PREMISES.

[7] Proofpoint, Inc. is an enterprise security company based in Sunnyvale, California, that provides software as a service and other products for email security.

43. I reviewed Chase Bank records for accounts belonging to LTC Products and CHAVEZ. Both accounts list the SUBJECT PREMISES as the address for the account holder.

44. Based on my investigation, I believe CHAVEZ is the user of mchavez@ltc-products.com.

45. I reviewed a screen capture of LTC Products' website (ltc-products.com/about_us.html) taken on August 24, 2018, which included the following description of the company: "LTC Products, Inc. was created in order to meet the demand of the Aviation and Aerospace community for both Aircraft parts and Technical Data. We have an extensive library of commercial, private and military component repair manuals that cover popular aircraft such as the Boeing, Douglas, Airbus, and Cessna models to name a few."

46. During my review of DLA and DOD records, I was unable to locate any active accounts or records associated with CHAVEZ or LTC Products. As described below, however, I did locate DLA records indicating CHAVEZ previously served as the Data Custodian for a defense contractor.

2. CHAVEZ Pays the YOUSUFs for TOs via PayPal

47. I reviewed PayPal records for a PayPal account associated with CHAVEZ. The records list the accountholder as CHAVEZ, the business as "LTC Products, Inc." and the address associated with the account as the SUBJECT PREMISES. Between January 2015 and July 2020, the CHAVEZ PayPal account sent approximately $132,280 to I. YOUSUF's PayPal account (discussed above).

48. Based on my investigation in this case, I believe that CHAVEZ sent the money to the YOUSUFs in exchange for the unlawful purchase of TOs. Based on my review of email correspondence and financial records, I believe that between January 2015 and July 2020, CHAVEZ, unlawfully purchased at least 1,875 TOs from the YOUSUFs in exchange for at least $132,280.

3. June 2020 Sale of Air Force TOs to CHAVEZ

49. On July 1, 2020, the YOUSUFs' Yahoo e-mail account e-mailed CHAVEZ's e-mail account: "Marc, than (sic) you so much for June purchase (sic). Invoice attach (sic) and a Pay-Pal will follow shortly…Mandy." An invoice referencing approximately 34 TOs sold by "Mandy" to CHAVEZ and a total amount due of $2,170 was attached.

50. I reviewed the 34 TOs referenced in the invoice from the YOUSUFs and provided the TO numbers to Air Force personnel along with 17 others identified from additional invoices as discussed in paragraph 34 above. All 34 TOs were marked with distribution restrictions as follows: 3 were marked Distribution Statement B, 20 were marked Distribution Statement C, 6 were marked Distribution Statement D, and 5 were marked Distribution Statement E.

51. One of the referenced TOs was "5A11-2-77-3 3 JUN 2019". The invoice noted that TO 5A11-2-77-3 3 JUN 2019 was sold on "06.23" -- referring to June 23, 2020 -- for a price of $70.00.

52. On June 23, 2020, CHAVEZ received an e-mail from an LTC Products customer that said, “Hi Marc, I need manual forP/N (sic) 16C0705-3…T.O. 5A11-2-77-8-1 CAN YOU ASSIST?..”

53. Shortly thereafter, CHAVEZ e-mailed the YOUSUFs’ Yahoo e-mail account “5A11-2-77-2 We have July/2017” and “5A11-2-77-3 – We have July/2017”. The subject line of the email read “Currency”.

54. That same day, the YOUSUFs’ Yahoo e-mail account sent CHAVEZ’s e-mail account an e-mail with TO “5A11-2-77-3 3 JUN 2019” attached, noting that the July 2017 revision of TO 5A11-2-77-2 was “current”.

55. I reviewed the June 2019 revision of TO 5A11-2-77-3, which is a technical manual with overhaul instructions for a “Rate Gyro Assembly Flight Control.” The cover page is marked with “DISTRIBUTION STATEMENT E – Distribution authorized to DoD components only, direct military support, 24 March 2011. Other requests for this document shall be referred to OO-ALC/416 SCMS/GUBAB, Hill AFB, Utah 84056-5826.”[8] The cover page also provides a warning that the “document contains technical data whose export is restricted by the Arms Export Control Act”, “[v]iolations of these export laws are subject to severe criminal penalties”, and to “[d]isseminate in accordance with provisions of DoD Directive 5230.25”.

[8] Distribution Statement E applies to documents “contain[ing] export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operational military advantage of the United States, another country, or a joint U.S.-foreign program.” DOD Instruction 5230.24.

56. On June 30, 2020, the same LTC Products customer e-mailed CHAVEZ, “Hi Marc, I need T.O. for P/N 16C0705-3 T.O. 5A11-2-77-3 can you assist?...” CHAVEZ replied several minutes later, “We will send”. Later that day, CHAVEZ sent the customer an e-mail with three attachments, including T.O. 5A11-2-77-3 and an invoice referencing a “SERVICE CHARGE” in the amount of $150.

57. CHAVEZ also sold TO 5A11-2-77-3 3 to another LTC Products customer on approximately August 13, 2020.

58. Agents reviewed I. YOUSUF’s PayPal account records and identified a $2,170 payment from CHAVEZ’s PayPal account on July 7, 2020. The records reflected several retail transactions made using I. YOUSUF’s PayPal account after July 7, 2020, and, on July 20, 2020, a transfer of $4,300 to the Chase Bank account belonging to S. YOUSUF.

59. The PayPal records also included an activity log, identifying the IP address[9] that was used to access the account at certain points in time. On July 20, 2020, IP Address 73.179.26.183 was used to access the account. According to

[9] An IP address is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Many companies control a range or a block of IP addresses. A single IP address can manage Internet traffic for more than one computer or device, such as when a router in one’s home routes traffic to one’s desktop computer, as well as one’s tablet or smartphone, while all using the same IP address to access the Internet. A newer system used by some computers or networks, referred to as IP version 6, serves the same function and uses a longer value that is a combination of numbers and letters (allowing for more addresses).

Comcast records, on July 20, 2020, at the time of the PayPal login, IP address 73.179.26.183 was attributable to the Miramar residence.

60. Because S. YOUSUF accessed the 34 TOs sold to CHAVEZ in June 2020, including TO 5A11-2-77-3, pursuant to inquiries from CHAVEZ, I do not believe he had a legitimate business need to access the TOs as part of his employment. Because the subsequent sale of TOs to others, whether or not they are qualified defense contractors, is not a legitimate business need, I believe that S. YOUSUF converted the TOs to his own use. Moreover, because DOD records do not identify I. YOUSUF or CHAVEZ as qualified recipients of government technical data, I do not believe they were authorized to access or receive the TOs, including TO 5A11-2-77-3.

F. CHAVEZ is Aware of the Appropriate Process to Procure Military Technical Data

61. According to California Secretary of State records, CHAVEZ was previously associated with Coastal Aeronautical, Inc., a now-suspended corporation. Coastal Aeronautical, Inc. was incorporated on October 29, 1992, and CHAVEZ was the agent for service of process. The last corporate filing was on November 6, 2000.

62. According to DLA records, which are publicly available online, Coastal Aeronautical, Inc. was a JCP certified contractor until November 15, 2006. Because DLA only maintains a contractor’s DD Form 2345 (Militarily Critical Technical Data Agreement) for five years after JCP certification expires, DLA

no longer has the DD Form 2345 for Coastal Aeronautical, Inc. But DLA's online database listing JCP certified contractors includes records for previously certified contractors, including Coastal Aeronautical, Inc. I reviewed those records, which name CHAVEZ as the corporation's point of contact. Based on information provided to me by DLA and my review of Summit Aviation, Inc.'s DD Form 2345, I am aware that the point of contact listed in DLA's online database is the Data Custodian for the certified contractor as provided on the DD Form 2345. Thus, I believe CHAVEZ was the Data Custodian for Coastal Aeronautical, Inc., and, in that role, assumed responsibility for the dissemination of military technical data.

63. Based on my conversation with an individual previously associated with NASC, I am aware that CHAVEZ was employed by NASC in the early 1990s.[10] In that capacity, CHAVEZ was involved with the receipt and dissemination of military technical data and familiar with the relevant distribution restrictions.

64. During my review of CHAVEZ's emails, I observed several instances in which CHAVEZ was notified about and/or demonstrated his knowledge of Distribution Statements and the restrictions placed on dissemination of military technical data.

[10] I interviewed this individual as part of my investigation in this case. The individual's attorney was present during the interview. The individual has not been charged with a crime but does have a prior conviction related to the unlawful dissemination of military technical data. To the extent possible, agents have corroborated the information provided by the individual and are not aware of any false or misleading information provided by the individual.

a. For example, on January 22, 2020, CHAVEZ e-mailed an LTC contact[11] based in Addison, Texas, asking, "Any Chance you have access to this one?" referring to an attached image with "DMWR 11-6615-306". Later that day, the contact replied, "I submitted a request for this specific manual to CECOM[12] yesterday and received the following response this morning: '[redacted] I have received your request for, DMWR 11-6615-306, NIIN's 013162743 and 015382841. The distribution statement on these are Distribution Statement D; limited to Department of Defense and U.S. DoD Contractors only. In order to obtain a copy of these you must hold a current contract to perform Depot level maintenance for the Government, if this is the case you may obtain a copy from your contracting officer…'" The e-mail contained a signature block for a Government Information Specialist assigned to U.S. Army Materiel Command Legal Center, APG Office of the Chief Counsel. CHAVEZ replied, "Okay thanks".

b. That same day, CHAVEZ –- appearing to copy and paste the response from the Texas contact -- e-mailed another LTC customer, "I submitted a request for this manual to CECOM and received the following response: Dear Sirs, I have received your request for, DMWR 11-6615-306, NIIN's 013162743 and 015382841. The distribution statement on these are Distribution

[11] Based on my review of emails between CHAVEZ and the LTC contact, I believe that CHAVEZ provides the contact with Air Force TOs in exchange for Army Technical Data, specifically Depot Maintenance Work Requirements ("DMWR"), that the contact appears to have access to.

[12] I believe CECOM is a reference to the U.S. Army Communications-Electronics Command.

Statement D; limited to Department of Defense and U.S. DoD Contractors only. In order to obtain a copy of these you must hold a current contract to perform Depot level maintenance for the Government, if this is the case you may obtain a copy from your contracting officer."

c. In another instance, on July 15, 2020, CHAVEZ received an email from a prospective customer inquiring about the availability of two TOs. In response, CHAVEZ noted that he could provide the customer with one of the TOs for $125, noting that the second was restricted, but that he would need "a copy of [the prospective customer's] DD form 2345 for the purchase of T.O.'s".

i. Notably, neither CHAVEZ nor LTC Products were qualified government contractors with an approved DD Form 2345 or a legitimate business need to obtain or disseminate military technical data. Moreover, the sale of military technical data is never considered a legitimate business need so CHAVEZ could not have disseminated it to his customers for that purpose even if CHAVEZ and/or the customer were otherwise authorized to receive the information.

65. For the foregoing reasons, I believe that CHAVEZ was aware of, and disregarded, the restrictions placed on the dissemination of military technical data when he unlawfully purchased and sold TO 5A11-2-77-3.

///

///

G. CHAVEZ and YOUSUF Respond to the Arrest of NASC Employees

66. Shortly after the arrest NASC employees Mirabal and Posey, discussed above, became public on September 2, 2020, CHAVEZ and the YOUSUFs appeared to communicate by phone for the first time in seven months.

67. Agents identified an email from CHAVEZ to the YOUSUFs dated May 3, 2017, in which CHAVEZ provided his cell phone number, "[redacted]", to "talk about other sources" and "to make sure [they] don't lose track of each other." CHAVEZ also asked for the YOUSUFs' cell phone number. In response, the YOUSUFs provided "cell #[redacted]".

68. I reviewed call records for the YOUSUFs' phone number (ending 9140) and observed four calls and two text messages between the YOUSUFs and CHAVEZ on September 3, 2020. Prior to that date, there did not appear to have been any communication between those phone numbers since February 6, 2020. Based on the timing of the communications, as well as the extended period of time without communication, I suspect that CHAVEZ and the YOUSUFs contacted each other to discuss the arrest of the NASC employees.

69. CHAVEZ and the YOUSUFs again communicated by phone calls and text messages on December 1, 2020, the most recent date for which I have phone records. Based on my investigation in this case, including my review of several years' worth of emails between the YOUSUFs and CHAVEZ, I do not believe that the YOUSUFs and CHAVEZ maintained a personal or business

relationship other than for the purposes of selling unlawfully obtained TOs. Therefore, I believe they likely communicated regarding their past criminal activities and their attempts to conceal their conduct from law enforcement (as described further below).

1. CHAVEZ Attempts to Cover for the Unlawful Sale of Military Technical Data

70. Shortly after the arrest of the NASC employees, CHAVEZ reached out to various LTC Products customers to inquire about the status of the customers' respective DD Form 2345s. For example, on September 29, 2020, CHAVEZ e-mailed a LTC Products customer, "Hi Laura, I hope all is well. We are updating our records and wanted to see if we can get an updated DD Form 2345 (Militarily Critical Technology Data Agreement). Please let us know when you can…" The next day, the customer replied, "Sorry, ours expired." After CHAVEZ responded, "Yes I know we are looking for an updated copy," the customer added, "Good answer. We used to keep current, then restrictions got tight many years ago. That's why we started contacting you, because you could get these documents. If we had a current DD2345, we would not have to contact you." Based on my review of publicly available DLA records, I believe the customer's JCP certification is current. However, based on the expiration date of the customer's JCP, I believe their JCP became current in approximately November 2020. Agents also identified an e-mail on November 12, 2020, where the customer said, "Please see attached, as per your request. Thanks for your help…" The e-

mail contained the DD Form 2345 for the customer, which was accepted on November 12, 2020.

a. As noted above, it is irrelevant whether the customer had a current JCP certification as CHAVEZ was not authorized to possess or disseminate restricted military technical data.

71. Agents also identified an e-mail chain in which CHAVEZ stated that LTC Products was not required to comply with the JCP certification process. On November 11, 2020, a potential LTC Products customer sent an e-mail to CHAVEZ reading, “Mr. Chavez, We have been contacted by one of our clients regarding a contract with our company and they have mentioned you as a vendor that we may be able to utilize. In order to set up this relationship between our companies I would need to have some information from you. Please complete the attached form and provide me with your JCP certification number and your DDTC registration?” CHAVEZ replied, “Hi Tracy, I have attached your form. None of these applies to us but I filled it out for you.” When the prospective customer asked “Do you have a JCP certification number and a DDTC ITAR registration?”, CHAVEZ replied, “No we would need your DD form 2345”.

72. Additionally, CHAVEZ continued to sell TOs without authorization after September 2, 2020. For example, on December 9, 2020, CHAVEZ e-mailed an LTC customer an Air Force TO (15X4-3-22-3) that was marked with Distribution Statement D, along with an invoice in the amount of $150.

2. The YOUSUFs Delete Their Emails

73. Prior to the October 2020 issuance of the warrant pursuant to 18 U.S.C. § 2703 for information associated with the YOUSUFs' Yahoo e-mail account, agents sent the email provider a preservation letter on August 19, 2020. When agents received the information responsive to the search warrant, they discovered two sets of information. Both sets indicated a requested start date of February 1, 2015, but the first set indicated it was compiled on August 20, 2020, a day after the date of the preservation request, while the second set indicated it was compiled on October 15, 2020, around the time the warrant was served. Based on my review of the information, I am aware that the second set did not include any emails that took place prior to September 15, 2020, while the first set included regular email communications as far back as June 2015, indicating that the account information was deleted on or around September 15, 2020. Accordingly, based on my review of the information and the September 2020 communications between CHAVEZ and the YOUSUFs, I believe that the YOUSUFs attempted to delete the contents of the Yahoo email account to conceal their criminal activity.

H. Evidence, Fruits, and Instrumentalities of the Subject Offenses will be found in the SUBJECT PREMISES

74. As previously discussed, the address of record associated with LTC Products is the SUBJECT PREMISES. In addition, I reviewed California DMV records listing the SUBJECT PREMISES as the address of record for CHAVEZ. DMV records also

indicate both CHAVEZ and LTC Products have vehicles registered to the SUBJECT PREMISES. Accordingly, I believe that CHAVEZ resides at the SUBJECT PREMISES where he operates LTC Products.

75. Agents conducted surveillance in the vicinity of SUBJECT PREMISES on April 2 and 6, 2021. During the periods of surveillance, agents' observations indicated that CHAVEZ continues to reside at the SUBJECT PREMISES. Relevant events from the surveillance are as follows:

a. On April 2, 2021, between approximately 2:00 p.m. and 3:05 p.m., an agent saw two vehicles parked in the driveway of the SUBJECT PREMISES and a third parked on the street. All three of the vehicles were registered to CHAVEZ at the SUBJECT PREMISES. There were an additional three vehicles parked on the street that were not registered to CHAVEZ.

b. On April 6, 2021, an agent arrived in the vicinity of the SUBJECT PREMISES at around 6:10 a.m. and saw what appeared to be four of the six vehicles previously observed parked in the driveway or near the SUBJECT PREMISES. At approximately 9:31 a.m., a male matching the physical appearance of, and believed to be, CHAVEZ departed the SUBJECT PREMISES and took a dog for a walk. He returned a couple of minutes later and carried trashcans from the street onto the property.

76. Because CHAVEZ uses the SUBJECT PREMISES as the principal business address for LTC Products as well as the address of record for bank accounts for both himself and LTC Products, as discussed above, I believe that, amongst other items, financial and business records associated with the

Subject Offenses will be located at the SUBJECT PREMISES. Because CHAVEZ communicated with the YOUSUFs by phone and email, I further believe that the digital devices CHAVEZ used for such communications will be located at the SUBJECT PREMISES.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[13]

77. 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 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.

[13] 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.

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, email, 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.

78. 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.

79. 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.

c. 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 CHAVEZ's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of CHAVEZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

80. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

81. For all the reasons described above, there is probable cause to believe that YOUSUF and CHAVEZ have committed a violation of Title 18, United States Code, Sections 641, 2(a) (Theft of Government Property; Aiding and Abetting).

82. 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 Offenses will be found in the SUBJECT PREMISES, as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 7th day of May, 2021.

Karen E. Scott

HONORABLE KAREN E. SCOTT
UNITED STATES MAGISTRATE JUDGE