UNITED STATES DISTRICT COURT

for the

District of Colorado

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The e-mail account known as kevin.kuciapinski@mac.com that is in the possession of Apple Inc., whose office is located at 1 Infinite Loop, Cupertino, California, 95014-2084, more fully described in Attachment A	Case No. 17-sw-5770-CBS

APPLICATION FOR A SEARCH WARRANT

I am 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 attached hereto and hereby incorporated by reference.

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

See Attachment B attached hereto and hereby incorporated by reference.

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. § 371	Conspiracy

The application is based on these facts:

See Attachment C and Affidavit attached hereto and hereby incorporated by reference.

- ☑ Continued on the attached affidavit, which is incorporated by reference.
- ☐ 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.

s/ Dana Grant
Applicant's signature

Dana Grant, Special Agent, Air Force OSI
Printed name and title

Sworn to before me and: ☐ signed in my presence.

☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: ***3:32 pm, Jun 02, 2017***

Judge's signature

City and state: Denver, Colorado

Craig B. Shaffer
United States Magistrate Judge
Printed name and title

Affidavit in Support of a Search Warrant Application

I, Dana Grant**,** being duly sworn, hereby depose and state the following:

Introduction

1. I am a Special Agent with the Air Force Office of Special Investigations (AFOSI) and have been since March 9, 2005. I am currently assigned to Buckley Air Force Base within the Office of Procurement Fraud. Over the course of my employment with AFOSI, I have investigated a wide variety of fraud matters including false claims, false statements, public corruption, counterfeit parts, and other white collar matters. I have been investigating fraud since the beginning of my AFOSI career. At all times during the investigation, described herein, I have acted in my official capacity as a Special Agent of AFOSI.
2. This affidavit is made pursuant to Title 18, USC (USC), Section 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), in support of an application for a warrant to search the email account titled kevin.kuciapinski@mac.com maintained by KEVIN KUCIAPINSKI (SUBJECT ACCOUNT) and all content found therein, there being probable cause to believe that located in the place described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of Title 18 USC, Section 371. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that evidence, fruits, and instrumentalities of violations of Title 18 USC, Section 371, are present at the location described.

3. The information contained in this affidavit is based on, among other things, my personal knowledge and observations during the course of this investigation, information received from other government agencies and officials including the National Reconnaissance Office (NRO), information received from other law enforcement agencies and officials such as the NRO Office of Inspector General (OIG), and my review of records, documents and other evidence obtained during this investigation. I also rely on information provided to me by NRO Investigator Donna Ennis.
4. Due to my training, my experience and this investigation, I am also familiar with the internet and service providers. Moreover, references to my experience include my discussions with other law enforcement officers who also have such experience with the internet and service providers.

Relevant Statutes

5. This investigation concerns alleged violations of Title 18 USC, Section 371 (Conspiracy to commit offense or to defraud United States).
6. Title 18 USC, Section 371 (Conspiracy to commit offense or to defraud United States) prohibits two or more persons from conspiring to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy.

Definitions

7. The following definitions apply to this Affidavit and Attachment B to this Affidavit.

8. **The Internet**

a. The "Internet" is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web is a functionality of the Internet which allows users of the Internet to share information.

9. **Email Provider**:

a. In my training and experience, I have learned that Apple Inc. provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Subscribers obtain an account by registering with Apple Inc. During the registration process, Apple Inc. asks subscribers to provide basic personal information. Therefore, the computers of Apple Inc. are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Apple Inc. subscribers) and information concerning subscribers and their use of Apple Inc. services, such as account access information, e-mail transaction information, and account application information.

b. In general, an e-mail that is sent to an Apple Inc. subscriber is stored in the subscriber's "mail box" on Apple Inc. servers until the subscriber deletes the e-mail, or until a preservation letter is sent to the email provider. If the subscriber does not delete the message, or if the email provider preserves the content of the account pursuant to a preservation letter, the message can remain on Apple Inc. servers indefinitely.

c. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Apple Inc.'s servers, and then transmitted to its end destination.

d. Apple Inc. subscribers can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Apple Inc.

10. **Internet Service Providers** ("ISPs")

a. ISPs are companies that provide access to the Internet. ISPs can also provide other services for their customers including website hosting, E-mail service, remote storage, and co-location of computers and other communications equipment. ISPs offer different ways to access the Internet including telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or cable television,

dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data (bandwidth). Many ISPs assign each subscriber an account name, such as a user name, an E-mail address, and an E-mail mailbox, and the subscriber typically creates a password for his/her account.

11. **ISP Records**

a. ISP Records are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), E-mails, information concerning content uploaded and/or stored on the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

12. **Internet Protocol Address (IP Address)**:

a. IP address refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, that is, an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

13. **Host Computers:**

a. A host computer is one that is attached to a dedicated network and serves many users. These host computers are sometimes commercial online services, such as America On-line (AOL), which allow subscribers to dial a local number and connect to a network, which is in turn connected to their host systems. These service providers allow electronic mail service between their own subscribers, and those of other networks or individuals on the Internet.

Background of Investigation

14. Kevin Kuciapinski was an active duty Air Force Major employed with the National Reconnaissance Office (NRO) stationed at the Aerospace Data Facility-Colorado (ADF-C), Buckley AFB, CO, as the Technical Director of Experiments and Initiatives Division.

15. Randolph Stimac was a GS-15 National Security Agency (NSA) employee located at the ADF-C, Buckley AFB, CO. Stimac was a technical expert for the NSA dealing with signals intelligence (SIGINT).

16. Mykhael Kuciapinski is the owner and Chief Executive Officer (CEO) of Gordian Polaris Sirius Corporation (GPSC), a company which was attempting to do business with the U.S. government.

17. Stimac and Mykhael Kuciapinski knew each other through Mykhael Kuciapinski's husband, Air Force Major Kevin Kuciapinski. Stimac and Kevin Kuciapinski worked on several U.S. government projects together, beginning around the 2008 timeframe.

18. Clinton West is a CIA employee who was assigned to the NRO in Chantilly, Virginia. From 2008 to February 2015, he served as the Director of the Office of Congressional and Public Affairs for the NRO. Starting around 2009, Clinton West developed a professional and personal relationship with Kevin Kuciapinski. Clinton West met Mykhael Kuciapinski through Kevin Kuciapinski. In December 2013, Mykhael Kuciapinski introduced Clinton West to Stimac.

19. In January of 2015, a review of documents on NRO computer systems, revealed Kevin Kuciapinski's, Stimac's and Mykhael Kuciapinski's involvement in the award of a U.S. government contract that was designed to benefit Mykhael Kuciapinski financially.

Mykhael Kuciapinski's increased income from the contract would also benefit her husband, Kevin Kuciapinski.

20. Kevin Kuciapinski, Stimac and Mykhael Kuciapinski communicated about this contract primarily through email.
21. In September of 2013, through email exchanges obtained via an NRO OIG subpoena served on GPSC, Stimac and Mykhael Kuciapinski established a goal to have Stimac work as the Contracting Officer's Technical Representative (COTR) on a contract awarded to Mykhael Kuciapinski. Stimac stated he wanted to hire Mykhael Kuciapinski and Mykhael Kuciapinski expressed an interest in working on an NRO contract.
22. Clinton West assisted in scheduling meetings with appropriate individuals for Stimac and Kevin Kuciapinski to brief the potential contract effort.
23. In December of 2013, Stimac traveled to Washington, D.C., to solicit funding from U.S. Government agencies for the contract. During these meetings, Stimac failed to secure the funding for the future contract.
24. During the last week of January 2014 and the first week of February 2014, Kevin Kuciapinski traveled with Stimac to Washington, D.C. and conducted briefings with U.S. Government agencies in a second attempt to obtain funding for the contract. Kevin Kuciapinski participated in the official briefings as a subject matter expert. These briefings resulted in Kevin Kuciapinski and Stimac obtaining funding for the contract.
25. In February of 2014, through email exchanges obtained via an NRO OIG subpoena served on Mykhael Kuciapinski, Mykhael Kuciapinski provided Kevin Kuciapinski and Stimac with a possible contracting vehicle utilized by Health and Human Services (HHS) that she

would perform under as a subcontractor. Stimac responded that he could direct funding to that vehicle. Stimac also forwarded Mykhael Kuciapinski a copy of the Statement of Objectives (SOO) for the pending contract award.

26. In July of 2014, Kevin Kuciapinski filed for divorce from Mykhael Kuciapinski. The divorce proceedings were still ongoing in the middle of 2015.

27. During an interview with investigators, Clinton West stated in the first half of 2014, Kevin Kuciapinski brought up the contract project to Clinton West on several occasions. West advised that Kevin Kuciapinski wanted the project to succeed even though he and Mykhael Kuciapinski did not get along. Both Kevin Kuciapinski and Mykhael Kuciapinski set aside their personal differences to work together in order to benefit financially from the contract. West further stated Kevin Kuciapinski contacted him approximately six times regarding the status of Mykhael Kuciapinski's security clearance and requested Clinton West help her with her clearances.

28. In August and September of 2014, through email exchanges obtained via an NRO OIG subpoena served on Mykhael Kuciapinski, Stimac sent Mykhael Kuciapinski the Technical Evaluation criteria for the pending contract award; the Government Cost Estimate; and communications between himself and the HHS Contracting Officer regarding the pending award, to include the names of the competing companies and the status of their proposal submissions. Stimac sent all of this information to Mykhael Kuciapinski prior to the award of the contract.

29. On 18 September 2014, the prime contractor, AMAR Health IT, LLC (AHIT), submitted a proposal to the U.S. government. AHIT is a joint venture that exists for the purposes of

obtaining an HHS Government Wide Acquisition Contract (GWAC). Progressive Technology Federal Systems, Inc. (PTFS) is the member of the joint venture that put together the proposal and intended to execute performance as the prime contractor on the project.

30. The proposal AHIT submitted listed Mykhael Kuciapinski as a key person for the effort. GPSC, Mykhael Kuciapinski's company, was also included in the proposal as a key subcontractor.

31. On 26 September 2014, HHS awarded Delivery Order #HHSN316201200115W_HHSP233201400203W to AHIT under its existing contract vehicle with HHS. The contract required key personnel, which included Mykhael Kuciapinski.

Probable Cause Statement Related to Kevin Kuciapinski's Apple Mac Account

32. Kevin Kuciapinski used his Apple mac account to communicate with Mykhael Kuciapinski and Stimac regarding follow-up actions to the funding briefings on the pending contract award and the related strategic challenges and obstacles.

Kevin.Kuciapinski@mac.com

33. On 18 December 2015, NRO OIG served an NRO OIG subpoena on Mykhael Kuciapinski's attorney. As part of this subpoena, NRO OIG requested Mykhael Kuciapinski produce all communications related to the HHS contract award.

34. Beginning on 9 February 2016, Mykhael Kuciapinski provided documents subsequent to this subpoena. Included in these documents were emails to and from Mykhael Kuciapinski's GPSC email account showing Mykhael Kuciapinski's communications with Kevin Kuciapinski at the Apple mac account. A review of these emails revealed they contained evidence of violations of Title 18 USC, Section 371, in reference to the HHS contract discussed in the background section.

35. As an example, on 20 February 2014, Mykhael Kuciapinski sent an email to Stimac and Kevin Kuciapinski at their personal email accounts. Kevin Kuciapinski's personal email was the Apple mac account. In this email, Mykhael Kuciapinski summarized the actions taken to date to obtain the contract award and listed the many remaining obstacles. Mykahel Kuciapinski told Kevin Kuciapinski and Stimac "The ball is in your court" and stated she had "done all of the groundwork, laid the infrastructure and more." Mykhael Kuciapinski further stated "The rest is up to the government suits to close the deal" and she was "waiting on your actions for the next engagement."

36. Furthermore, on 14 May 2014, Mykhael Kuciapinski sent an email to Stimac and Kevin Kuciapinski at their personal email accounts. Kevin Kuciapinski's personal email was the Apple mac account. In this email, Mykhael Kuciapinski referenced a planned "telecom" Stimac and Kevin Kuciapinski had scheduled for the next day. Mykhael Kuciapinski recommended that Kevin Kuciapinski and Stimac inform the funding stakeholders during the telecom that they should not invest their money on an existing technology program with known problems. Additionally, they should tell the stakeholders to invest the funds on their project because it had a clear path to success. On 15 May 2014, Kevin Kuciapinski

responded to Mykhael Kuciapinski via his Apple mac account to modify her suggested telecom strategy.

37. NRO OIG obtained access to Kevin Kuciapinski's official NRO emails that are stored on government servers. Included in these official emails were correspondence sent to or from Kevin Kuciapinski's Apple mac account.

38. As an example, on 4 February 14, Mykhael Kuciapinski sent an email to Kevin Kuciapinski at his personal and official email accounts. Kevin Kuciapinski's personal email was the Apple mac account. In this email, Mykhael Kuciapinski provided Kevin Kuciapinski with proposed language to respond to a potential stakeholder's concerns about the long term transition plan for the technology supported by the contract.

39. Furthermore, on 10 February 2014, Kevin Kuciapinski sent an email from his Apple mac account to Mykhael Kuciapinski with proposed email language to the financial stakeholders requesting a meeting to give a progress update from the briefings held in Washington, D.C. On 11 February 2014, Mykhael Kuciapinski responded to Kevin Kuciapinski's email at his personal and official email accounts. Kevin Kuciapinski's personal email was the Apple mac account. In this email, Mykhael Kuciapinski provided Kevin Kuciapinski with alternate versions of his suggested email language.

40. Investigators believe further evidence of violations of of Title 18 USC, Section 371 exist in the kevin.kuciapinski@mac.com account because Mykhael Kuciapinski's production in response to the NRO OIG subpoena appears to be incomplete. In particular, the emails provided were missing attachments and did not include the complete email strings. In addition, besides the above referenced subpoena production, the government is not currently

in possession of any emails from the Apple mac account which did not get sent to Kevin Kuciapinski's official NRO email account.

41. In summary, your Affiant believes Kevin Kuciapinski used his kevin.kuciapinski@mac.com account to communicate directly with Mykhael Kuciapinski and Stimac regarding the pending HHS contract award.

Conclusion

42. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, USC, Section 2711 and referenced in Title 18 USC Sections 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated" (Title 18 USC Section 2711(3)(A)(i)).

43. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of Title 18 USC, Section 371 may be located within the e-mail account kevin.kuciapinski@mac.com maintained by KEVIN KUCIAPINSKI. Specifically, during our search we will be looking for evidence of this violation related to HHS Delivery Order #HHSN316201200115W_HHSP233201400203W. I further state that if evidence located within the email account kevin.kuciapinski@mac.com maintained by KEVIN KUCIAPINSKI appears to relate to criminal acts other than those outlined in this affidavit, those items will not be further examined unless and until a search warrant is applied for and issued for evidence of any such separate criminal acts.

44. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

s/ Dana Grant
Dana Grant, Special Agent
Air Force Office of Special Investigations

Reviewed and submitted by Jeremy Sibert, Assistant United States Attorneys.

Submitted, attested to, and acknowledged by reliable electronic means on June 2, 2017.

_____
UNITED STATES MAGISTRATE JUDGE
DISCTRICT OF COLORADO

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The email account known as kevin.kuciapinski@mac.com maintained by KEVIN KUCIAPINSKI which is in the possession of or under the control of the Email and Internet Service Provider Apple Inc. whose office is located at 1 Infinite Loop, Cupertino, CA, 95014-2084.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

Pursuant to Title 18 USC § 2703, Apple Inc., who provides mac email and whose office is located at 1 Infinite Loop, Cupertino, CA, 95014-2084 (the PROVIDER) is hereby ordered as follows:

I. SEARCH PROCEDURE

a. The search warrant will be presented to personnel of the PROVIDER, who will be directed to isolate those accounts and files described in Section II below;

b. In order to minimize any disruption of computer service to innocent third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;

c. The PROVIDER's employees will provide one copy of the exact duplicate in **electronic form** of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant; and

d. Law enforcement personnel will thereafter review all information and records received from the PROVIDER's employees to determine the information to be seized by law enforcement personnel specified in Section III.

II. FILES AND ACCOUNTS TO BE COPIED BY THE PROVIDER'S EMPLOYEES

a. All electronic mail stored and presently contained in, or on behalf of, subscriber kevin.kuciapinski@mac.com maintained by KEVIN KUCIAPINSKI including but not limited to the accounts associated with: kevin.kuciapinski@mac.com maintained by KEVIN KUCIAPINSKI ("SUBJECT ACCOUNTS") including received messages, sent messages, deleted messages, and messages maintained in trash or other folders, including the draft folder and contacts folder;

b. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNTS described above in Section II(a), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and

c. All records indicating the services available to subscribers of the SUBJECT ACCOUNTS described above in Section II(a).

d. All existing printouts from original storage of all of the electronic mail described above in Section II(a), if requested by case agents after review of items in paragraphs a, b & c (above);

e. All transactional information of all activity of the SUBJECT ACCOUNTS described above in Section II(a), including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations, if requested by case agents after review of items in paragraphs a, b & c (above);

III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT PERSONNEL

a. The following electronic mail, attachments and related computer files and account information regarding the SUBJECT ACCOUNTS from July 1, 2013 to the date of the execution of the search warrant -- which constitute evidence and instrumentalities of violations of Title 18 USC, Section 371, related to HHS Delivery Order #HHSN316201200115W_HHSP233201400203W, including, but not limited to, the procurement of the government contract.

b. All electronic mail, attachments and related computer files that identify the account user, individuals or correspondents engaged in violations of Title 18 USC, Section 371.

c. All "address books" or other lists of correspondents.

d. All saved "chat" transcripts that relate to violations of Title 18 USC, Section 371.

e. All of the records and information described above in Sections II(c), (d), and (e).

IV. PROVIDER PROCEDURES

a. The PROVIDER shall deliver the information set forth above within **10 days** of the service of this warrant and the PROVIDER shall send the information via facsimile or United States mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium, to:

National Reconnaissance Office-Office of the Inspector General (NRO/OIG)
Aerospace Data Facility – Colorado
18201 E. Devils Thumb Ave., Stop 77
Aurora, CO 80011
Attn: Inv. Donna Ennis

b. Pursuant to 18 USC § 2703(g) the presence of an agent is not required for service or execution of this warrant.