

TOP SECRET// [] //NF

(U) IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

(U) IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
[] THAT IS
STORED AT PREMISES CONTROLLED BY
APPLE INC.

(U) Case No. 10-774-M-01

(U) Filed Under Seal

(U) AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

(U) I, Joseph Capitano, being first duly sworn, hereby depose and state as follows:

(U) INTRODUCTION AND AGENT BACKGROUND

1. (U) I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Apple Inc., an e-mail provider headquartered at Cupertino, 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 Apple Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. (U) I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been employed with the FBI for approximately 6 years. I am currently assigned to a squad at the Washington Field Office that handles national security cases. During my tenure with the FBI, I have handled federal criminal investigations and the execution of numerous arrest and

TOP SECRET// [] //NF

search warrants. I have also received specialized training in national security matters and in the use of the Internet, email accounts, and other technologies to commit federal criminal violations.

3. (U) The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and government agencies, including the FBI, Central Intelligence Agency ("CIA"), and Department of Defense ("DoD"). 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. (U) Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 793 (disclosure of national defense information) have been committed and that there exists evidence of violations of 18 U.S.C. § 793 in the email account described in Attachment A. Accordingly, there is probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

(U) PROBABLE CAUSE

(U) Background of Investigation

5. (U) This investigation concerns allegations relating to the unauthorized disclosure of national defense information relating to or arising from the capture, detention, interrogation of certain detainees.

6. (TS//SI)¹ John Kiriakou is a subject of the investigation. Kiriakou was a CIA intelligence officer from 1990 to 2004. Kiriakou worked as [redacted] and has stated publicly that he was involved in Abu Zubaydah's capture and initial detention. Thereafter, Kiriakou worked at CIA headquarters, [redacted]. In that capacity, Kiriakou had access to classified reporting relating to the Counterterrorism Center's High Value Target ("HVT") program, the Renditions, Detention, and Interrogation ("RDI") program, and [redacted] among other matters.

7. (U) Upon leaving the employment of the CIA, Kiriakou gave a series of high-profile media interviews based purportedly on his experience as a former CIA officer and addressing such matters as terrorist detention and interrogation. In 2010, Kiriakou published his memoirs, *The Reluctant Spy: My Secret Life in the CIA's War on Terror*, which purports to describe his work at the CIA. Prior to the book's publication, Kiriakou submitted multiple drafts of the book, beginning on or about October 11, 2007, to the CIA Publications Review Board ("PRB"), which determined that several of the drafts contained classified information and so advised Kiriakou.

8. (U) Our investigation has revealed the following, among other things:

¹ Paragraph classification markings denoted in this affidavit are included solely to ensure proper handling of the affidavit and information contained therein and are not provided for the purpose of establishing probable cause or intended to be relied upon by the Court in making its probable cause determination.

a. (TS//SI) On or about June 22, 2008, [redacted] published in the New York Times an article, "Inside a 9/11 Mastermind's Interrogation," describing the capture of Abu Zubaydah, the interrogation of KSM, and identifying and describing the role of a particular CIA interrogator [redacted], among other things. As described in paragraphs 9-33, *infra*, according to preliminary CIA analysis, certain information in [redacted] New York Times article appears to represent first-time disclosures of classified CIA information, including sensitive details regarding intelligence operations, sources and methods. The article also includes attributed information that bears a strong resemblance in style and substance to language that Kiriakou submitted to the PRB prior to the publication of the New York Times article, and that he later published in his book. For example, in manuscripts submitted to the PRB in October 2007 and November 2007, respectively, Kiriakou described a [redacted]

[redacted] The chronology of the PRB submissions, [redacted] New York Times article, and Kiriakou's book publication supports an inference that Kiriakou was strategically disclosing information to the media to put that information in the public domain and thereby make PRB approval of the use of such information in his book more likely.

b. (TS//SI) Subsequent to the publication of the New York Times article, on or about January [redacted] 2009, attorneys for [redacted] now detained

at Guantanamo Bay, Cuba, filed a Motion [redacted] (the "Motion") with the Office of Military Commissions. The Motion sought, *inter alia*, information relating to the detention and interrogation of [redacted]. An Attachment to the Motion identifies numerous persons by name and alleges that those persons have direct knowledge and could testify about the detention and interrogation of [redacted] while in the HVD program. Based on preliminary CIA analysis, the Attachment includes possible first-time unauthorized disclosures of classified information regarding certain individuals, including current and former Agency staff officers and contractors who were involved in the Counterterrorism Center's HVT program and later the RDI program. The analysis further suggests that the Motion's authors may have obtained classified information from a source or sources with access to CIA's high value target, renditions, and detention programs, like Kiriakou. To ensure their security and as part of the investigation, CIA and FBI personnel have contacted and interviewed many of the persons named in the Motion to warn them of the possible compromise of their identity and assist in identifying possible sources. As described more fully below (*see* paragraphs 40-57, *infra*), at least three such persons identified Kiriakou as a possible source due in part to his familiarity with these individuals as former colleagues at the CIA.

c. (U) When contacted by CIA and FBI personnel, the three former colleagues also described being contacted by reporters in 2008, 2009, or both, as described further in paragraphs 39-57, *infra*. These reporters included [redacted]. [redacted] By order pursuant to 18 U.S.C. 2703(d), the government obtained email header information from Apple Inc. for Kiriakou's email account described in Attachment A. Based on my review of the email header

information, Kiriakou was in contact with [redacted] (20 times) [redacted] (123 times), and [redacted] (30 times). Further, based on the email header information and the information provided to us by the former colleagues regarding when the reporters contacted them, I have learned that Kiriakou was in email contact with [redacted] prior to their contact with each of Kiriakou's three former colleagues. Further, Kiriakou appears to have lied to one such employee about his contact with [redacted] including by sending an email to the employee asserting that his "only contact with the author was three days before the article was published," a claim contradicted by the email header information, described in paragraph 45, *infra*.

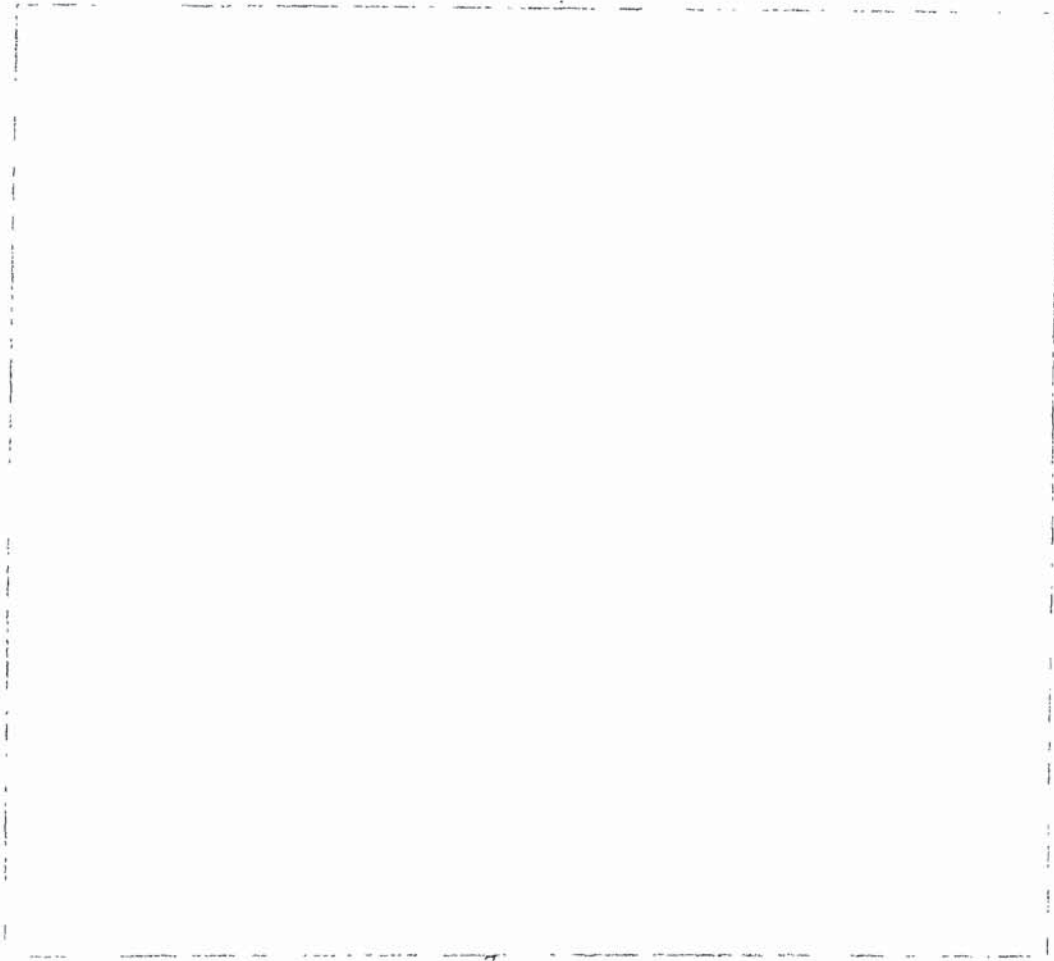
Background Regarding June 22, 2008 Article by [redacted]

9. (U) On or about June 22, 2008, [redacted] published in the *New York Times* an article, "Inside a 9/11 Mastermind's Interrogation," describing the capture of Abu Zubaydah, the interrogation [redacted]; the role of a particular interrogator, and other matters. [redacted]

10. (TS// [redacted] /NF) According to a CIA report dated [redacted] specific information relating to or arising from the interrogation of detainees is classified. While there have been numerous articles previously covering the topic of detainee interrogation, certain information in the [redacted] article appears to represent first-time disclosures of classified CIA information. The information disclosed in the article constitutes an unauthorized disclosure of classified information at the TOP SECRET codeword level. CIA subject matter experts have

assessed that the disclosure of this information could reasonably be expected to cause exceptionally grave damage to the national security. The classified information had not been officially released and has not been cleared for publication.

11. (TS/ [] /NF) Among the classified information identified by the CIA in its [] report was the following (as stated in the report):



~~TOP SECRET~~

~~/NF~~

~~TOP SECRET~~

~~/NF~~

(U) Similarities in Style and Substance to Unattributed Information

14. (U) Several instances of unattributed information revealed in the [REDACTED] article bear a strong resemblance in style and substance to language that Kiriakou submitted to the PRB, used in the published version of his book, and/or used in other attributed media interviews.³

³ (S/SECRET) In its October 24, 2007 response to Kiriakou's October 11, 2007 manuscript, the PRB informed Kiriakou that the manuscript was considered classified, could not be published, and that, should he wish to object to the PRB decision, he could submit "citations or copies of similar references that show this information to have been previously released and already in the public domain." It is possible that Kiriakou, by disclosing classified information to [REDACTED] sought to place such information in the public domain and thereby make PRB approval of his manuscript more likely. Indeed, based on an interview with a former colleague of Kiriakou, Kiriakou stated to the former colleague, in sum and substance, that, although the clearance process with PRB for his book was difficult, he was able to include sensitive information based on what had been reported in the press.

~~TOP SECRET~~

~~TOP SECRET~~

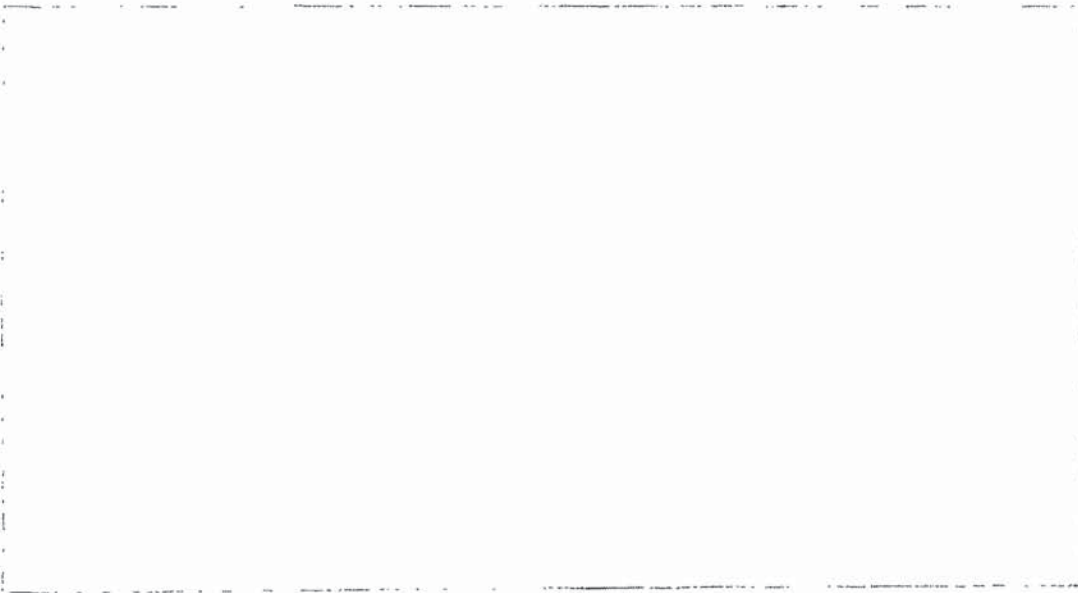
~~TOP SECRET~~

~~TOP SECRET~~

~~TOP SECRET//NF~~



(TS//SI) "Magic Box"



⁴(U) It is also noteworthy Kiriakou was an attributed source for a portion of the [REDACTED] article:



~~TOP SECRET//NF~~

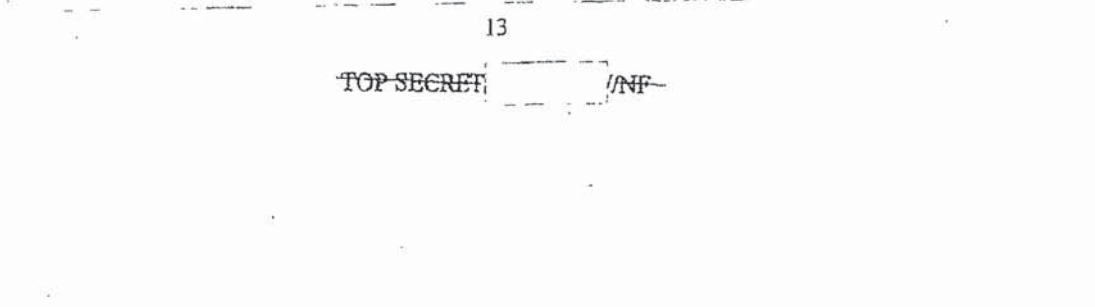
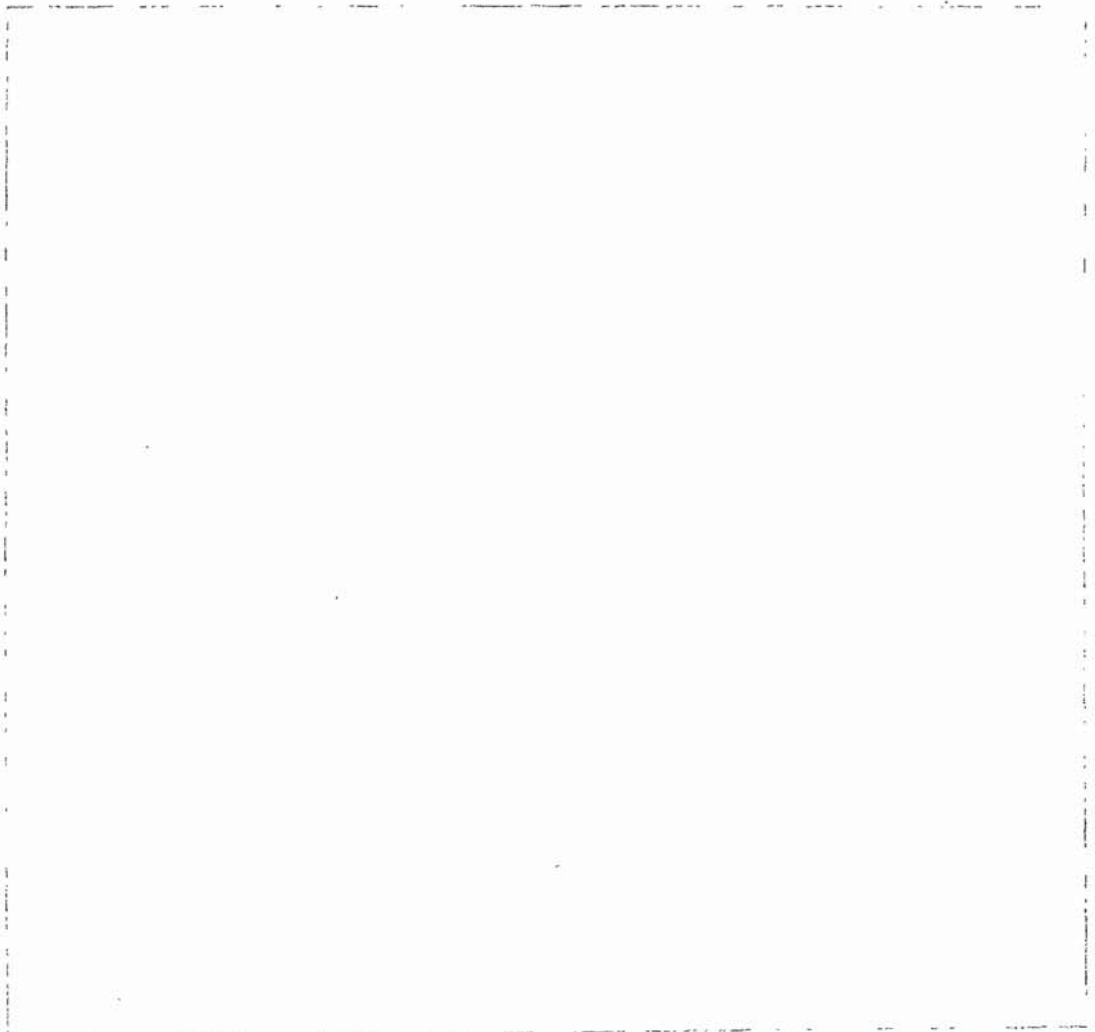
As noted in paragraph 11, *supra*, the foregoing passage was considered classified by the CIA.

21. (TS//SI) Kiriakou wrote to the PRB on or about July 28, 2008 and stated that he had read about the term "magic box" in a New York Times article and sought to publish it in his book, stating: "The information in the [New York Times] article was clearly fabricated, as we used no such device. I am unaware of any device called a 'magic box,' but I thought it intriguing, so I added it to this chapter. As it is fictionalized, I believe it is unclassified." Specifically, Kiriakou proposed including the following passage:



22. (TS//SI) The PRB denied Kiriakou's request on or about October 17, 2008

because the use of the magic box was considered classified



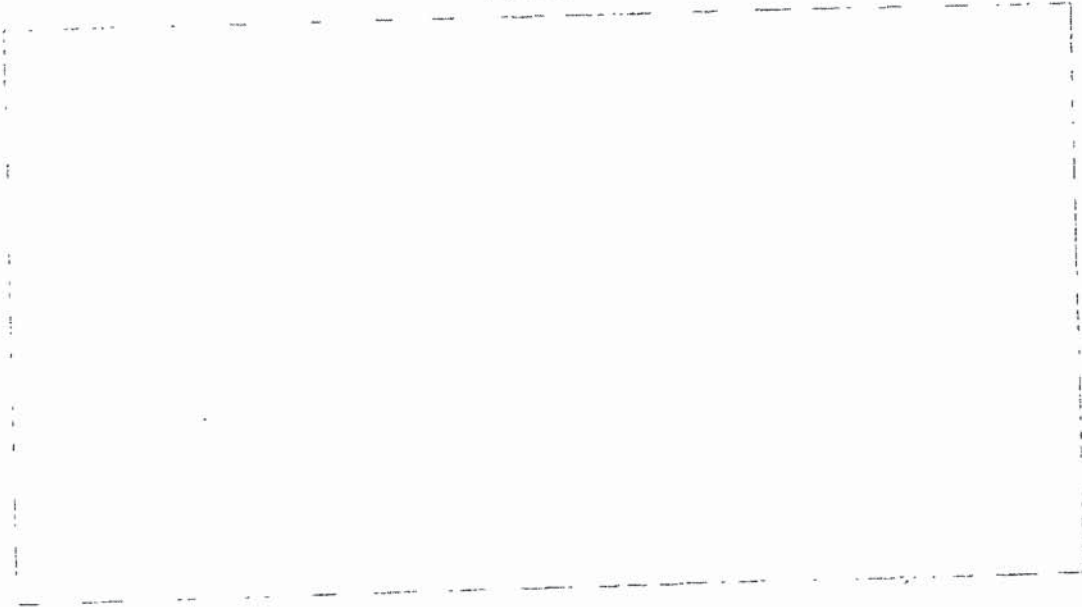
~~TOP SECRET~~ ~~INF~~

~~TOP SECRET~~ ~~INF~~

~~TOP SECRET//NF~~

~~TOP SECRET//NF~~

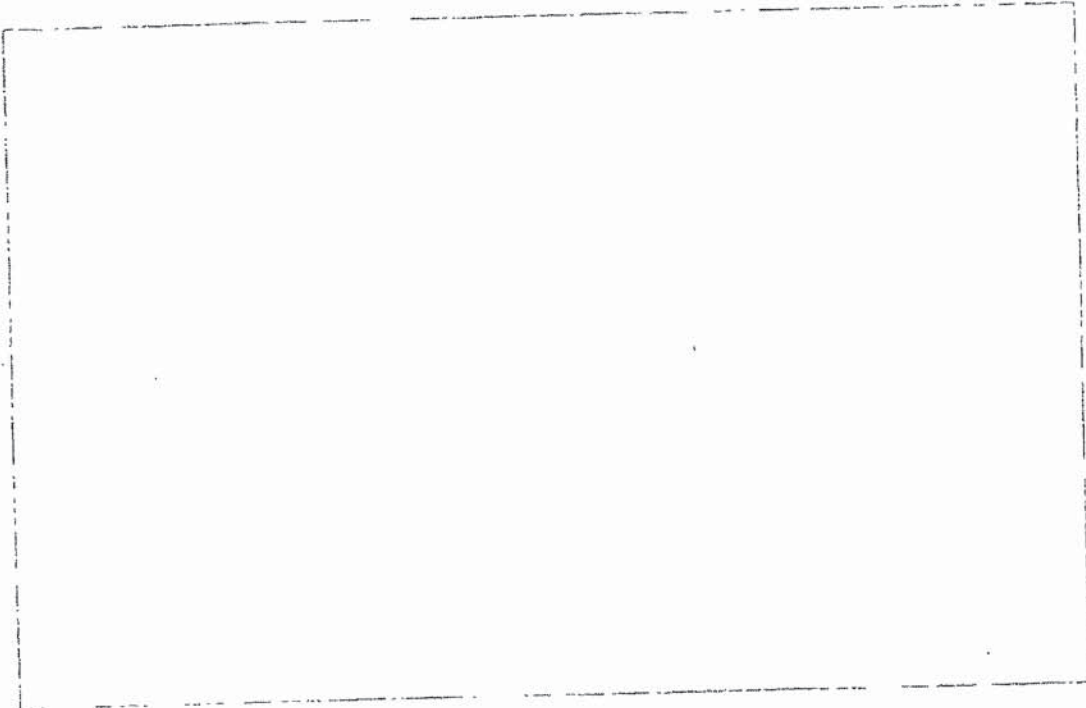
(U) *Other*



9) The Motion

34. (U) On or about January [redacted], 2009, attorneys for [redacted] [redacted] now detained at Guantanamo Bay, Cuba, filed a Motion [redacted] (the "Motion") with the Office of Military Commissions. The Motion sought, *inter alia*, information relating to the detention and interrogation of: [redacted] The Motion asserts that [redacted] was in a CIA detention program known as the High Value Detainee ("HVD") program during this time period. An Attachment to the Motion identifies numerous persons by name, alleges that those persons have direct knowledge and could testify about the [redacted]

detention and interrogation of [] while in the HVD program, and makes factual claims regarding those persons' intelligence activities on behalf of the United States government.



36. (TS//SI) To ensure their security and as part of the investigation, CIA and FBI personnel have contacted and interviewed many of the persons named in the Motion to warn them of the possible compromise of their identity and assist in identifying possible sources. As described more fully below, several such persons were also contacted directly by reporters and identified John Kiriakou as a possible source due in part to his familiarity with these individuals as former colleagues at the CIA.

(U) Email Account

37. (U) According to CIA records, Kiriakou's email addresses have included [redacted] (the "Target Account"). On or about July 29, 2010, the Government faxed a letter to Apple Inc., the service provider for the Target Account, requesting that its contents be preserved pursuant to 18 U.S.C. § 2703(f), for 90 days. On or about August 13, 2010, the Government sought and obtained an order from the U.S. District Court for the District of Columbia, pursuant to 18 U.S.C. § 2703(d), to obtain the subscriber information for the Target Account and non-content information associated with email communications stored in the Target Account, including email header information. On the same day, the Government served the order on Apple. On or about August 19, 2010, Apple responded to the Government's request by providing subscriber information and non-content email header information (i.e., sender, recipient, date, and time of email communications without email subject lines). On or about October 26, 2010, the Government faxed a letter to Apple Inc., the service provider for the Target Account, requesting that its contents continued to be preserved pursuant to 18 U.S.C. § 2703(f), for another 90 days.

38. (U) Based on the subscriber information provided by Apple, the Target Account is currently active and registered to an individual named "John Kiriakou" at [redacted] Arlington, VA [redacted] is Kiriakou's home address. The Target Account has been active since June 5, 2005.

39. (TS//SCF) As described further in paragraphs 40-57, *infra*, my review of the email header information provided by Apple (the "Email Header Information") reflects, collectively,

approximately 175 email contacts between Kiriakou and three journalists: [REDACTED] [REDACTED] [REDACTED] (20 contacts from in or about April 2008 through in or about January 2010), [REDACTED] (123 contacts from in or about November 2008 through in or about August 2010), and [REDACTED] (30 contacts from in or about December 2007 through in or about March 2010). Three former CIA colleagues of Kiriakou were contacted by one or more of these three journalists in 2008, 2009, or both (i.e., "Employee-2," "Employee-3," respectively).

(U)



45. (U) Prior to the publication of [REDACTED] *New York Times* article, Kiriakou and [REDACTED] were in contact, thereby giving Kiriakou the opportunity to provide [REDACTED] with information regarding [REDACTED]. For example, based on the Email Header Information, there were at least 12 email contacts between Kiriakou and an individual listed in the email headers as [REDACTED] (with an email address of [REDACTED]) during the months and weeks leading up to the publication of the *New York Times* article. These email contacts took place on or about the following dates: April 15 (5 contacts), April 21 (3 contacts), May 28 (2 contacts),

May 29 (1 contact), and June 3, 2008 (1 contact). Four of these contacts were incoming emails to Kiriakou, and the remaining eight contacts were outgoing emails.⁶

46. (TS//SI) Prior to the publication of the New York Times article, on or about May 8, 2008, an individual identifying himself as [REDACTED] called the residence of [REDACTED] he spouse of [REDACTED] answered the phone [REDACTED]

47. (TS//SI) After placing the phone call, but prior to the publication of the New York Times story [REDACTED] emailed [REDACTED] at his personal email address. [REDACTED] had provided his personal email address to Kiriakou, but not to [REDACTED] or any other journalist. In his email to [REDACTED] [REDACTED] asked to speak with [REDACTED]

48. (U) On June 30, 2008, approximately one week after the publication of the New York Times article, Kiriakou sent an email to [REDACTED] personal email address. The email, [REDACTED]

⁶ The Email Header Information also reflect at least 8 contacts between Kiriakou and [REDACTED] after the publication of the article in or about November 2008, January 2009, and January 2010.

which [redacted] stated, among other things: "I had a conversation over the weekend with the ombudsman at the New York Times regarding the article about you in last week's paper. . . . I told the ombudsman that I thought the use of your name in the article was despicable and unnecessary, and that I thought it could put you in personal danger. . . . I also wanted to let you know . . . that I did not cooperate with the article. *My only contact with the author was three days before the article was published.* He called me and asked if we could talk. I declined. He then asked if I thought he should mention you by name. I said absolutely not. He countered with the fact that you have not been under cover. I said that made no difference, and that while it might not be illegal to name you, it would certainly be immoral." (emphasis added) The Email Header Information confirms that there was an email contact between Kiriakou and [redacted] personal email address on June 30, 2008. As noted in paragraph 45, *supra*, contrary to Kiriakou's assertions to [redacted] Kiriakou was in contact with [redacted] on numerous occasions prior to the [redacted] article's publication.

49. (TS//SI) After the New York Times article was published, [redacted] recalls receiving an email not only from Kiriakou, but also from [redacted] and from [redacted] of [redacted]. Based on [redacted] recollection, both [redacted] contacted [redacted]'s personal email address. As with [redacted] had not provided his email address to [redacted]

50. (U) Based on the Email Header Information, Kiriakou had been in contact not only with [redacted] prior to the publication of the New York Times article, but also with an individual listed in the email headers as [redacted] (with an email address of

[]). From in or about December 2007 through in or about April 2008, there were at least 6 email contacts between Kiriakou and [] (1 contact on December 10, 2007; 2 contacts on March 28, 2008; 1 contact on April 16, 2008; and 2 contacts on April 25, 2008). Further, telephone records reflect that a number associated with [] direct telephone line at [] was in contact with a phone number associated with John Kiriakou on or about May 15, 2008. Specifically [] phone called Kiriakou's phone, and the two spoke for approximately 5 minutes (303 seconds).

52. (U) Prior to [] March 18, 2009 email, Kiriakou and [] were in contact by email at least 3 times (2 contacts in February 10, 2009, and February 17, 2009, respectively; and 1 contact on March 12, 2009). Based on telephone records, they were also in contact by phone at least twice: one call, on February 18, 2009, lasted approximately 22 minutes

(1,315 seconds), and another call, on March 13, 2009, lasted approximately 15 minutes (890 seconds).

(U) Employee-2

53. ~~(S/SECRET)~~ Employee-2,

was contacted by [redacted] journalists in 2009, as

described further below.

~~TOP SECRET~~/

~~INF~~



⁸ It is noteworthy that Kiriakou also served as an [REDACTED] consultant from approximately August 2008 through approximately December 2008, based on a review of Kiriakou statements in the media.

~~TOP SECRET~~/

~~INF~~

~~TOP SECRET~~

~~NF~~



(U) Employee-3



(U) Other Former Colleagues of Kiriakou Listed in the Motion

~~TOP SECRET~~

~~NF~~

58. ~~(TS/SC)~~ Other than [] Employee-2, and Employee-3, who were both named in the Motion and contacted by journalists, there were other former CIA colleagues of Kiriakou, who, although they were not contacted by journalists, were named in the Motion and had contact with Kiriakou.



59. (U) In my training and experience, I understand that, in addition to contacting each other by email and phone, individuals participating in a crime often meet separately in person to share sensitive information. Further, the details regarding these meetings may not be reflected in the content of emails, but rather in calendar entries.

(U) Email Records at Apple Inc.

60. (U) 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. Apple Inc. allows subscribers to obtain e-mail accounts at the domain name mac.com, like the e-

mail account listed in Attachment A. 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 unretrieved 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.

61. (U) 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. If the subscriber does not delete the message, the message can remain on Apple Inc. servers indefinitely.

62. (U) 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. Apple Inc. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Apple Inc. server, the e-mail can remain on the system indefinitely.

63. (U) A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Apple Inc. but may not include all of these categories of data.

64. (U) An Apple Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Apple Inc.

65. (U) Subscribers to Apple Inc. might not store on their home computers copies of the e-mails stored in their Apple Inc. account. This is particularly true when they access their Apple Inc. account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

66. (U) In general, e-mail providers like Apple Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

67. (U) E-mail 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 Apple Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail 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 e-mail account.

68. (U) In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing

inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

69. (U) In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

70. (U) As a federal agent, I am train and experienced in identifying communications relevant to the crimes under investigation. The personnel of Apple are not. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. It would be inappropriate and impractical, however, for federal agents to search the vast computer network of Apple for the relevant account and then to analyze the contents of that account on the premises of Apple. The impact on Apple's business could be severe. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities to Apple, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Apple to make a digital copy of the entire contents of the information subject to seizure specified in Section I of Attachment B. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section II of Attachment B.

(U) INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

71. (U) I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular: 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

(U) CONCLUSION

72. (U) Based on the forgoing, I request that the Court issue the proposed search warrant.

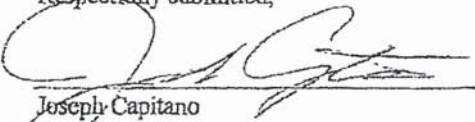
73. (U) This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

74. (U) Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

(U) REQUEST FOR SEALING

75. (U) I further request that the Court order that all papers in support of this application, including the 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 seriously jeopardize that investigation.

Respectfully submitted,



Joseph Capitano
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
On November 19, ~~2008~~ 2014 *let*



UNITED STATES DISTRICT JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with _____ that is
stored at premises owned, maintained, controlled, or operated by Apple Inc., a company
headquartered at Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple Inc., Apple Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

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 types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, and calendar data;

d. All records pertaining to communications between Apple Inc. and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 793 (disclosure of national defense information) involving John Kiriakou in the period of December 2007 through August 2010, including, for the account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications and records relating to the capture, detention, and interrogation of detainees, including but not limited to _____ and Abu Zubaydah.
- b. Communications and records relating to CIA personnel, operations, sources, and methods.
- c. Communications and records relating to communications with news organizations and journalists, including but not limited to _____
- d. Communications and records relating to who created, used, or communicated with the account and identifier, including records about their identities and whereabouts.

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 Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. 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 Apple Inc., 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 Apple Inc.; and
- c. such records were made by Apple Inc. 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