AAS:MAA
F. #2021R00963

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

KAMBIZ ATTAR KASHANI,

Defendant.

----------X

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN SUPPORT OF ARREST WARRANT

(50 U.S.C. § 1705; 18 U.S.C. § 2)

Case No. 22 MJ 31

EASTERN DISTRICT OF NEW YORK, SS:

LAUREN HARRY, being duly sworn, deposes and states that she is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

In or about and between February 2019 and June 2021, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant KAMBIZ ATTAR KASHANI, together with others, did knowingly and willfully conspire to cause the export, re-export, sale and supply, directly and indirectly, of goods, technology and services, to wit: two subscriptions to a proprietary computer software program; several fixed attenuators; two subscriptions to operating software; six power supplies; and several storage systems, from the United States to Iran and the Government of Iran, without having first obtained the required licenses or other authorization from the U.S.

Department of the Treasury Office of Foreign Assets Control, contrary to Title 50, United States Code, Section 1705.

(Title 50, United States Code, Section 1705(a) and (c); Title 18, United States Code, Section 2)

The source of your deponent's information and the grounds for her belief are as follows:[1]

1. I am a Special Agent with the Federal Bureau of Investigation and have been involved in the investigation of numerous cases involving espionage and the illegal export of U.S. goods and technology. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of the investigative file, and from reports of other law enforcement officers involved in the investigation.

I. Relevant Statutory Background

2. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1706, authorizes the President of the United States to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy or economy of the United States when the President declares a national emergency with respect to that threat. Pursuant to IEEPA, beginning in May 1995, the President has signed a series of Executive Orders imposing economic sanctions, including trade restrictions, against Iran. The Executive Orders have prohibited the exportation, re-exportation, sale or supply, directly or indirectly, to Iran of any goods,

[1] Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all of the relevant facts and circumstances of which I am aware.

technology or services from the United States. Under IEEPA, it is a crime willfully to violate, attempt to violate, conspire to violate or cause a violation of any regulation issued pursuant to the statute. 50 U.S.C. § 1705.

3. To implement the economic sanctions on Iran imposed by the Executive Orders, the U.S. Department of the Treasury, through its Office of Foreign Assets Control ("OFAC"), promulgated the Iranian Transactions and Sanctions Regulations ("ITSR"). 31 C.F.R. Part 560. The ITSR prohibits, among other things, the unlicensed export, re-export, sale or supply, directly or indirectly, from the United States or by a United States person, of any goods, services or technology to Iran or to the Government of Iran. The regulations also prohibit conspiring to and attempting to evade, avoid, or violate the regulations. The prohibitions further include the unauthorized export of goods from the United States to a third country if the goods are intended or destined for Iran.

II. The Defendant and Other Relevant Entities and Individuals

4. The Central Bank of Iran ("CBI") is the official bank of the Government of Iran. The U.S. Department of the Treasury recognizes that CBI "is an agency, instrumentality and controlled entity of the Government of Iran for all purposes under [C.F.R. § 535]." See 31 C.F.R. § 535.433 (U.S. Iranian Assets Control Regulations). In September 2019, OFAC classified CBI as a Specially Designated National ("SDN"), which designation signifies that CBI is acting for or on behalf of a terrorist organization. According to the OFAC press release issued at the time of the SDN designation, CBI has materially assisted, sponsored and provided financial, material or technological support, goods or services to Lebanese Hizballah, a terrorist organization, and to the Qods Force of Iran's Islamic Revolutionary Guards Corps ("IRGC"). The latter is a branch of the Iranian

armed forces and the Iranian government's primary means of directing and implementing its global terrorism campaign. By virtue of this designation, CBI itself became and is now subject to economic and trade sanctions, and any goods, technology or service exported from the United States to CBI requires an export license issued by OFAC.

5. Iran Company 1 is an electronic banking organization based in Iran, which provides information technology services to almost all Iranian commercial banks and many Iranian financial institutions. Iran Company 1 was founded in 1993 as the executive and technological arm of CBI; CBI is Iran Company 1's largest client. According to its website, Iran Company 1 is the largest electronic banking organization in the Middle East. Because Iran Company 1 is located in Iran, any goods, technology or service exported from the United States to Iran Company 1 requires an export license issued by OFAC.

6. UAE Company 1 is a company based in Dubai, United Arab Emirates ("UAE"). According to UAE Company 1's website, it creates computer networks to process financial transactions and is a global provider of electronic payment solutions that add value at the point-of-transaction for financial institutions, consumers, merchants, and acquirers. UAE Company 1 appears to have fewer than 60 employees, and as few as 12 to 14 employees. Of these employees, fewer than ten appear to physically work in the UAE Company 1 office in UAE.

7. UAE Company 2 is a company based in Dubai, UAE. According to its trading license, UAE Company 2 conducts software trading and computer and data processing. UAE Company 2 has approximately nine employees.

8. The investigation has revealed that UAE Company 1 and UAE Company 2 function as alter-ego companies and are licensed to conduct substantially the

same activities. The companies operate from the same physical office space in UAE. The majority of UAE Company 1 employees also are UAE Company 2 employees, and maintain both UAE Company 1 and UAE Company 2 email addresses and use those email addresses interchangeably. In addition, UAE Company 1 and UAE Company 2 each appear to have only one direct customer, specifically, Iran Company 1. Many of the UAE Company 1 and UAE Company 2 employees also have Iran Company 1 email addresses. The investigation has revealed that UAE Company 1 and UAE Company 2 appear to engage in the sole purpose of illegally providing U.S.-origin goods and technology to Iran Company 1.

9. KASHANI is a dual U.S. and Iranian citizen who resides in the UAE. KASHANI's online business profiles indicate that he has worked for companies that distribute technology in the Middle East and that work in cooperation with the Iranian government. KASHANI is a partial owner and a board member of UAE Company 1 and serves as UAE Company 1's technical manager, business development manager, and general contact for outbound shipments. KASHANI also is the founder, sole owner, and CEO of UAE Company 2 and is listed on its public trading license as its manager. In addition, KASHANI manages the finances and bank accounts for UAE Company 1 and UAE Company 2. KASHANI works from the UAE Company 1/UAE Company 2 physical space in UAE. Moreover, KASHANI has had an Iran Company 1 telephone number since in or about 2019 and an Iran Company 1 email address since in or about 2021; the email address is readily associated with Iran because the email address has an Iranian email domain (".ir").

10. The Coworker is an employee at both UAE Company 1 and UAE Company 2. The Coworker, like KASHANI, works from the UAE Company 1/UAE Company 2 physical space in UAE. The Coworker served as the point person for various

UAE Company 1/UAE Company 2 transactions with U.S. companies, including the transactions described below with U.S. Company 2, U.S. Company 3 and U.S. Company 4. The Coworker reports directly to KASHANI.

III. The Conspiracy to Violate IEEPA

11. Due to U.S. and international sanctions, Iran's direct access to U.S. goods, technology and services is heavily restricted. Iran and Iranian businesses are barred from procuring U.S. goods for export to Iran unless OFAC grants an export license for the shipment.

12. Accordingly, to procure goods, technology, and services manufactured and sold by U.S. companies, Iran Company 1 – sometimes acting on behalf of CBI – tasked KASHANI and others to purchase the goods, technology and services and arrange their transshipment into Iran. To fulfill Iran Company 1's requests, KASHANI and his co-conspirators used UAE Company 1 and UAE Company 2 – companies in which KASHANI is at least a partial owner and that appear to exist solely to circumvent U.S. export laws and sanctions by illegally procuring goods, services and technology for their only direct customer, Iran Company 1 – to conceal their purchases of U.S. goods, technology and services for end users in Iran. In furtherance of the scheme, KASHANI and others intentionally concealed from U.S. companies that they intended to ship U.S.-origin goods, technology and services from UAE Company 1 and UAE Company 2 to Iran. As detailed below, at least one of the companies targeted by KASHANI is located in the Eastern District of New York.

13. KASHANI and his co-conspirators facilitated these transactions without obtaining required licenses from OFAC. Indeed, at no time relevant to this

Complaint did KASHANI, the Coworker, UAE Company 1, UAE Company 2, Iran Company 1 or any other co-conspirator apply for, receive or possess an OFAC license or authorization to export, re-export, sell or supply any goods, services or technology from the United States to Iran.

14. The investigation has revealed that KASHANI took steps to conceal his business dealings with Iranian individuals and companies. For example, on or about July 15, 2020, KASHANI sent an email to the managing director of UAE Company 1, who also served as the commercial director of Iran Company 1. KASHANI advised that a UAE Company 2 account at a UAE bank had been blocked, and speculated that the account had been blocked due to two recent payments by UAE Company 2 to an Iranian UAE Company 2 employee. KASHANI further speculated that the payments had aroused suspicion given the high sensitivity toward accounts associated with Iranian passports, and suggested not further pursuing the blocked account with the bank. On or about July 23, 2020, KASHANI sent an email to the managing director, requesting that the managing director stop payment on a check that had been issued to the same Iranian UAE Company 2 employee from the same UAE Company 2 bank account. KASHANI referenced the problem with the UAE Company 2 bank account and suggested that, to avoid problems with the account, the check be re-issued in the name of a different UAE Company 1 employee – one who was not Iranian. Separately, on or about August 9, 2020, KASHANI signed a "Sanctions Assessment Questionnaire" for a UAE bank, in which KASHANI represented that, to the best of his knowledge, UAE Company 2 did not have any current or planned business activity in Iran. KASHANI also represented that, to the best of his knowledge, UAE Company 2 and its connected/related parties did not have a presence in Iran and that UAE Company 2 and its

connected/related parties were not then targeted for sanctions administered by, among others, OFAC. KASHANI further represented that none of UAE Company 2's sales or revenues were derived from Iran. As described below, both before and after August 2020, UAE Company 2 had business activity in Iran and sales or revenues derived from Iran. In addition, Iran Company 1 and CBI, both of which are connected/related parties to UAE Company 2, had a presence in Iran, and CBI is targeted for sanctions by OFAC. Notably, as part of the "Sanctions Assessment Questionnaire," KASHANI, as UAE Company 2's manager, agreed UAE Company 2 "committed to and shall fully comply with all applicable international sanctions (including EU . . . and US)."

U.S. Company 1

15. U.S. Company 1 is a U.S.-based technology company that designs, develops, and sells computer software, consumer electronics and online services. One of U.S. Company 1's products is a program that allows large organizations to develop and deploy proprietary, internal-use applications to their employees (the "Program"). At all times relevant to this Complaint, the export, re-export, sale and supply of the Program to Iran required an export license issued by OFAC.

16. KASHANI initially purchased the Program in or about 2016, and subsequently purchased annual renewals. At some point prior to 2019, KASHANI shared his Program account login information, which is associated with his UAE Company 1 email address, with Iran Company 1 in order to enable Iran Company 1 to access the Program.

17. In or about November 2019, an Iran Company 1 employee emailed KASHANI, the Coworker and others, requesting renewal of the subscription for the Program. The Coworker responded that, according to KASHANI, the Program automatically

would be renewed and a UAE Company 1 invoice would be generated after payment. The Coworker further stated that KASHANI could not provide information about the exact amount until the payment was completed.

18. On or about February 12, 2020, U.S. Company 1 sold KASHANI a one-year subscription to the Program on behalf of UAE Company 1 and emailed a receipt to KASHANI's UAE Company 1 email address. However, UAE Company 1 was not eligible to utilize the Program under the terms of U.S. Company 1's policies because UAE Company 1 had too few employees; to be eligible for the Program, a company needed to have at least 100 employees, whereas UAE Company 1 had no more than 60 employees, and as few as 12-14 employees.

19. On or about February 16, 2020, the Coworker provided an invoice for the Program to Iran Company 1. On or about March 2, 2020, the Coworker confirmed payment from Iran Company 1 to UAE Company 2 for the Program.

20. On or about March 15, 2020, apparently unaware that this transaction had occurred, a CBI employee sent an internal email requesting "immediate renewal" of the Program, noting that it must be updated in CBI's system before expiring on March 31, 2020. The CBI employee emphasized the importance of the task given the limited time before the Program expired, and that "regeneration [wa]s practically impossible due to the sanctions." The email ultimately was forwarded to KASHANI's UAE Company 1 and UAE Company 2 email accounts. On or about March 18, 2020, KASHANI responded that the subscription for the Program already had been renewed for another year and requested that the purchase price be paid to him, forwarding the receipt from his February 12, 2020 purchase.

21. On or about February 14, 2021, U.S. Company 1 sold KASHANI another one-year subscription for the Program. On or about February 15, 2021, KASHANI forwarded the purchase confirmation to an Iran Company 1 employee, who stated that KASHANI would be reimbursed. On or about February 27, 2021, an Iran Company 1 employee emailed KASHANI, copying the Coworker, requesting confirmation that they had received the payment. On or about March 3, 2021, the Coworker confirmed to the Iran Company 1 employee that KASHANI had received the payment.

22. On or about June 7, 2021, U.S. Company 1 updated the Program license agreement. In connection with that update, KASHANI was required to – and did – confirm that he had read and agreed to be bound by the Program license agreement. That agreement provided, in part:

> **14.8 Export Control**
>
> A. You may not use, export, re-export, import, sell, release, or transfer the [U.S. Company 1] Software, Services, or Documentation except as authorized by United States law, the laws of the jurisdiction in which You obtained the [U.S. Company 1] Software, and any other applicable laws and regulations. In particular, but without limitation, the [U.S. Company 1] Software, Services, source code, technology, and Documentation (collectively referred to as "[U.S. Company 1] Technology" for purposes of this Section 14.8) may not be exported, re-exported, transferred, or released (a) into any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce's Denied Persons List or on any other restricted party lists. By using the [U.S. Company 1] Technology, You represent and warrant that You are not located in any such country or on any such list. You also agree that You will not use the [U.S. Company 1] Technology for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of nuclear, missile, chemical or biological weapons or any other military end uses as defined in 15 C.F.R § 744. You certify that pre-

> release versions of the [U.S. Company 1] Technology will only be used for development and testing purposes, and will not be rented, sold, leased, sublicensed, assigned, or otherwise transferred. Further, You certify that You will not sell, transfer or export any product, process or service that is a direct product of such pre-release [U.S. Company 1] Technology.
>
> B. You represent and warrant that You and any entity or person that directly or indirectly controls You, or is under common control with You, are not: (a) on any sanctions lists in the countries in which the [U.S. Company 1 application] is available, (b) doing business in any of the US embargoed countries, and (c) a military end user as defined and scoped in 15 C.F.R § 744. As used in this Section 14.8, "control" means that an entity or person possesses, directly or indirectly, the power to direct or cause the direction of the management policies of the other entity, whether through ownership of voting securities, an interest in registered capital, by contract, or otherwise.

23. By agreeing to be bound by the Program license agreement, KASHANI represented, among other things, that he was not doing business – and would not do business – in any U.S. embargoed country. At the time KASHANI made that representation, he was doing business in Iran, a U.S. embargoed country. KASHANI has continued to do business in Iran since making that representation and agreeing to be bound by the Program license agreement.

24. KASHANI subsequently, on or about June 18, 2021, purchased a digital content platform from U.S. Company 1. That same day, U.S. Company 1 sent an email to KASHANI's UAE Company 1 email address, alerting him that someone had logged into his U.S. Company 1 account (which KASHANI had provided to Iran Company 1 in order to enable Iran Company 1 to access the Program) from Iran. The email from U.S. Company 1 stated "[T]his download was initiated from Iran," and instructed that, if

KASHANI had not initiated the download, he should contact U.S. Company 1. KASHANI did not contact U.S. Company 1 in response to the email.

25. On or about June 21, 2021, an Iran Company 1 employee sent an email to KASHANI requesting non-Iranian SIM cards so that Iran Company 1 employees could use U.S. Company 1 software, which was prohibited in Iran.

26. At no time did KASHANI use his Iran Company 1 email address or telephone number – or any other contact information associated with the country of Iran – in connection with the above purchases from U.S. Company 1.

27. At no time relevant to this Complaint did KASHANI, the Coworker, UAE Company 1, UAE Company 2, Iran Company 1 or any other co-conspirator obtain a license from OFAC to export, re-export, sell or supply the Program.

U.S. Company 2

28. U.S. Company 2 is a U.S. company headquartered in Brooklyn, New York, which designs, manufactures and distributes radio frequency and microwave components and integrated assemblies. According to its website, U.S. Company 2 has locations in more than 30 countries and offers more than 10,000 models widely used in commercial, industrial and military applications. At all times relevant to this Complaint, any goods, technology, and services exported from U.S. Company 2 to Iran required an export license issued by OFAC.

29. On or about May 12, 2020, an employee of Iran Company 1, using the employee's UAE Company 2 email address, requested that the Coworker send price quotes for several items, including several fixed attenuators, which are devices found in various electronic equipment with uses that include extending the dynamic range of measuring

equipment and preventing signal overload in transmitters and receivers. These attenuators are manufactured in India, shipped to Brooklyn, and then exported worldwide from the United States.

30. Between about June and September 2020, the Coworker, using the Coworker's UAE Company 2 email address, communicated with U.S. Company 2 regarding the purchase of these attenuators. During these communications, U.S. Company 2 expressly informed the Coworker that the parts could not be shipped to Iran:

> This quote is not applicable for distribution in the following Embargo/Restricted countries and/or any entity on the U. S. Dept. of Commerce denials list: Iran, Iraq, Libya, Cuba, North Korea, Syria and Sudan.

31. The Coworker nevertheless proceeded with the purchase from U.S. Company 2, with the intention of providing the parts to Iran Company 1 in Iran. In connection with the purchase, the Coworker attached an end user form, signed by the Coworker, indicating that UAE Company 2 was the end user and requesting shipment to UAE Company 1. The end user form stated, in part:

> Your company declares that the information stated in this Export End User Form ("EEUF") is accurate and that the part(s) ordered by your company will not be exported, re-exported, or transferred to any person, entity or country, or for any use, except in compliance with all applicable United States and foreign laws, rules, restrictions and regulations, including, without limitation, the EAR, the Arms Export Control Act, and the International Traffic in Arms Regulations. Diversion therefrom contrary to U.S. law is prohibited.

32. On or about September 2, 2020, the Coworker emailed an invoice to an Iran Company 1 employee. The invoice was addressed to Iran Company 1 and listed UAE

Company 2's bank account. The first ten part numbers listed on the spreadsheet matched the part numbers the Coworker had procured from U.S. Company 2.

33. On or about September 16, 2020, the Coworker emailed the Iran Company 1 employee, confirming receipt of the parts from U.S. Company 2.

34. On or about February 6, 2021, an Iran Company 1 employee requested that the Coworker and others ship U.S. Company 2 goods to an Iran Company 1 location in Iran. The Coworker subsequently confirmed receipt of the email.

35. At no time did the Coworker use any contact information associated with the country of Iran in connection with the above purchases from U.S. Company 2.

36. At no time relevant to this Complaint did KASHANI, UAE Company 1, UAE Company 2, Iran Company 1 or any other co-conspirator obtain a license from OFAC to export, re-export, sell or supply any U.S. Company 2 goods, technology or services from the United States to Iran.

U.S. Company 3

37. U.S. Company 3 is a U.S. software company, based in North Carolina, which sells open-source products to businesses. U.S. Company 3 software both is created on and resides on servers located in the United States. At all times relevant to this Complaint, any goods, technology or services exported from U.S. Company 3 to Iran required an export license issued by OFAC.

38. In or about February 2019, an Iran Company 1 employee emailed the Coworker a request to renew two subscriptions to the U.S. Company 3 operating system. In subsequent correspondence, the Iran Company 1 employee suggested that the Coworker

"check with Mr. Kashani" regarding payment. On or about April 25, 2019, U.S. Company 3 issued a receipt for two one-year subscriptions, expiring on or about April 3, 2020.

39. On or about May 14, 2019, the Coworker emailed the UAE Company 1 username and password to the Iran Company 1 employee to enable Iran Company 1 to access the U.S. Company 3 subscriptions. Subpoena returns reflect IP logins to the U.S. Company 3 subscriptions from Iran Company 1 employees in Iran associated with the UAE Company 1 username.

40. In or about March 2020, U.S. Company 3 disabled UAE Company 1's accounts because it had discovered that U.S. Company 3 software associated with UAE Company 1's license was being accessed from Iran and that one of the email addresses associated with the account belonged to an Iranian domain. A U.S. Company 3 employee subsequently emailed the Coworker to inform the Coworker that the UAE Company 1 account had been disabled because it appeared to violate U.S. export regulations. The Coworker forwarded that email to employees at Iran Company 1 and UAE Company 2, as well as at least one other person.

41. In or about April 2020, an Iran Company 1 employee emailed the Coworker and a UAE Company 2 employee, with the subject "[U.S. Company 3]'s Update," requesting a price quote. Subsequently, the Coworker set up a new account with a U.S. Company 3 supplier using the Coworker's UAE Company 2 email address, rather than the Coworker's UAE Company 1 email address. On or about May 4, 2020, the Coworker used this new UAE Company 2 account to request quotes for several products, including two subscriptions to the U.S. Company 3 operating system. In the Coworker's email to the

supplier, the Coworker represented that "[o]ur company [UAE Company 2] is the end-user" of the product.

42. On or about June 7, 2020, the Coworker emailed employees at Iran Company 1 and UAE Company 2, reporting "they cannot send us the quotation as [U.S. Company 3] through thorough investigation found out, that [UAE Company 2] is related to [UAE Company 1] which was already blocked with them since they found out the previous purchased licenses had been accessed in Iran."

43. At no time did the Coworker use any contact information associated with the country of Iran in connection with the above purchases (and attempted purchases) from U.S. Company 3.

44. At no time relevant to this Complaint did KASHANI, the Coworker, UAE Company 1, UAE Company 2, Iran Company 1 or any other co-conspirator obtain a license from OFAC to export, re-export, sell, or supply any U.S. Company 3 goods, technology or services from the United States to Iran.

U.S. Company 4

45. U.S. Company 4 is a U.S. technology company with corporate offices in Massachusetts and Texas, which operates in the realm of information technology, cloud, and digital workplace infrastructure and emerging technologies, including 5G and artificial intelligence. The network storage systems, described below, are manufactured by U.S. Company 4 in Massachusetts. At all times relevant to this Complaint, any goods, technology and services exported from U.S. Company 4 to Iran required an export license issued by OFAC.

46. In or about August 2019, an Iran Company 1 employee asked the Coworker to acquire six power supplies. On or about December 22, 2019, the Coworker, using the Coworker's UAE Company 1 email address, informed the Iran Company 1 employee that UAE Company 1 had received the power supplies and asked the employee how to ship the supplies to Iran Company 1. In or about June 2020, UAE Company 2 hired a third-party courier to transport the goods from UAE to Iran Company 1. The Coworker also sent a UAE Company 2 invoice for the products to Iran Company 1.

47. On or about July 22, 2020, a different Iran Company 1 employee sent an email to a UAE Company 2 employee with a subject line naming certain U.S. Company 4 network storage systems. The Iran Company 1 employee advised that Iran Company 1 had ordered five of these systems and asked UAE Company 2 to help arrange their shipment from a company in Denmark.

48. In or about 2020 and 2021, the Coworker, UAE Company 2 and others facilitated this shipment. For example, on or about January 12, 2021, an Iran Company 1 employee sent an email advising that the shipment needed to clear customs in Tehran, Iran, to which the Coworker responded with various options for sending the shipment to Tehran. On or about April 21, 2021, UAE Company 2 provided Iran Company 1 with an invoice for the items with a total cost, including packing and export, which was addressed to Iran Company 1 at an address in Tehran and which reflected Iranian custom information, such as the Iranian port of arrival. On or about April 28, 2021, the shipping company emailed the Coworker, at the Coworker's UAE Company 2 email address, advising that the transport company in Europe needed import permission or a registration permit in Tehran. That day,

the Coworker responded, attaching the requested documentation, which listed the U.S. Company 4 products and the shipping destination in Tehran.

49. At no time relevant to this Complaint did KASHANI, the Coworker, UAE Company 1, UAE Company 2, Iran Company 1 or any other co-conspirator obtain a license from OFAC to export, re-export, sell or supply any U.S. Company 4 goods, services or technology from the United States to Iran.

50. Based on my training and experience, as well as the facts set forth in this Complaint, there is probable cause to believe that the defendant KASHANI, together with others, did violate Title 50, United States Code, Section 1705.

51. 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, the arrest warrant, and the Complaint. The defendant currently is at liberty and

accordingly I seek to seal this application to prevent the defendant from fleeing justice, avoiding arrest and prosecution, and destroying evidence.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant KAMBIZ ATTAR KASHANI so that he may be dealt with according to law.

Lauren B. Harry

LAUREN HARRY
Special Agent
Federal Bureau of Investigation

Sworn to before me by telephone
this 11 day of January, 2022

THE HONORABLE VERA M. SCANLON
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK