ELECTRONIC EVIDENCE & SEARCH WARRANT TRANSMITTAL FORM

Case No. 1:17-SW- 374 Date: June 23, 2017

(S)AUSA: Brandon Van Grack

I. TYPE OF LEGAL REQUEST:

- ☐ ECPA Grand Jury Subpoena and Non-Disclosure Order (§§ 2703(c)(2), 2705(b))
- ☐ ECPA Court Order (§ 2703(d))
- ☐ ECPA Content Search (§ 2703(a), (b)(1)(A))
- ☐ Pen Register/Trap & Trace (§ 3122(a)(1))
- ☐ PRTT/Search Warrant Hybrid (§§ 3122(a)(1), 2703(c)(1)(A))
- ☐ Regular Search Warrant (Rule 41(e)(2)(A))
- ☒ ESI Search Warrant (Rule 41(e)(2)(B))
- ☐ Tracking Device Search Warrant (Rule 41(e)(2)(C))
- ☐ Other _____

II. INFORMATION TO BE OBTAINED OR ITEMS TO BE SEARCHED/SEIZED:

- ☐ Cell Phone Account from Provider
- ☐ Land Line Account from Provider
- ☒ Email Account from Provider
- ☐ IP Address from Provider
- ☐ Real-Time Cell Site Records from Provider
- ☐ Social Media/Messaging Account from Provider
- ☐ Computer/Laptop/Hard Drive/Cell Phone (Rule 41(e)(2)(A))
- ☐ Tracking Device (Rule 41(e)(2)(C))
- ☐ Premises/Property/Vehicle (Rule 41(e)(2)(A))
- ☐ Other _____

III. INVESTIGATIVE OFFENSE:

- ☐ Drugs
- ☐ Extortion/Racketeering
- ☐ Fraud
- ☐ Fugitive/Escape
- ☐ Immigration
- ☐ Kidnapping
- ☐ Sex Offenses
- ☐ Tax
- ☐ Terrorism
- ☐ Theft
- ☐ Weapons
- ☒ Other _18 U.S.C. § 951; 22 U.S.C. § 611 *et seq.* (FARA)

IV. DELAYED NOTICE:

☒ ECPA Non-Disclosure (§§ 2703(d), 2705(b))

☒ Initial – 2 years ☐ Renewal

☐ ECPA Non-Disclosure for Priority Terrorism Enterprise Investigations (§§ 2703(d), 2705(b))

☐ Initial – 3 years ☐ Renewal

☐ PRTT Non-Disclosure (§§ 3123(d)(2))

☐ Initial – 5 years ☐ Renewal

☐ Search Warrant Delayed Notice (§ 3103a(b), Rule 41(f)(3))

☐ Rule 41(e)(2)(A), (B), or (C) Warrants

☐ § 2703(a), (b)(1)(A), or (c)(1)(A) Searches

_____ Days

_____ Days Extension

Updated: 5/2/17

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH MULTIPLE EMAIL ADDRESSES THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE	)	Case No. 1:17-SW-374

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

See Attachment A.

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

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 7, 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. Theresa C. Buchanan
(United States Magistrate Judge)

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

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

Date and time issued: 6/23/17 3:10 pm

Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Hon. Theresa C. Buchanan, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Target Accounts listed below that are contained in the following Google Suite (G Suite) services:

Gmail: Custom Business Email
Calendar: Scheduling for Teams
Google+: Social Network for Business
Hangouts/Meet: Video meetings
Docs: Documents with real-time co-editing
Sheets: Online spreadsheets
Forms: Surveys and forms
Slides: Presentations
Sites: Easy-to-build websites
Jamsboard: a collaborative, digital whiteboard
Drive: Secure cloud storage and file sharing
Google Cloud Search: Search across G Suite
Admin: Manage user, device, and security settings
Vault: Archive, search, and export information
Mobile: Secure data with mobile device management

that are stored at premises owned, maintained, controlled, or operated by Google, a company which accepts legal process at 1600 Ampitheater Parkway, Mountain View, California.

Target Accounts:

[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]ames@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com

(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) @Flynnintelgroup.com
(b)(6), (b)(7)(C) @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) per F @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FB @Flynnintelgroup.com
(b)(6), (b)(7)(C) per F @Flynnintelgroup.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 5, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents (including attachments) of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number(s));

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of 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, occurring after January 1, 2013, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, records, documents and other files that reveal efforts by Flynn, FIG, FIG associates, or the users of the **Target Accounts** 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, documents and other files that reveal associations between Flynn, FIG, FIG associates, or the users of the **Target Accounts** 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, FIG, FIG associates, or the users of the **Target Accounts** by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

d. Communications, records, documents and other files that pertain to representations that Flynn, FIG, FIG associates, or the users of the **Target Accounts** have made to the U.S. government;

e. Documents or presentations created by the users of the **Target Accounts** on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

f. Communications, records, documents and other files that reveal efforts by Flynn, FIG, FIG associates, or the users of the **Target Accounts** to mask sources of funds or income;

g. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

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

i. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and

j. The identity of any person(s)—including records that help reveal the person(s)' whereabouts—who communicated with the account about any matters relating to activities conducted by Flynn, FIG, FIG associates, or the users of the **Target Accounts** on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [redacted]@FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted]@ FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted]@FLYNNINTELGROUP.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE	2017 **UNDER SEAL** Case No. 1:17-SW-374

ORDER TO SEAL AND FOR
NONDISCLOSURE PURSUANT TO 18 U.S.C. § 2705(b)

The United States, pursuant to Local Rule 49(B) of the Local Criminal Rules for the U.S. District Court for the Eastern District of Virginia and 18 U.S.C. § 2705(b), having moved to seal the search warrant, application, supporting affidavit, motion to seal, and this Order, and having further moved for a § 2705(b) nondisclosure order covering these materials;

The Court, having considered the government's submissions, including the facts presented by the government to justify sealing; having determined that that there is reason to believe that notification of the existence of these materials will seriously jeopardize the ongoing investigation, including by giving the subjects an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence or witnesses, change patterns of behavior, or notify confederates, if any, *see* 18 U.S.C. §§ 2705(b)(2), (3), & (5); having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing; finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED that the United States' motion is GRANTED, and the search warrant, application, supporting affidavit, motion to seal, and this Order be SEALED until further order of the Court.

IT IS FURTHER ORDERED under 18 U.S.C. § 2705(b) that Google or its affiliates shall not disclose the existence of these materials to any person or entity, for a period of two years from the date of this Order, except that Google may disclose this Order to law enforcement officers of the Federal Bureau of Investigation as part of its cooperation with law enforcement agents to execute the search warrant. This non-disclosure order is subject to further renewal upon a proper showing under 18 U.S.C. § 2705(b).

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Date: June 23, 2017

Hon. Theresa C. Buchanan
United States Magistrate Judge

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

3 2017

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
IINFORMATION ASSOCIATED WITH MULTIPLE EMAIL ADDRESSES THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE

Case No. 1:17-SW-374

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 Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

This warrant is sought pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A).

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 951;	Acting as a foreign agent without notice to the Attorney General;
22 U.S.C. § 611 et seq.	Foreign Agents Registration Act
18 U.S.C. § 1001	False Statements

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ 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.

(b)(6), (b)(7)(C) per FBI

Applicant's signature

Reviewed by AUSA/SAUSA:

SAUSA Brandon Van Grack

(b)(6), (b)(7)(C) per FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 06/23/2017

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

Hon. Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Target Accounts listed below that are contained in the following Google Suite (G Suite) services:

Gmail: Custom Business Email
Calendar: Scheduling for Teams
Google+: Social Network for Business
Hangouts/Meet: Video meetings
Docs: Documents with real-time co-editing
Sheets: Online spreadsheets
Forms: Surveys and forms
Slides: Presentations
Sites: Easy-to-build websites
Jamsboard: a collaborative, digital whiteboard
Drive: Secure cloud storage and file sharing
Google Cloud Search: Search across G Suite
Admin: Manage user, device, and security settings
Vault: Archive, search, and export information
Mobile: Secure data with mobile device management

that are stored at premises owned, maintained, controlled, or operated by Google, a company which accepts legal process at 1600 Ampitheater Parkway, Mountain View, California.

Target Accounts:

[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com

(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) @Flynnintelgroup.com
(b)(6), (b)(7)(C) pe @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) per F @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) per F @Flynnintelgroup.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 5, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents (including attachments) of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number(s));

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of 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, occurring after January 1, 2013, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, records, documents and other files that reveal efforts by Flynn, FIG, FIG associates, or the users of the **Target Accounts** 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, documents and other files that reveal associations between Flynn, FIG, FIG associates, or the users of the **Target Accounts** 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, FIG, FIG associates, or the users of the **Target Accounts** by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

d. Communications, records, documents and other files that pertain to representations that Flynn, FIG, FIG associates, or the users of the **Target Accounts** have made to the U.S. government;

e. Documents or presentations created by the users of the **Target Accounts** on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

f. Communications, records, documents and other files that reveal efforts by Flynn, FIG, FIG associates, or the users of the **Target Accounts** to mask sources of funds or income;

g. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

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

i. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and

j. The identity of any person(s)—including records that help reveal the person(s)' whereabouts—who communicated with the account about any matters relating to activities conducted by Flynn, FIG, FIG associates, or the users of the **Target Accounts** on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [redacted]@FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted]@ FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted]@ FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted] FLYNNINTELGROUP.COM [redacted]@ FLYNNINTELGROUP.COM [redacted]@FLYNNINTELGROUP.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE	**UNDER SEAL** Case No. 1:17-SW-374

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, [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 for a search warrant for information associated with email accounts: [redacted]@ FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted]@ FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted]@ FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted]@ FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted]@FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; [redacted] FLYNNINTELGROUP.COM; and [redacted]@FLYNNINTELGROUP.COM (hereafter the "**Target Accounts**") that is stored at premises controlled by Google, an email provider which accepts legal process at 1600 Ampitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Attachment A. Upon receipt of the information described in Attachment A, government-authorized persons will review that information to locate the items described in Attachment B.

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, DC.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. 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 ("Flynn") and individuals working for or with Flynn and the FLYNN INTEL GROUP, INC. ("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, 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 Attachment A for evidence, contraband, fruits, and/or instrumentalities of these crimes, further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *Id.* §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating Flynn, 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, Flynn, 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 Flynn, FIG, and FIG associates masked the fact that they were working at the direction 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, Flynn's and FIG's work with Inovo focused almost exclusively on Fethullah Gulen, a cleric whom the Government of Turkey blames for a failed coup attempt in that country that occurred in July 2016.

7. Under the Foreign Agents Registration Act ("FARA"), any persons acting "at the order, request, or under the direction or control of a foreign principal" and who engages within the United States in political activities in the interests of such foreign principal must register with the Attorney General. *See* 22 U.S.C. § 611, *et seq.* It is also against the law to

willfully make a false statement of a material fact or omit a material fact in that registration statement. *See* 22 U.S.C. § 218.

8. 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.

9. There is also probable cause to believe that Flynn made material misstatements on multiple government forms with respect his work on behalf of other foreign nationals, foreign entities, and foreign governments. Specifically, and as discussed further below, in 2016, Flynn failed to disclose income he received from foreign entities and associations he had with foreign individuals and entities on his Questionnaire for National Security Positions (Form SF 86). Additionally, in 2017, Flynn failed to disclose income he received from foreign entities on one of his Public Financial Disclosure Reports.

10. In furtherance of this investigation, the FBI has obtained information through interviews, legal process issued by a grand jury in Alexandria, Virginia, and public filings of relevant documents. Through a review of this information, the FBI has learned the following information about Flynn and FIG's work with Alptekin, Inovo, the Government of Turkey, and Russian entities.

A. Unregistered Foreign Agents

11. Flynn started his own company soon after being honorably discharged from the military in September 2014. On or about June 2015, Flynn, Bijan Rafiekian (aka Bijan Kian)

("Kian"), and [redacted] incorporated FIG in Delaware, with its principal address at [redacted]

12. The FIG Board of Directors were Flynn, Kian, and [redacted] Flynn was the Chairman and CEO; Kian was the Vice Chairman, and [redacted] was the President.

i. FIG Utilized G Suite for its Business Operations

13. Based on information provided by FIG, to include email correspondence and financial records, as well as interviews of a relevant FIG associate, I am aware that FIG used G Suite as a platform for email communications, and the transmission of documents, and other business functions in support of the project with Alptekin and Inovo.

14. Based on my experience and open source research, I am aware that Google promotes G Suite to businesses as providing an all-in-one solution to their online business needs. By utilizing G Suite, according to Google, businesses can take advantage of more than just Google email services; they can share and store documents, presentations, calendars, and contact lists. Open source information advertises G Suite as:

> a brand of cloud computing,.productivity and collaboration tools, software and products developed by Google. G Suite comprises Gmail, Hangouts, Calendar, and Google+ for communication; Drive for storage; Docs, Sheets, Slides, Forms, and Sites for collaboration; and, depending on the plan, an Admin panel and Vault for managing users and the services. It also includes the digital interactive whiteboard Jamboard.
>
> G Suite adds enterprise features such as custom email addresses at a domain (@yourcompany.com), option for unlimited cloud storage, additional administrative tools and advanced settings, as well as 24/7 phone and email support.

15. On or about May 30, 2017, in response to legal process, attorneys for Flynn advised me that [redacted], a FIG associate, told them that FIG utilized G Suite as a platform for its email service using the domain name "@flynnintelgroup.com." This fact has been corroborated by my review of FIG's business records, which include emails by FIG employees

and associates utilizing the domain "@flynnintelgroup.com." Flynn's attorneys also indicated that FIG did not possess or utilize its own servers to conduct business – other than the servers provided by Google pursuant to FIG's contract with G Suite - nor did FIG issue any computers, phones, or devices to its employees and associates. This fact has been corroborated by an interview I conducted of an individual who shared office space with FIG, and confirmed that, to the best of that individual's knowledge, employees were not issued any electronic devices by FIG and that FIG utilized Google for its online business needs.

16. On or about May 30, 2017, the FBI interviewed [redacted], who confirmed that FIG utilized the G Suite as a platform for its email communications and other online business services. [redacted] advised that he assumed the responsibility for managing FIG's G Suite account at the request of [redacted] at FIG.

17. Based on information from FIG's FARA filing, I am aware that on or about November 30, 2016, FIG ceased to do business. A review of documents provided by the FIG in response to legal process identified an email from [redacted] to FIG employees and associates. The email advised them that as of November 30, 2016, FIG emails accounts would be shut down. [redacted] directed the employees and associates to "take appropriate actions in saving any Google Drive documents, contacts, or correspondence you might want to keep prior to that date." The FIG email addresses identified in the [redacted] email are the **Target Accounts** listed in this application.

18. A review of financial documents identified multiple payments from FIG's bank account to Google under the title of Flynn Intel Group, Inc. Based on open source research, I am aware that Google offers G suite services to businesses at a minimum price of $5 per user per

month and at higher prices depending on what specific G Suite services are utilized by the business.

ii. Turkey Seeks Gulen's Extradition from the United States

19. 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 attempt. Gulen lives in the United States and operates a network of charter schools.

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

iii. FIG Receives Approval from the Government of Turkey to Investigate Gulen and Promote Stability in Turkey

21. On or about July 27, 2016, Kian using (b)(6), (b)(7) @flynnintelgroup.com 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 "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.

22. 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 at (b)(6), (b)(7) @flynnintelgroup.com 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.

23. On or about August 8, 2016, Alptekin emailed Flynn at [redacted]@flynnintelgroup.com and Kian at [redacted]@flynnintelgroup.com 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 Minster Binali Yildirim.

24. On or about August 10, 2016, Alptekin emailed Kian at [redacted]@flynnintelgroup.com and Flynn at [redacted]@flynnintelgroup.com that he had had several meetings with the Turkish Ministers of Economy and Foreign Affairs, and he (Alptekin) has "a green light to discuss confidentiality, budget and the scope of the contract."

iv. FIG and Alptekin Agree to Provide Alptekin with 20% of Any Funds Received for the Turkey Project

25. 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 it signed the Inovo contract whereby Alptekin would receive 20% of any funds FIG received from 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.

26. On or about August 11, 2016, Kian using kian@flynnintelgroup.com informed 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."

27. On or about August 25, 2016, Kian sent an email indicating that Alptekin's company, Inovo, would be the official client for FIG's project related to Turkey. Specifically, Kian using [redacted]@flynnintelgroup.com emailed Alptekin, and copied Flynn at [redacted]@flynnintelgroup.com, to thank 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."

28. On or about September 3, 2016, Kian using [redacted]@flynnintelgroup.com emailed Alptekin, and copied Flynn at [redacted]@flynnintelgroup.com, with an agreement between Inovo and FIG. Kian stated to Alptekin that "we have been at work on this engagement since July 31st."

29. On or about September 8, 2016, Alptekin emailed Kian at [redacted]@flynnintelgroup.com 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.

30. 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.

31. On or about September 12, 2016, Kian using [redacted]@flynnintelgroup.com emailed Flynn at [redacted]@flynnintelgroup.com and (b)(6), (b)(7)(C) per FBI at [redacted]@flynnintelgroup.com 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 the Alptekin was performing those services under Inovo, and signed by Flynn on October 30, 2016.

32. 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.

33. On or about October 7, 2016, Kian using [redacted]@flynnintelgroup.com emailed Alptekin an invoice for $200,000 for the "Confidence Project."

34. On or about October 11, 2016, according to FIG bank records, Alptekin transferred $185,000 to FIG.

35. On or about October 13, 2016, Kian using [redacted]@flynnintelgroup.com emailed Flynn ([redacted]@flynnintelgroup.com), (b)(6), (b)(7)(C) per FBI ([redacted]@flynnintelgroup.com) and Alptekin, requesting that (b)(6), (b)(7)(C) per FBI wire transfer $40,000 from FIG to Inovo "as soon as Mr. Alptekin sends us an invoice for consulting services that he is providing to FIG on the Confidence project."

36. On or about October 15, 2016 Kian emailed an invoice from Inovo for $40,000 to (b)(6), (b)(7)(C) per FBI at [redacted]@flynnintelgroup.com with copies to Alptekin and Flynn at [redacted]@flynnintelgroup.com.

37. On or about October 17, 2016, six days after Alptekin transferred $185,000 to FIG, FIG wire transferred $40,000 to Inovo for work associated with the "Confidence Project."

38. On or about November 10, 2016, Kian using [redacted]@flynnintelgroup.com emailed Alptekin a third invoice for the "Confidence Project." In the email, Kian advised that Inovo was owed $55,000 for "research and consultation services," and requested an invoice to that affect from Alptekin. The attachment with this email is an invoice from FIG to Alptekin for $200,000.

39. On or about November 14, 2016, according to FIG bank records, Alptekin transferred $145,000 to FIG. Based on the previous email, I believe that Alptekin deducted $55,000 from the scheduled $200,000 payment to FIG to arrive at a payment of $145,000.

40. 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 during September and October 2016.

v. FIG's Work Exclusively Focused on Gulen and Promoting Stability in Turkey

41. 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. 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.

42. On or about September 5, 2015 Kian, using [redacted]@flynnintelgroup.com, emailed Flynn at [redacted]@flynnintelgroup.com about 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.

43. On or about September 6, 2016, Kian using [redacted]@flynnintelgroup.com emailed (b)(6), (b)(7)(C) per FBI ([redacted]@flynnintelgroup.com) and Flynn ([redacted]@flynnintelgroup.com), and advised that the "client is seeking a high level meeting in NYC on September 19th or 20th."

44. On or about September 18, 2016, Kian, using [redacted]@flynnintelgroup.com, emailed Flynn at [redacted]@flynnintelgroup.com background material and talking points for a planned meeting in New York the following day. The attachment included a series of questions regarding Gulen and drew comparisons between Gulen and the late Ayatollah Khomeini of Iran.

45. On or about September 19, 2016, according to publicly filed documents and interviews conducted by the FBI, Kian, Flynn, Brian McCauley, 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. 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.

46. On or about September 21, 2016, Kian using [redacted]@flynnintelgroup.com emailed Flynn at [redacted]@flynnintelgroup.com and advised that he had met with Alptekin and that the feedback from the earlier meeting was "positive." Nevertheless, Kian was concerned about

expectations that Alptekin had shared, and indicated that he would find out "what caused the elevated expectation on their side tomorrow." (Emphasis added).

47. On or about October 21, 2016, Kian used [redacted]@flynnintelgroup.com to email Alptekin copies of proposed board games for Project Confidence entitled "Gulenopoly" and "Mula Mullah." Because Gulen is a religious cleric, and the term "mullah" is sometimes used to refer to Muslim clerics, I believe the titles of both board games contain references to Gulen. In the email, Kian opines that Gulen is destabilizing Turkey.

48. 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 earlier, Kian using [redacted]@flynnintelgroup.com emailed a version of that op-ed to Alptekin and Bob Kelley, FIG General Counsel, at [redacted]@flynnintelgroup.com.

vi. Multiple Persons Worked with FIG on its Project for the Government of Turkey

49. Based on a review of emails from FIG, including the September 5, 2016 email from Kian in which he identified the team members for "Operation CONFIDENCE," there were multiple persons associated with FIG involved in this project. In the above-referenced email alone, Kian identified "senior team members" of the team to include as [redacted] "JW", "Brian McCauley", and "Mike Boston." Based on my knowledge of this investigation, I believe [redacted] is short for [redacted]; and JW is short for James Woolsey.

50. Based on a review of material submitted by FIG pursuant to legal process, I am aware that Michael Boston is a FIG Principal, and utilized the FIG-provided email address [redacted]@flynnintelgroup.com. There are multiple instances in which he utilized that email address as part of the project with Alptekin and Inovo. For example, on or about October 4, 2016, Boston used [redacted]@flynnintelgroup.com to communicate with Kian, Brian McCauley,

[redacted] ([redacted]@flynnintelgroup.com), [redacted] ([redacted]@flynnintelgroup.com), and [redacted] ([redacted]@flynnintelgroup.com) to schedule a meeting for the project. Boston communicated that the "project is moving along rapidly" and they needed to meet to sync the work of the various groups.

51. Boston, using [redacted]@flynnintelgroup.com, circulated documents and presentations pertaining to the project with Alptekin and Inovo. For example, on or about October 22, 2016, Boston used [redacted]@flynnintelgroup.com to send multiple documents to Flynn at [redacted]@flynnintelgroup.com. Based on the titles of the documents, I believe the documents were related to the Inovo project. Additionally, on or about October 31, 2016, Boston used [redacted]@flynnintelgroup.com to communicate with other FIG associates engaged in the project and attached a Power Point presentation and PDF document to the email. The recipients of this email included [redacted] ([redacted]@flynnintelgroup.com), [redacted] ([redacted]@flynnintelgroup.com), and Kian ([redacted]@flynnintelgroup.com).

52. There are also multiple instances in which Brian McCauley, a FIG associate who led FIG's investigation of Gulen, utilized [redacted]@flynnintelgroup.com. For example, on or about September 23, 2016, Kian emailed McCauley at [redacted]@flynnintelgroup.com with an attachment labeled "OPEN SOURCE INFORMATION – PROJECT CONFIDENCE." Additionally, on or about November 6, 2016, [redacted]@flynnintelgroup.com was included in a communication among Alptekin, Kian, Boston, and Flynn in which documents were transmitted to Alptekin.

53. [redacted] also received communications regarding the Inovo contract at a FIG-provided email account. On or about August 12, 2016, Kian using [redacted]@flynnintelgroup.com emailed [redacted] at [redacted]@flynnintelgroup.com and Flynn regarding

the costs for the Inovo contract. Attached to the email was a spreadsheet labeled "Costs and revenue pro forma." Kian wrote in the email that there was a cost for "Senior Advisor" and that term COGS refers to this cost. A review of the spreadsheet reflected an entry for COGS at 20% of $200,000. Based on my knowledge of this investigation, I believe that the entry COGS payment is Alptekin's 20% advisory fee.

vi. FIG Makes Material False Statements and Omits Material Facts on its FARA Filing

54. 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.

55. 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 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.

56. 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. Kian made similar denials in emails to Alptekin.

57. When certain media outlets reported on $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 not 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."

B. Other Material False Statements

58. In addition to failing to properly disclose to the United States government his and FIG's work with the Government of Turkey, Flynn appears to have made material misstatements on multiple government forms with respect his work on behalf of other foreign nationals, foreign entities, and foreign governments.

59. On or about December 10, 2015, Flynn traveled to Moscow, Russia, to speak at an event for RT, a media organization with ties to the Government of Russia. According to records from the company who helped arrange Flynn's participation, Flynn was paid $33,750 to attend and speak at the event. Open source reporting indicates that at the event Flynn sat at the same table as Russian President Vladimir Putin.

60. On or about January 21, 2016, Flynn submitted and electronically signed an SF-86 for the Defense Intelligence Agency ("DIA"), in order to maintain his security clearance. On the SF-86, and in subsequent representations to the DIA, Flynn did not disclose that he had received $33,750 from RT. On or about February 11, 2016, in an interview with a background investigator for his security clearance, Flynn acknowledged traveling to Russia to speak at a conference for the Russian media, but he did not disclose to the interviewer that he was paid $33,750 for his work.

61. On or about August 19, 2015, Flynn spoke at an event in Washington, DC, for which he was paid $11,250 by Volga Dnepr Airlines. Flynn's participation in the event was booked through the speaking firm Leading Authorities Inc. According to open source information, Volga Dnepr Airlines is based in Ulanovsk, Russia, and specializes in air charter services. The event at which Flynn spoke was a Middle East & African Logistical Security Conference.

62. On or about October 20, 2015, Flynn was a keynote speaker for Eugene Kaspersky's Government Cybersecurity Forum in Washington, DC, for which he was paid $11,250. According to open source information Kaspersky is a Russian national and Chairman and CEO of Kaspersky Labs. Additional open source research reflects that Kaspersky was educated at a KGB-sponsored cryptography institute.

63. On or about February 11, 2017, pursuant to his selection as National Security Advisor, Flynn submitted and electronically signed a Public Financial Disclosure Report for the U.S. Office of Government Ethics. On that report, Flynn did not disclose his speaking engagements with, and payments received from RT, Volga-Dnepr Airlines and Kaspersky Government Solutions.

64. On or about March 31, 2017, after Flynn resigned as National Security Advisor and extensive public reporting about his work for foreign principals and entities, Flynn filed a second Public Financial Disclosure Report, which disclosed his paid work for RT, Volga-Dnepr Airlines, and Kaspersky Government Solutions.

65. Based on the evidence described above, there is probable cause to believe that G Suite records associated with FIG and the **Target Accounts** contain information pertaining to FIG's work with Inovo, Alptekin, and the Government of Turkey. That conclusion is supported

by the fact numerous FIG employees and associates utilized G Suite email addresses to communicate, transmit documents, transmit slide presentations, and schedule meetings and because the investigation to date has failed to identify any other online services or service provider that supported FIG's work.

BACKGROUND CONCERNING EMAIL

66. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, but also offers customers using G Suite a unique domain name, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

67. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

68. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number(s)). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

69. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

70. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically

retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

71. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.[1]

72. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled

[1] It is possible that Google stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Google. The government also seeks the disclosure of the physical location or locations where the information is stored.

the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crimes under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

73. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

74. I further request that the Court order that all papers in support of this application, including the application, affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

(b)(6), (b)(7)(C) per FBI

Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 23rd day of June, 2017.

The Honorable Theresa C. Buchanan
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Target Accounts listed below that are contained in the following Google Suite (G Suite) services:

Gmail: Custom Business Email
Calendar: Scheduling for Teams
Google+: Social Network for Business
Hangouts/Meet: Video meetings
Docs: Documents with real-time co-editing
Sheets: Online spreadsheets
Forms: Surveys and forms
Slides: Presentations
Sites: Easy-to-build websites
Jamsboard: a collaborative, digital whiteboard
Drive: Secure cloud storage and file sharing
Google Cloud Search: Search across G Suite
Admin: Manage user, device, and security settings
Vault: Archive, search, and export information
Mobile: Secure data with mobile device management

that are stored at premises owned, maintained, controlled, or operated by Google, a company which accepts legal process at 1600 Ampitheater Parkway, Mountain View, California.

Target Accounts:

[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]ack@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com
[redacted]@Flynnintelgroup.com

(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) @Flynnintelgroup.com
(b)(6), (b)(7)(C) p @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) per F @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FBI @Flynnintelgroup.com
(b)(6), (b)(7)(C) per FB @Flynnintelgroup.com
(b)(6), (b)(7)(C) per F @Flynnintelgroup.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 5, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents (including attachments) of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number(s));

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of 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, occurring after January 1, 2013, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, records, documents and other files that reveal efforts by Flynn, FIG, FIG associates, or the users of the **Target Accounts** 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, documents and other files that reveal associations between Flynn, FIG, FIG associates, or the users of the **Target Accounts** 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, FIG, FIG associates, or the users of the **Target Accounts** by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

d. Communications, records, documents and other files that pertain to representations that Flynn, FIG, FIG associates, or the users of the **Target Accounts** have made to the U.S. government;

e. Documents or presentations created by the users of the **Target Accounts** on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

f. Communications, records, documents and other files that reveal efforts by Flynn, FIG, FIG associates, or the users of the **Target Accounts** to mask sources of funds or income;

g. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

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

i. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and

j. The identity of any person(s)—including records that help reveal the person(s)' whereabouts—who communicated with the account about any matters relating to activities conducted by Flynn, FIG, FIG associates, or the users of the **Target Accounts** on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and

c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH

[redacted]@FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted]@ FLYNNINTELGROUP.COM
[redacted]@ FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted]@ FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted] FLYNNINTELGROUP.COM
[redacted]@FLYNNINTELGROUP.COM

THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE

- 3 2017

UNDER SEAL

Case No. 1:17-SW-374

UNITED STATES' MOTION TO SEAL AND
FOR 18 U.S.C. § 2705(b) NONDISCLOSURE ORDER

The United States of America, pursuant to Local Rule 49(B) of the Local Criminal Rules for the U.S. District Court for the Eastern District of Virginia, now asks for an order to seal the search warrant, application, supporting affidavit, and this motion and proposed order, until the United States makes a motion to unseal these materials. In addition, pursuant to 18 U.S.C. §

2705(b), the United States asks this Court to order Google not to disclose the existence of these materials except to the Federal Bureau of Investigation as part of its cooperation with law enforcement agents to execute the search warrant until such time as the materials are unsealed.

I. Reasons for Sealing (*See* Local Rule 49(B)(1))

1. At the present time, law enforcement officers of the Federal Bureau of Investigation are conducting an investigation into violations related to 18 U.S.C. § 951 (acting as a foreign agent without notice to the Attorney General), the Foreign Agents Registration Act, 22 U.S.C. § 611 *et seq*, and 18 U.S.C. § 1001 (making a material false statement). It does not appear all of the individuals involved in the investigation are currently aware that they are subjects of the investigation.

2. Premature disclosure of the specific and sensitive details of this ongoing investigation would jeopardize this ongoing criminal investigation, including by giving the subjects an opportunity to flee prosecution, destroy or tamper with evidence and witnesses, change patterns of behavior, and notify confederates, if any. In addition, given the nature of the crimes under investigation and the status of the investigation, the specific details of the evidence included in the affidavit necessarily contain sensitive law enforcement information about an ongoing and proactive investigation. If such information were made public at this time, it would jeopardize the ongoing investigation by alerting the person suspected of engaging in criminal conduct of undercover law enforcement activity and other information known to law enforcement. Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. The Governing Law (*See* Local Rule 49(B)(2))

4. It is generally recognized that the public has a common-law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrants and orders issued pursuant to 18 U.S.C. § 2703. *See In re Application of the United States of America for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 292 (4th Cir. 2013); *Media Gen. Operations, Inc. v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005). To substantively overcome the common law presumption of access to search warrant materials, a court must find that there is a "significant countervailing interest" in support of sealing that outweighs the public's interest in openness. *In re Application*, 707 F.3d at 293, *citing Under Seal v. Under Seal*, 326 F.3d 479, 486 (4th Cir. 2003).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. *Ashcraft v. Conoco, Inc.*, 218 F.3d 288, 302 (4th Cir. 2000).

6. Regarding the notice requirement in the specific context of search warrants, the Fourth Circuit has cautioned that "the opportunity to object" cannot "arise prior to the entry of a sealing order when a search warrant has not been executed." *Media Gen. Operations*, 417 F.3d at 429. "A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search

warrant." *Id.* Accordingly, in the context of search warrants, "the notice requirement is fulfilled by docketing 'the order sealing the documents,' which gives interested parties the opportunity to object after the execution of the search warrants." *Id.* at 430 (quoting *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 65 (4th Cir. 1989)); *see also* Local Rule 49(B) ("Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.").

7. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that "'in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,'" *Media Gen. Operations*, 417 F.3d at 430 (quoting *Goetz*, 886 F.2d at 65), so long as the ultimate "decision to seal the papers . . . [is] made by the judicial officer," *Goetz*, 886 F.2d at 65. Moreover, "[i]f appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." *Id.* at 65; *see also In re Wash. Post Co.*, 807 F.2d 383, 391 (4th Cir. 1986) ("[I]f the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal."). The government's interest in sealing may be supported by a desire to maintain the secrecy of the investigation, preventing the potential subject from being tipped off, or altering behavior to thwart the government's ongoing investigation. *In re Application*, 707 F.3d at 293.

III. Period of Time the United States Seeks to Have Matter Remain Under Seal (*See* Local Rule 49(B)(3))

8. Pursuant to Local Rule 49(B)(3), the search warrant materials will remain sealed until the need to maintain the confidentiality of these materials and the related investigation expires, after which time the United States will move to unseal the materials.

9. Notwithstanding this motion to seal, the United States requests authorization to provide copies as necessary to execute the application.

IV. Reasons for Order of Nondisclosure Pursuant to 18 U.S.C. § 2705(b)

10. Pursuant to 18 U.S.C. § 2705(b), this Court may order Google not to notify any other person or entity (including any customer) of the existence of a search warrant issued pursuant to § 2703 for such times as this Court deems appropriate, so long as this Court finds that there is reason to believe such notification would result in, among other factors, "flight from prosecution," "destruction of or tampering with evidence," or "otherwise seriously jeopardizing an investigation." *Id.* at §§ 2705(b)(2), (3), & (5).

11. In this case, there is reason to believe that notification to any person or entity of the existence of the search warrant would result in flight from prosecution and destruction of or tampering with evidence or witnesses. This is because the investigation is ongoing and because the subjects, who are unaware of the ongoing investigation, may, upon becoming aware of investigation, flee or destroy and delete electronic and other evidence of their illegal actions. In addition, a notified subject may also alert other subjects involved in the criminal activity, if any, thus seriously jeopardizing the investigation.

WHEREFORE, the United States respectfully requests that the search warrant, application, supporting affidavit, and this motion and proposed order, be sealed until the United States makes a motion to unseal. The United States further requests that the Court order Google not to notify any person or entity, including any of its customers, of the existence of the search warrant and related materials except to law enforcement officers of the Federal Bureau of Investigation as part of its cooperation with law enforcement agents to execute the search

warrant, pursuant to 18 U.S.C. § 2705(b), for the period of two years from the date of this Order, subject to renewal upon a proper showing under 18 U.S.C. § 2705(b).

Date: June 23, 2017

Respectfully submitted,

Dana J. Boente
United States Attorney

By: _____

Brandon L. Van Grack
Special Assistant U.S. Attorney (LT)
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Ave.
Alexandria, VA 22314
Tel. (b)(6), (b)(7)(C) per FBI
Fax. (b)(6), (b)(7)(C) per FBI
(b)(6), (b)(7)(C) per FBI