

UNITED STATES DISTRICT COURT

for the District of Columbia

FILED

JUL 28 2017

Clerk, U.S. District and Bankruptcy Courts

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



Case No. 17-MJ-536

APPLICATION FOR A SEARCH WARRANT

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

See Attachment A

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

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

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

The search is related to a violation of:

Table with 2 columns: Code Section, Offense Description. Rows include 18 U.S.C. § 951, 22 U.S.C. § 611 et seq., 18 U.S.C. § 1001 and their corresponding offense descriptions.

The application is based on these facts:

See attached Affidavit.

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

Reviewed by AUSA/SAUSA:



Applicant's signature



Printed name and title

Sworn to before me and signed in my presence.

Date: July 27, 2017

Beryl A. Howell

Judge's signature

City and state: Washington, D.C.

Hon. Beryl A. Howell, Chief U.S. District Judge

Printed name and title

FILED

JUL 28 2017

Clerk, U.S. District and
Bankruptcy Courts


IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF COLUMBIA

**IN THE MATTER OF THE SEARCH OF
TROUT CACHERIS & JANIS PLLC**




Case No. 17-MJ-536

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

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

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure to search the premises known as Trout Cacheris & Janis PLLC, , hereinafter "PREMISES," further described in Attachment A, for the property – electronic devices – described in Attachment B; to seize the property described in Attachment B; and to extract from that property the electronically stored information described in Attachment C. Because the premises to be searched is a law firm, and in light of the sensitivities attendant to such a search, I will limit the execution of this search to the process described infra in Paragraph 8.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and *FBI Headquarters in Washington, D.C.* assigned to the ~~Washington Field Office~~. I am a law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and I am authorized by law to conduct investigations and to make arrests for felony offenses. I have been a Special Agent with the FBI since 2006. This affidavit is intended to show only that there is sufficient

*@/AMT
7/28/2017*

probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. On July 7, 2017, the United States submitted an application for a search warrant, attached hereto as Exhibit 1, in connection with which I swore to an affidavit, attached hereto as Exhibit 2 and described herein as the “July 7 Affidavit,” that established that there is “probable cause to believe that Michael T. Flynn, Bijan Rafiekian, and other individuals working for or with Flynn, the Flynn Intel Group Inc. and the Flynn Intel Group LLC (collectively “FIG”) committed violations of 18 U.S.C. § 951 (acting as a foreign agent without notice to the Attorney General), the Foreign Agents Registration Act (“FARA”), 22 U.S.C. § 611 et seq, and 18 U.S.C. § 1001 (making a material false statement).” Exhibit 2 is incorporated herein by reference. That affidavit further established that there is probable cause to search the electronic devices that Rafiekian used in furtherance of his employment with and work for FIG “for evidence, contraband, fruits, and/or instrumentalities of these crimes.” Exhibit 2, Attachment B3.

4. Pursuant to that application, on July 7, 2017, Chief Judge Beryl A. Howell granted a warrant to search the electronic devices Rafiekian used in furtherance of his employment with and work for FIG for all records relating to those violations. The warrant is attached hereto as Exhibit 3. The application contemplated that Rafiekian would produce the devices sought pursuant a Grand Jury subpoena, which was attached to the application. See Exhibit 3. Rafiekian did not produce the devices in response to that subpoena but rather, on July 14, 2017, he moved to quash the subpoena through his counsel, Trout Cacheris & Janis PLLC. Because Rafiekian did not produce the devices sought, the United States never executed the search warrant attached hereto as Exhibit 3.

PROBABLE CAUSE

5. Paragraphs 9 through 31 of Exhibit 2, which are incorporated herein by reference, establish probable cause to believe that the named individuals committed the listed crimes and to search the devices described in Attachment B hereto for evidence of those crimes.

6. On July 13, 2017, six days after the subpoena referenced above had been served on Rafiekian through his counsel, Rafiekian's counsel informed the government attorneys handling this matter that they were taking control of their client's electronic devices referenced in the July 7 Affidavit.

7. Based on my investigation to date, I am aware that among the electronic devices Rafiekian utilized in furtherance of his employment with and work for FIG are a computer and an iPhone. The following facts support that conclusion:

- a. Covington & Burling ("Covington") represent FIG. On May 26, 2017, Covington informed me that FIG had not provided any of its employees or associates with electronic devices to be used for business purposes. Rather, FIG employees and associates used their personal electronic devices—including computers and cellular phones—to conduct FIG's business. Covington further explained that, when FIG ceased operations in November 2016, FIG associate [REDACTED] had instructed all persons associated with FIG to download their FIG-related emails from the FIG network should they wish to retain those emails. In the same conversation, Covington represented that Rafiekian provided FIG attorneys with his FIG-related emails, which they reviewed for responsiveness.
- b. Less than two weeks after the May 26, 2017 conversation, the government obtained toll and billing records from Verizon Wireless, the service provider for Rafiekian's cellular phone. Those records, along with other materials in the

government's possession, revealed that Rafiekian has used an iPhone mobile device with International Mobile Equipment Identity ("IMEI") number

IMEI is a unique number associated with a mobile phone that is usually printed inside the battery compartment and that the service provider can interpret to provide the make and model of the phone associated with the IMEI. The last number of the IMEI is called a check digit. On billing records, Verizon reports the last digit as a zero; the actual last digit can be calculated by using the Luhn formula.

- c. The device with IMEI [REDACTED] has been assigned the telephone number [REDACTED]. Of relevance, from July 2016 through December 2016, approximately 500 calls were made from the [REDACTED] number linked to Rafiekian's device to phone numbers associated with FIG principals and FIG business associates. In addition, emails that FIG has produced to the government reflect that Rafiekian listed the [REDACTED] number as his work number as early as February 2016 and that, as of August 2016, Rafiekian was using an iPhone to send FIG-related emails.

8. Because the warrant sought herein authorizes the search of a law office, and the government is extremely sensitive to the need to prevent any potential intrusion into the attorney-client privilege, execution of the warrant will entail government agents alerting Rafiekian's counsel at Trout Cacheris & Janis PLLC to the existence of the warrant and asking them to comply by providing the property listed in Attachment B to the government, rather than government agents physically searching the PREMISES. If that execution plan is ultimately insufficient to obtain custody of the property listed in Attachment B, government agents will not

take any additional actions to execute the search warrant without further consultation with the Court. In addition, the search of the property listed in Attachment B for the electronically stored information described in Attachment C would in the first instance be conducted by a “filter” or “taint” team of agents and attorneys, rather than the agents and attorneys working on the investigation, whose mandate would be to review for material potentially subject to the attorney-client privilege and to remove that material from the information eventually turned over to the investigators for their review. Finally, where appropriate, officers will copy data, rather than physically seize computer and phone, to reduce the extent of disruption. If, after inspecting the computer and phone, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

CONCLUSION

9. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A, seize the property described in Attachment B, and to extract from that property electronically stored information described in Attachment C.

REQUEST FOR SEALING

10. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant, except as may be necessary for law enforcement purposes. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation, not all of the targets and subjects of this investigation are aware that they are targets and subjects, and not all of the potentially relevant materials for those targets and subjects will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other

online criminals as they deem appropriate. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

A large black rectangular redaction box covers the signature of the Special Agent.

Special Agent
FBI

ENCLOSURES

Attachment A (Premises To Be Searched)

Attachment B (Property To Be Seized)

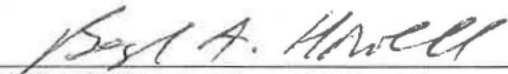
Attachment C (Electronically Stored Information To Be Searched)

Exhibit 1 (July 7, 2017 Application For A Search Warrant)

Exhibit 2 (Affidavit In Support of July 7, 2017 Search Warrant Application)

Exhibit 3 (Signed July 7, 2017 Search Warrant)

Subscribed and sworn to before me
on July 28, 2017:



HONORABLE BERYL A. HOWELL
CHIEF UNITED STATES DISTRICT JUDGE

ATTACHMENT A

The premises to be searched is Trout Cacheris & Janis PLLC, [REDACTED]
[REDACTED], further described as the office of a law firm located in
a suite of a 12-story, approximately 192,000 square foot brick building at the above street
address.

ATTACHMENT B

The property to be seized are the computer and iPhone that Bijan Rafiekian utilized in furtherance of his employment with and work for FIG. The first fourteen digits of the mobile device's IMEI # are [REDACTED] This warrant authorizes the forensic examination of the computer and iPhone for the purpose of identifying the electronically stored information described in Attachment C.

ATTACHMENT C

1. All records that relate to violations of 18 U.S.C. § 951, 22 U.S.C. § 611 *et seq.*, and 18 U.S.C. § 1001, and involve Michael T. Flynn, Bijan Rafiekian, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc. and/or the Flynn Intel Group LLC. (collectively, “FIG”), since January 1, 2014, including:

a. Communications, records, information, documents and other files that reveal efforts by Flynn, Rafiekian, Alptekin, FIG, and FIG associates to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

b. Communications, records, information, documents and other files that reveal associations between Flynn, Rafiekian, Alptekin, FIG, and FIG associates and any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

c. Records of any funds or benefits received by or offered to Flynn, Rafiekian, Alptekin, FIG, and FIG associates by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

d. Communications, records, information, documents and other files that pertain to representations that Flynn, Rafiekian, Alptekin, FIG, and FIG associates have made to the U.S. government;

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

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

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

c. evidence of the lack of such malicious software;

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

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

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

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

h. evidence of the times the COMPUTER was used;

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

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

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

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

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

As used above, the terms "records" and "information" include all of the foregoing items
of evidence in whatever form and by whatever means they may have been created or stored,
including any form of computer or electronic storage (such as flash memory or other media that
can store data) and any photographic form.

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

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

Exhibit 1

UNITED STATES DISTRICT COURT

FILED

JUL -7 2017

for the District of Columbia

Clerk, U.S. District and Bankruptcy Courts

In the Matter of the Search of

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

ELECTRONIC DEVICES TO BE PROVIDED TO A GRAND JURY IN THE DISTRICT OF COLUMBIA, IN RESPONSE TO GRAND JURY SUBPOENA 17-1/2008, BY SUBPOENA RECIPIENT BIJAN RAFIEKIAN A/K/A BIJAN KIAN

Case No: 1:17-mj-477

Assigned To: Chief Judge Beryl A. Howell

Date Assigned: 7/7/2017

Description: Search and Seizure Warrant

APPLICATION FOR A SEARCH WARRANT

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

See Attachment A3

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

See Attachment B3

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

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

The search is related to a violation of:

Table with 2 columns: Code Section and Offense Description. Rows include 18 U.S.C. § 951; 22 U.S.C. § 611 et seq.; 18 U.S.C. § 1001.

The application is based on these facts:

See attached Affidavit.

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

Reviewed by AUSA/SAUSA:

[Redacted signature box]

[Redacted signature]

Applicant's signature

[Redacted name]

Printed name and title

Sworn to before me and signed in my presence.

Date: 07/7/2017

[Handwritten signature]

Judge's signature

City and state: Washington, D.C.

Hon. Beryl A. Howell, Chief U.S. District Judge

Printed name and title

Exhibit 2

FILED

JUL -7 2017

**Clerk, U.S. District and
Bankruptcy Courts**

**IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF COLUMBIA**

**IN THE MATTER OF THE SEARCH OF
ELECTRONIC DEVICES TO BE
PROVIDED TO A GRAND JURY IN THE
DISTRICT OF COLUMBIA, IN
RESPONSE TO GRAND JURY
SUBPOENAS 17-1/2006, 17-1/2007 and 17-
1/2008, BY SUBPOENA RECIPIENTS
MICHAEL T. FLYNN, [REDACTED]
[REDACTED], and BIJAN RAFIEKIAN also
known as BIJAN KIAN.**

Case No: 1:17-mj-477
Assigned To: Chief Judge Beryl A. Howell
Date Assigned: 7/7/2017
Description: Search and Seizure Warrant

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

I, [REDACTED] [REDACTED], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for three search warrants authorizing the examination of property—electronic devices—which will be in the custody of law enforcement in Washington, D.C. at the time the warrants are executed, and the extraction from that property of electronically stored information described in Attachments B1, B2, and B3.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and assigned to the Washington Field Office. I am a law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and I am authorized by law to conduct investigations and to make arrests for felony offenses. I have been a Special

Agent with the FBI since November 1999. I have conducted numerous investigations involving both National Security and Criminal matters to include Espionage, Counterterrorism, Drug Trafficking, and non-Traditional Organized Crime. Prior to my position as a Special Agent with the FBI, I was an Intelligence Officer with the Defense Intelligence Agency in Washington, D.C. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Michael T. Flynn, Bijan Rafiekian, and other individuals working for or with Flynn, the Flynn Intel Group Inc. and the Flynn Intel Group LLC (collectively "FIG") committed violations of 18 U.S.C. § 951 (acting as a foreign agent without notice to the Attorney General), the Foreign Agents Registration Act ("FARA"), 22 U.S.C. § 611 *et seq.*, and 18 U.S.C. § 1001 (making a material false statement). There is also probable cause to search the information described in Attachments A1, A2, and A3 for evidence, contraband, fruits, and/or instrumentalities of these crimes, further described in Attachments B1, B2, and B3.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The premises to be searched are comprised of electronic devices to be provided to a Grand Jury in this District, pursuant to validly-issued Grand Jury subpoenas attached hereto as Exhibits 1, 2, and 3, by Michael T. Flynn, [REDACTED], and Bijan Rafiekian (collectively, the "Subjects"). The premises will be referred to herein as the "Subject Premises."

5. On July 7, 2017, a Grand Jury in this district issued the subpoenas attached as Exhibits 1, 2, and 3, which, respectively, compel Michael T. Flynn, [REDACTED] [REDACTED], and Bijan Rafiekian to provide: "Any electronic device, including but not limited to laptops, cell phones,

and electronic storage media such as USB drives, memory cards and external hard drives, that you used in connection with your work for or with” Michael T. Flynn, Bijan Rafiekian, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc., and/or the Flynn Intel Group LLC. The FBI currently plans to serve those subpoenas on the three Subjects on or about July 7, 2017.

6. The subpoenas require the Subjects to produce the requested devices to the Grand Jury on July 14, 2017. At that time, the FBI intends to take possession of the devices and execute this search warrant, should the instant application be approved. Because the Grand Jury sits in this district, should the Subjects produce the subpoenaed devices to the Grand Jury, the search will be executed in this district – specifically, at the Washington Field Office of the FBI. Should the Subjects choose to comply with the attached subpoenas by producing the devices directly to the FBI on or before July 14, 2017, the FBI will only execute this search warrant once the devices have been transported to the Washington Field Office, located in this district.

7. For the reasons described infra, I believe, based on my training, experience, and information I have learned over the course of this investigation, that the Subject Premises contain evidence of the crimes listed in Paragraph 3, supra. The Subject Premises are comprised of devices which the Subjects used in furtherance of their employment with and work for the now-defunct corporate entity, FIG. As discussed further infra, FIG did not appear to provide its employees computers, phones, or other equipment, but instead allowed its employees to use their personal electronic devices, including phones and computers, for all company businesses during the term of their employment. I have been unable to determine over the course of this investigation the exact model and serial numbers of the devices used by the Subjects in furtherance of their work for FIG – thus, I seek this anticipatory search warrant and anticipate

executing it upon those devices which the Subjects indicate, by their compliance with the attached subpoenas, were the personal devices utilized by the Subjects for FIG business during the term of their employment with the company.

8. The applied-for warrants would authorize the forensic examination of the Subject Premises for the purpose of identifying electronically-stored data particularly described in Attachments B1, B2, and B3.

PROBABLE CAUSE

A. Overview of the Investigation

9. The FBI is investigating the Subjects, FIG, and persons working for or with FIG in connection with activities they conducted in the United States on behalf of foreign governments and foreign principals without having properly disclosed such relationships to the United States government. Specifically, as discussed further below, there is probable cause to believe that, since as early as July 2016, the Subjects, FIG, and persons working for or with FIG performed work on behalf of, at the direction of, and for the principal benefit of the Government of Turkey, without disclosing such relationships to the United States government. The evidence indicates there is reason to believe that the Subjects, FIG, and FIG associates masked the fact that they were working at the direction of and for the principal benefit of the Government of Turkey by utilizing an intermediary, Ekim Alptekin, a foreign businessman with Turkish and Dutch passports, and his company, Inovo BV (“Inovo”), which is incorporated in the Netherlands. As described in the emails below, the Subjects’ and FIG’s work with Inovo focused almost exclusively on Fethullah Gulen, a U.S. citizen and cleric whom the Government of

Turkey blames for a failed coup attempt in that country that occurred in July 2016 and whose extradition from the United States Turkey sought in July 2016.

10. There are some limited exemptions to the requirement to register under FARA, such as if the foreign agent registers under the Lobbying Disclosure Act (“LDA”). The LDA exemption, however, does not apply if the foreign principal is a foreign government or if a foreign government is the principal beneficiary of the political activities. *See* 22 U.S.C. § 213; 28 C.F.R. § 5.307.

1. The Subjects

11. Michael T. Flynn is the former Director of the Defense Intelligence Agency and the former National Security Advisor. Flynn started his own company soon after being honorably discharged from the military in September 2014. Specifically, in or around June 2015, Flynn, Bijan Rafiekian (also known as “Bijan Kian”) (hereinafter “Kian”), and [REDACTED] incorporated FIG in Delaware, with its principal address at [REDACTED] [REDACTED], [REDACTED] ([REDACTED] is not included amongst the “Subjects” in this application.) The FIG Board of Directors were Flynn, Kian, and [REDACTED]. Flynn was the Chairman and CEO and Kian was the Vice Chairman. [REDACTED], served as Flynn’s Chief of Staff at FIG.

2. The Unregistered Foreign Agent Allegations

12. Based on a review of open source material, I am aware that on or about July 15, 2016, a coup d’etat was attempted in Turkey against President Recep Tayyip Erdogan. President Erdogan and his administration claimed that Fethullah Gulen and his followers instigated the coup. Gulen lives in the United States and operates a network of charter schools.

13. On or about July 23, 2016, the Government of Turkey formally sought Gulen's extradition from the United States.

14. On or about July 27, 2016, Kian, using his FIG email address, emailed Alptekin to discuss FIG working on a project that appeared to be for the principal benefit of the Government of Turkey. In the email, Kian indicated that he had had a "detailed discussion" with "MF" and that they "are ready to engage on what needs to be done. Turkey's security and stability is extremely important to world security. [President Erdogan] can lead the campaign against Radical Islam to protect the image of Islam." Based on my knowledge of this investigation, I believe "MF" is Michael T. Flynn, the head of FIG.

15. Soon after these initial discussions, Alptekin engaged with high-level officials within the Government of Turkey to get approval and funding for the project. For example, on or about July 29, 2016, Alptekin emailed Kian that Alptekin had met with "MC" in Turkey. Based on my knowledge of this investigation, I believe that MC is the Turkish Foreign Minister, Melvut Cavusoglu. According to the email, "MC" asked Alptekin to work with FIG "to formulate what kind of output we can generate on the short to mid-term as well as an indicative budget ... Ps: Needles [sic] to tell you but he asked me not to read in anyone else for the time being and keep this confidential." Based upon my training and experience, as well my knowledge of this investigation, I believe the instruction "not to read in anyone else" was an instruction not to tell anyone else about the terms of the project for which the Government of Turkey was engaging FIG.

16. On or about August 8, 2016, Alptekin emailed Flynn and Kian, at their respective FIG email addresses, to inform them that he met with the Turkish Minister of Economy to discuss Alptekin and FIG's proposed work for Turkey, and that the Minister of Economy agreed

to discuss the proposal with other Turkish ministers, including Turkish Prime Minister Binali Yildirim. Alptekin then sent a follow-up email, on or about August 10, 2016, to Flynn and Kian at their same FIG email addresses letting them know that he had had several meetings with the Turkish Ministers of Economy and Foreign Affairs, and he (Alptekin) had “a green light to discuss confidentiality, budget and the scope of the contract.”

17. As the above-described conversations indicate, it appears that the Government of Turkey, rather than Inovo and Alptekin, was FIG’s ultimate client in connection with this project. FIG also reached a side agreement with Alptekin at the time Flynn signed the Inovo contract whereby Alptekin would receive 20% of any funds FIG received for the project. Given that Alptekin was ostensibly paying FIG from his own funds for FIG’s work on the project, there is no clear business rationale for FIG to agree to repay Alptekin 20% of the funds it received from him in connection with the project. Thus, the below-described conversations provide additional evidence that Alptekin was not in fact FIG’s ultimate client on the project.

- a. On or about August 11, 2016, Kian used his FIG email address to inform Alptekin that he and Flynn had discussed the “campaign,” which they described as restoring “confidence through clarity,” and that the budget included providing Alptekin 20% of the fees for “advisory support.”
- b. On or about August 25, 2016, Kian sent an email from his FIG address, on which he copied Flynn, indicating that Alptekin’s company, Inovo, would be the official client for FIG’s project related to Turkey. Specifically, Kian thanked Alptekin for engaging FIG on “Operation CONFIDENCE.” In the email, Kian explained that the budget would be up to \$200,000 per month, 20% of which would be provided to Inovo for Alptekin’s “active participation and counsel on this engagement.”

- c. On or about September 8, 2016, Alptekin emailed Kian, at his FIG email address, an Independent Advisory Services Agreement signed by Alptekin. In the agreement, Inovo is listed as the “client;” FIG is the “advisor.” The agreement states that the advisor, FIG, “is prepared to deliver findings and results including but not limited to making criminal referrals if warranted.” Based on my knowledge of this investigation, I believe “criminal referrals” refers to referrals to U.S. law enforcement authorities regarding alleged criminal activity by Gulen. The agreement is effective on August 15, 2016, and continues for three months. The compensation for the “advisor,” FIG, is \$200,000 per month.
- d. On or about September 9, 2016, the day after email records indicate Flynn and Alptekin had both signed the Independent Advisory Services Agreement, bank records indicate that Alptekin transferred \$200,000 to FIG.
- e. On or about September 12, 2016, Kian, using his FIG email address, emailed Flynn at Flynn’s FIG address another Independent Advisory Services Agreement for Alptekin. In this second agreement, in a reversal of roles from the contract signed on September 8, Alptekin is listed as the “advisor” and FIG is the “client.” The agreement includes a “mobilization fee” of \$40,000 for the advisor, Alptekin. The agreement was later modified to state that Alptekin was performing those services under Inovo, and was ultimately signed by Flynn on October 30, 2016.
- f. According to bank records provided by FIG, on or about September 13, 2016, four days after receiving \$200,000 from Alptekin, FIG transferred \$40,000 to Inovo. Kian emailed [REDACTED] and tasked him to execute this transfer.

██████████ ██████████ advised Kian that he executed the transfer of funds on September 13, 2016.

- g. Similarly, Kian emailed ██████████ on or about October 14, 2016, and asked him to transfer another \$40,000 to Alptekin. ██████████ transferred the funds to Alptekin on October 14, 2016.
- h. According to the email and business records obtained from FIG, Alptekin does not appear to have provided any advisory, research, or consultation services to FIG in or around September and October 2016.

18. As the above-described communications indicate, it appears that the Government of Turkey, rather than Inovo and Alptekin, was FIG's ultimate client in connection with this project. Further support for this conclusion can be found within FIG's emails about the project, which indicate that FIG's work pursuant to the contract focused exclusively on Gulen – whose extradition the Government of Turkey was expending substantial resources in order to secure at this time – and promoting stability in Turkey, both of which are core interests of the Government of Turkey, rather than of the Dutch company Inovo.

19. On or about September 5, 2016, Kian, using his FIG address, emailed Flynn, at his FIG address, the "Operation CONFIDENCE Playbook." The "Playbook," which was attached to the email, described its mission goals as investigating the activities of "X" in the United States and registering "under Lobbying Disclosure Act representing a Dutch entity." Based on my review of the materials obtained in this investigation, I believe "X" refers to Gulen. Listed among the participants in the "Playbook" is Alptekin, whose role is defined as "strategy support," as opposed to the "client" or a similar moniker.

20. On or about September 6, 2016, Kian, using his FIG address, emailed both Flynn and [REDACTED] at their FIG addresses to advise them that the “client is seeking a high level meeting in NYC on September 19th or 20th.”

21. On or about September 19, 2016, according to publicly filed documents and interviews conducted by the FBI, Kian, Flynn, other FIG employees and James Woolsey, the former Director of Central Intelligence, met with Alptekin, Turkish Minister of Foreign Affairs Cavusoglu, and the Turkish Minister of Energy, Berat Albayrak, in New York City. According to open source information, Minister Albayrak is the son-in-law of President Erdogan. According to one of the meeting participants, the individuals discussed forcibly removing Gulen from the United States in lieu of extradition.

22. On or about November 8, 2016, Flynn published an op-ed in *The Hill* focusing on Gulen, whom Flynn called a “radical Islamist.” Flynn also called Turkey the US’s strongest ally against ISIS. Four days before the op-ed was published, Kian, using his FIG address, emailed a version of that op-ed to Alptekin and to Bob Kelley, FIG’s General Counsel.

23. On or about September 30, 2016, according to public records, FIG registered under the LDA that it was engaged in lobbying activity on behalf of Inovo. The filing, however, failed to identify that the Government of Turkey directed, controlled, or was the principal beneficiary of FIG’s lobbying activity. Moreover, the filing failed to specify that FIG would be lobbying on issues relating to Turkey and Gulen.

24. After receiving a letter from the U.S. Department of Justice, on or about March 7, 2017, over six months after it began working with Alptekin, FIG registered under FARA with respect to its work with Inovo. In its registration, FIG acknowledged that its work “could be construed to have principally benefitted the Republic of Turkey.” The filing, however, appeared

to contain multiple material misstatements, including that the Government of Turkey did not direct, control, or finance FIG's work with Inovo; that FIG did not know the extent of the Government of Turkey's involvement in the project; that the purpose of the project was business-related; and that project was related to Inovo's work for an Israeli company.

25. Following the publication of Inovo's relationship with FIG, Alptekin publicly denied that he worked on behalf of the Government of Turkey in his dealing with FIG. When certain media outlets reported about \$80,000 of payments from FIG to Alptekin listed in FIG's FARA filing as "Consultant Fees," Alptekin publicly claimed that those payments were refunds for lobbying work that FIG had not performed. However, as detailed above, as early as August 11, 2016, Alptekin and Kian discussed providing Alptekin with 20% of the contract for "advisory support."

3. The Subject Premises

26. As described supra, the Subject Premises consist of electronic devices used by the Subjects during the course of their employment with and work for FIG.

27. A subpoena issued by a Grand Jury in the Eastern District of Virginia was served on FIG, through its counsel, on or about April 25, 2017. That subpoena, attached hereto as Exhibit 4, sought "any and all documents and physical objects currently in the possession, custody, or control of [FIG], including but not limited to" a category of documents enumerated in the subpoena. See Ex. 4 at 1-2.

28. In discussion with FIG's counsel regarding the execution of the aforementioned subpoena, FIG's counsel indicated that, at the time of that conversation, he was not aware that FIG provided any of its employees or associates with electronic devices to be used for business

purposes. Rather, he advised that FIG employees and associates appeared to utilize their personal electronic devices, including laptops and phones, in order to conduct FIG business.

29. FIG ceased operations on November 30, 2016. On or about that date, according to FIG's attorney, FIG associate [REDACTED] instructed all employees to download their FIG-related emails from the FIG network – operated by Google – should they wish to retain them.

30. In responding to the subpoena provided in Exhibit 4, FIG's counsel indicated that Flynn and Kian had both retained responsive documents on their personal computers. Michael T. Flynn turned over his computer to be imaged by FIG's counsel. Kian provided the FIG attorneys with his FIG-related emails, which they reviewed for responsiveness. FIG's counsel further indicated that [REDACTED] had provided FIG-related emails that he had recovered from his personal devices to them in response to the subpoena.

31. Thus, there is reason to believe that the Subjects are currently in possession of electronic devices which contain the information described in Attachments B1, B2, and B3. Furthermore, there is probable cause to believe that the Subject Premises, which are comprised of those electronic devices, contain information pertaining to FIG's work with Inovo, Alptekin, and the Government of Turkey.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. There is probable cause to believe that things that were once stored on the Subject Premises may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

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

34. *Forensic evidence.* As further described in Attachments B1, B2, and B3, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Premises because:

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

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

35. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

36. *Manner of execution.* Because this warrant seeks only permission to examine a device that will be in law enforcement's possession at the time of execution, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

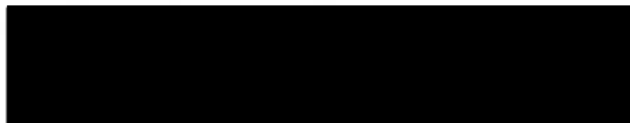
37. I submit that this affidavit supports probable cause for search warrants authorizing the examination of the Subject Premises described in Attachments A1, A2, and A3 to seek the items described in Attachment B1, B2, and B3.

REQUEST FOR SEALING

38. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation, not all of the targets and subjects of this investigation are aware that they are targets and subjects, and not all of the potentially relevant materials for those targets and subjects will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit

and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Special Agent
FBI

Subscribed and sworn to before me
on July 7, 2017:

A handwritten signature in black ink, appearing to read "Beryl A. Howell", written over a horizontal line.

HONORABLE BERYL A. HOWELL
CHIEF UNITED STATES DISTRICT JUDGE

ATTACHMENT A1

The premises to be searched consist of electronic device(s) provided to a Grand Jury in the District of Columbia, in response to Grand Jury subpoena 17-1/2006, by subpoena recipient Michael T. Flynn.

This warrant authorizes the forensic examination of the Device(s) for the purpose of identifying the electronically stored information described in Attachment B1.

ATTACHMENT B1

1. All records on the Device(s) described in Attachment A1 that relate to violations of 18 U.S.C. § 951, 22 U.S.C. § 611 *et seq*, and 18 U.S.C. § 1001, and involve Michael T. Flynn, Bijan Rafiekian, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc. and/or the Flynn Intel Group LLC. (collectively, "FIG"), since January 1, 2014, including:

a. Communications, records, information, documents and other files that reveal efforts by Flynn, Rafiekian, Alptekin, FIG, and FIG associates to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

b. Communications, records, information, documents and other files that reveal associations between Flynn, Rafiekian, Alptekin, FIG, and FIG associates and any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

c. Records of any funds or benefits received by or offered to Flynn, Rafiekian, Alptekin, FIG, and FIG associates by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

d. Communications, records, information, documents and other files that pertain to representations that Flynn, Rafiekian, Alptekin, FIG, and FIG associates have made to the U.S. government;

e. Evidence indicating the Device owner's state of mind as it relates to the crimes under investigation;

2. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT A2

The premises to be searched consist of electronic device(s) provided to a Grand Jury in the District of Columbia, in response to Grand Jury subpoena 17-1/2007, by subpoena recipient [REDACTED].

This warrant authorizes the forensic examination of the Device(s) for the purpose of identifying the electronically stored information described in Attachment B2.

ATTACHMENT B2

1. All records on the Device(s) described in Attachment A2 that relate to violations of 18 U.S.C. § 951, 22 U.S.C. § 611 *et seq*, and 18 U.S.C. § 1001, and involve Michael T. Flynn, Bijan Rafiekian, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc. and/or the Flynn Intel Group LLC. (collectively, "FIG"), since January 1, 2014, including:
 - a. Communications, records, information, documents and other files that reveal efforts by Flynn, Rafiekian, Alptekin, FIG, and FIG associates to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - b. Communications, records, information, documents and other files that reveal associations between Flynn, Rafiekian, Alptekin, FIG, and FIG associates and any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - c. Records of any funds or benefits received by or offered to Flynn, Rafiekian, Alptekin, FIG, and FIG associates by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - d. Communications, records, information, documents and other files that pertain to representations that Flynn, Rafiekian, Alptekin, FIG, and FIG associates have made to the U.S. government;
 - e. Evidence indicating the Device owner's state of mind as it relates to the crimes under investigation;

2. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT A3

The premises to be searched consist of electronic device(s) provided to a Grand Jury in the District of Columbia, in response to Grand Jury subpoena 17-1/2008, by subpoena recipient Bijan Rafiekian, also known as Bijan Kian.

This warrant authorizes the forensic examination of the Device(s) for the purpose of identifying the electronically stored information described in Attachment B3.

ATTACHMENT B3

1. All records on the Device(s) described in Attachment A3 that relate to violations of 18 U.S.C. § 951, 22 U.S.C. § 611 *et seq*, and 18 U.S.C. § 1001, and involve Michael T. Flynn, Bijan Rafiekian, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc. and/or the Flynn Intel Group LLC. (collectively, "FIG"), since January 1, 2014, including:
 - a. Communications, records, information, documents and other files that reveal efforts by Flynn, Rafiekian, Alptekin, FIG, and FIG associates to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - b. Communications, records, information, documents and other files that reveal associations between Flynn, Rafiekian, Alptekin, FIG, and FIG associates and any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - c. Records of any funds or benefits received by or offered to Flynn, Rafiekian, Alptekin, FIG, and FIG associates by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - d. Communications, records, information, documents and other files that pertain to representations that Flynn, Rafiekian, Alptekin, FIG, and FIG associates have made to the U.S. government;
 - e. Evidence indicating the Device owner's state of mind as it relates to the crimes under investigation;

2. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

AO 110 (Rev. 06/09) Subpoena to Testify Before a Grand Jury

UNITED STATES DISTRICT COURT
for the
District of Columbia

SUBPOENA TO TESTIFY BEFORE A GRAND JURY

To: Michael T. Flynn

c/o [REDACTED]
Covington & Burling LLP

YOU ARE COMMANDED to appear in this United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place: U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA U.S. Courthouse, 3rd Floor Grand Jury #17-1 333 Constitution Avenue, N.W. Washington, D.C. 20001	Date and Time: 07/14/2017 10:00 am
---	---

You must also bring with you the following documents, electronically stored information, or objects *(blank if not applicable)*:

PLEASE SEE ATTACHED

Personal appearance is not required if the requested devices are (1) produced on or before the return date to FBI Special Agent [REDACTED] and (2) accompanied by an executed copy of the attached Declaration of Custodian of Records. This subpoena remains in effect until all devices are provided.

Date: 07/07/2017

CLERK OF COURT



Signature of Clerk or Deputy Clerk

The name, address, e-mail, and telephone number of the United States attorney, or assistant United States attorney, who requests this subpoena, are:

[REDACTED] Senior Assistant Special Counsel
Department of Justice – Special Counsel's Office

Subpoena #17-1/7006

[REDACTED]

Michael T. Flynn
[REDACTED]

c/o [REDACTED]
[REDACTED]

Covington & Burling LLP
[REDACTED]

ATTACHMENT
(Grand Jury Subpoena dated July 7, 2017)

INSTRUCTIONS:

1. In complying with this subpoena, you are required to produce all responsive devices that are in your possession, custody, or control, whether held by you or your past or present agent, employee or representative acting on your behalf. You are also required to produce devices that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as devices that you have placed in the temporary possession, custody or control of any third party.
2. No devices called for by this request shall be destroyed, modified, removed, transferred, or otherwise made inaccessible to the grand jury. If you have knowledge that any subpoenaed device has been destroyed, discarded or lost, identify the subpoenaed device and provide an explanation of the destruction, discarding, loss, or disposal, and the date at which the device was destroyed, discarded, or lost.
3. This subpoena is continuing in nature. Any device not produced because it has not been located or discovered by the return date shall be provided immediately upon location or discovery subsequent thereto with an explanation of why it was not located or discovered until the return date.
4. All responsive devices must be provided in a fully decrypted state.

DEVICES REQUESTED:

Any electronic device, including but not limited to laptops, cell phones, and electronic storage media such as USB drives, memory cards and external hard drives, that you used in connection with your work for or with Bijan Rafiekian, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc., and/or the Flynn Intel Group LLC.

In lieu of appearance, all devices produced can be directed to:

FBI Special Agent [REDACTED]
[REDACTED]

AO 110 (Rev. 06/09) Subpoena to Testify Before a Grand Jury

UNITED STATES DISTRICT COURT
for the
District of Columbia

SUBPOENA TO TESTIFY BEFORE A GRAND JURY

To: [REDACTED]

YOU ARE COMMANDED to appear in this United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place: U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
U.S. Courthouse, 3rd Floor Grand Jury #17-1
333 Constitution Avenue, N.W.
Washington, D.C. 20001

Date and Time:
07/14/2017 10:00 am

You must also bring with you the following documents, electronically stored information, or objects (*blank if not applicable*):

PLEASE SEE ATTACHED

This subpoena remains in effect until all devices are provided.

Date: 07/07/2017

CLERK OF COURT


Signature of Clerk or Deputy Clerk

The name, address, e-mail, and telephone number of the United States attorney, or assistant United States attorney, who requests this subpoena, are:

[REDACTED], Senior Assistant Special Counsel
Department of Justice – Special Counsel's Office

Subpoena #17-1/7007

[REDACTED]

Michael G. Flynn
[REDACTED]

ATTACHMENT
(Grand Jury Subpoena dated July 7, 2017)

INSTRUCTIONS:

1. In complying with this subpoena, you are required to produce all responsive devices that are in your possession, custody, or control, whether held by you or your past or present agent, employee or representative acting on your behalf. You are also required to produce devices that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as devices that you have placed in the temporary possession, custody or control of any third party.
2. No devices called for by this request shall be destroyed, modified, removed, transferred, or otherwise made inaccessible to the grand jury. If you have knowledge that any subpoenaed device has been destroyed, discarded or lost, identify the subpoenaed devices and provide an explanation of the destruction, discarding, loss, or disposal, and the date at which the device was destroyed, discarded, or lost.
3. This subpoena is continuing in nature. Any device not produced because it has not been located or discovered by the return date shall be provided immediately upon location or discovery subsequent thereto with an explanation of why it was not located or discovered until the return date.
4. All responsive devices must be provided in a fully decrypted state.

DEVICES REQUESTED:

Any electronic device, including but not limited to laptops, cell phones, and electronic storage media such as USB drives, memory cards and external hard drives, that you used in connection with your work for or with Michael T. Flynn, Bijan Rafiekian, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc., and/or the Flynn Intel Group LLC.

AO 110 (Rev. 06/09) Subpoena to Testify Before a Grand Jury

UNITED STATES DISTRICT COURT
for the
District of Columbia

SUBPOENA TO TESTIFY BEFORE A GRAND JURY

To: Bijan Rafiekian
[Redacted]

YOU ARE COMMANDED to appear in this United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place: U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
U.S. Courthouse, 3rd Floor Grand Jury #17-1
333 Constitution Avenue, N.W.
Washington, D.C. 20001

Date and Time:
07/14/2017 10:00 am

You must also bring with you the following documents, electronically stored information, or objects *(blank if not applicable)*:

PLEASE SEE ATTACHED

Personal appearance is not required if the requested devices are (1) produced on or before the return date to FBI Special Agent [Redacted] and (2) accompanied by an executed copy of the attached Declaration of Custodian of Records. This subpoena remains in effect until all devices are provided.

Date: 07/07/2017

CLERK OF COURT


Signature of Clerk or Deputy Clerk

The name, address, e-mail, and telephone number of the United States attorney, or assistant United States attorney, who requests this subpoena, are:

[Redacted], Senior Assistant Special Counsel
Department of Justice – Special Counsel's Office
[Redacted]

Subpoena #17-1/7008

Bijan Rafiekian
[REDACTED]

ATTACHMENT
(Grand Jury Subpoena dated July 7, 2017)

INSTRUCTIONS:

1. In complying with this subpoena, you are required to produce all responsive devices that are in your possession, custody, or control, whether held by you or your past or present agent, employee or representative acting on your behalf. You are also required to produce devices that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as devices that you have placed in the temporary possession, custody or control of any third party.
2. No devices called for by this request shall be destroyed, modified, removed, transferred, or otherwise made inaccessible to the grand jury. If you have knowledge that any subpoenaed device has been destroyed, discarded or lost, identify the subpoenaed devices and provide an explanation of the destruction, discarding, loss, or disposal, and the date at which the device was destroyed, discarded, or lost.
3. This subpoena is continuing in nature. Any device not produced because it has not been located or discovered by the return date shall be provided immediately upon location or discovery subsequent thereto with an explanation of why it was not located or discovered until the return date.
4. All responsive devices must be provided in a fully decrypted state.

DEVICES REQUESTED:

Any electronic device, including but not limited to laptops, cell phones, and electronic storage media such as USB drives, memory cards and external hard drives, that you used in connection with your work for or with Michael T. Flynn, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc., and/or the Flynn Intel Group LLC.

In lieu of appearance, all devices produced can be directed to:

FBI Special Agent [REDACTED]
[REDACTED]



U.S. Department of Justice
United States Attorney's Office
Eastern District of Virginia

Dana J. Boente ■ United States Attorney ■ 2100 Jamieson Avenue ■ Alexandria, VA 22314
(703) 299-3700 ■ (703) 299-3982 (fax)

April 5, 2017

VIA ELECTRONIC MAIL

Flynn Intel Group

[REDACTED] 4

Attn: Custodian of Records

c/o [REDACTED]
Covington & Burling LLP

[REDACTED]

Re: 17-2 / 17GJ0835 / 17-1075

Dear Sir or Madam:

You have been served with a subpoena issued in connection with a criminal investigation being conducted in this District. That subpoena directs you to produce certain records on April 27, 2017, before the grand jury in Alexandria, Virginia.

As a convenience, you may, if you wish, deliver the requested documents in lieu of appearing personally before the grand jury to: United States Attorney's Office, Eastern District of Virginia, 2100 Jamieson Avenue, Alexandria, VA 22314.

Any questions pertaining to the records under subpoena should be directed to [REDACTED], Trial Attorney, U.S. Department of Justice, National Security Division [REDACTED], or Assistant U.S. Attorney [REDACTED].

We appreciate your cooperation in this matter. If you have any questions or concerns, please do not hesitate to contact us.

Sincerely,

Dana J. Boente
United States Attorney

By:



Assistant United States Attorney

Enclosure

AO 110 (Rev. 06/09) Subpoena to Testify Before a Grand Jury

17-2 / 17GJ0835 / 17 - 1075

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

SUBPOENA TO TESTIFY BEFORE A GRAND JURY

Flynn Intel Group



To:

Attn: Custodian of Records for Flynn Intel Group
c/o Robert Kelner, Covington & Burling, LLP

YOU ARE COMMANDED to appear in this United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place: U.S. District Court 401 Courthouse Square Alexandria, VA 22314	Date and Time: April 27, 2017 9:30 AM
--	---------------------------------------

You must also bring with you the following documents, electronically stored information, or objects (blank if not applicable):

See Attachment.

Date: April 05, 2017

CLERK OF COURT

Signature of Clerk or Deputy Clerk

The name, address, e-mail, and telephone number of the United States attorney, or assistant United States attorney, who requests this subpoena, [Redacted], AUSA [Redacted]

Office of the United States Attorney
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314 (703) 299-3700

Flynn Intel Group

[REDACTED] 4

Attn: Custodian of Records

c/o [REDACTED] [REDACTED]

Covington & Burling LLP

[REDACTED]

ATTACHMENT – Flynn Intel Group

Please provide any and all documents and physical objects currently in the possession, custody, or control of Flynn Intel Group (“FIG”), including but not limited to contracts, bank records, communications (whether paper or electronic (email)) and attachments, internal memoranda, and any drafts thereof, relating to:

1. Articles of Incorporation;
2. Documentation or charts reflecting organizational structure;
3. Names of all employees, shareholders, members of the Board of Directors, including their title, roles/responsibilities, including contact information;
4. All contracts or written agreements with employees, stockholders, members of the Board of Directors, or members of the laboratory team;
5. Payroll records;
6. Names of all FIG clients, including contact information;
7. All contracts or written agreements between FIG and its clients;
8. All financial holdings/bank accounts/transactions associated with FIG, including corporate business accounts, credit/charge accounts, and any assets and liabilities;
9. Names of third party service providers (including S.G.R. LLC Government Relations and Lobbying, Sphere Consulting, Operational Behavioral Services, White Canvas Group, consultants, editors, public relations firms, and research firms) utilized by FIG or its third party service providers, including contact information;

10. All contracts or written agreements between FIG and third party service providers;
11. Any records, research, payments, invoices, communications, correspondence, or internal memoranda (including related drafts thereof) relating to FIG's work for or interactions with Inovo BV;
12. Any records, research, payments, invoices, communications, correspondence, or internal memoranda (including related drafts thereof) relating to FIG's work for or interactions with Ekim Alptekin;
13. Any records, research, payments, invoices, communications, correspondence, or internal memoranda (including related drafts thereof) relating to FIG's work for or interactions with Ibrahim Kurtulus;
14. Any records, research, payments, invoices, communications, correspondence, or internal memoranda (including related drafts thereof) relating to FIG's work for or interactions with individuals associated with the government of the Republic of Turkey.
15. Any records, research, payments, invoices, communications, correspondence, or internal memoranda (including related drafts thereof) relating to articles (published, unpublished, or contemplated) relating to research conducted for Inovo BV or the Republic of Turkey.

IN LIEU OF APPEARANCE, RECORDS MAY BE SENT TO:

United States Attorney's Office
Eastern District of Virginia
ATTN: [REDACTED], Assistant U.S. Attorney
2100 Jamieson Ave.
Alexandria, VA 22314
Phone: (703) 299-3700
[REDACTED]

Exhibit 3

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Columbia

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

ELECTRONIC DEVICES TO BE PROVIDED TO A GRAND JURY IN
THE DISTRICT OF COLUMBIA, IN RESPONSE TO GRAND JURY
SUBPOENA 17-1/2008, BY SUBPOENA RECIPIENT BIJAN
RAFIEKIAN A/K/A BIJAN KIAN)

Case No: 1:17-mj-477
Assigned To: Chief Judge Beryl A. Howell
Date Assigned: 7/7/2017
Description: Search and Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of COLUMBIA
(Identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A3

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

SEE ATTACHMENT B3

YOU ARE COMMANDED to execute this warrant on or before July 21, 2017 *(not to exceed 14 days)*
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell
(United States District Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized *(check the appropriate box)*

for _____ days *(not to exceed 30)* until, the facts justifying, the later specific date of _____

Date and time issued: July 7, 2017 @ 12:05 PM

Beryl A. Howell
Judge's signature

City and state: Washington, D.C.

Chief U.S. District Judge Beryl A. Howell
Printed name and title

ATTACHMENT A3

The premises to be searched consist of electronic device(s) provided to a Grand Jury in the District of Columbia, in response to Grand Jury subpoena 17-1/2008, by subpoena recipient Bijan Rafiekian, also known as Bijan Kian.

This warrant authorizes the forensic examination of the Device(s) for the purpose of identifying the electronically stored information described in Attachment B3.

ATTACHMENT B3

1. All records on the Device(s) described in Attachment A3 that relate to violations of 18 U.S.C. § 951, the Foreign Agents Registration Act, 22 U.S.C. § 611 *et seq.*, and 18 U.S.C. § 1001, and involve Michael T. Flynn, Bijan Rafiekian, Ekim Alptekin, Inovo BV, the Flynn Intel Group Inc. and/or the Flynn Intel Group LLC. (collectively, "FIG"), since January 1, 2014, including:
 - a. Communications, records, information, documents and other files that reveal efforts by Flynn, Rafiekian, Alptekin, FIG, and FIG associates to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - b. Communications, records, information, documents and other files that reveal associations between Flynn, Rafiekian, Alptekin, FIG, and FIG associates and any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - c. Records of any funds or benefits received by or offered to Flynn, Rafiekian, Alptekin, FIG, and FIG associates by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
 - d. Communications, records, information, documents and other files that pertain to representations that Flynn, Rafiekian, Alptekin, FIG, and FIG associates have made to the U.S. government;
 - e. Evidence indicating the Device owner's state of mind as it relates to the crimes under investigation;

2. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.