

TOP SECRET// [REDACTED]

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

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

(U) Case No. _____

(U) Filed Under Seal

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

(U) I, John Kralik, 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 Microsoft Corporation ("Microsoft"), an e-mail provider headquartered at One Microsoft Way, Redmond, Washington. 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 Microsoft 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 10 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// [REDACTED]

~~TOP SECRET~~ [REDACTED]

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.¹

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

¹ (U) As explained more fully herein, as part of the instant investigation, this Court authorized the search of an email account associated with John Kiriakou, a subject of the investigation, on or about November 19, 2011. That search revealed, inter alia, a second email account associated with Kiriakou, which the government now seeks authority to search.

~~TOP SECRET~~ [REDACTED]

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, and relating to CIA sources, methods, operations, and personnel.

6. ~~(TS)~~ [redacted] ~~(NF)~~² John Kiriakou is a subject of the investigation. Kiriakou was a CIA intelligence officer from 1990 to 2004. Kiriakou worked in [redacted]

[redacted] and has stated publicly that he was involved in Abu Zubaydah's capture and initial detention.

Thereafter, Kiriakou worked at CIA headquarters, [redacted]

[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]

[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

² (U) 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. Where representations are made with respect to classification for purposes of establishing probable cause, they are made explicitly and should be considered preliminary determinations subject to further review.

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:

a. (TS// [redacted]//NF) 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 9-32, *infra*, according to preliminary CIA analysis, certain information in [redacted] New York [redacted] article appears to represent first-time disclosures of classified CIA information, including sensitive details regarding intelligence operations, sources and methods. The article also includes unattributed 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, [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. (U) 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]. A classified 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 information that may indicate 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.³ To ensure their security and as part of the investigation, CIA and FBI

personnel have contacted and interviewed many of the persons identified 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 an email account associated with Kiriakou (the "Mac Account," as described below). 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 44, *infra*, and subsequent search warrant.

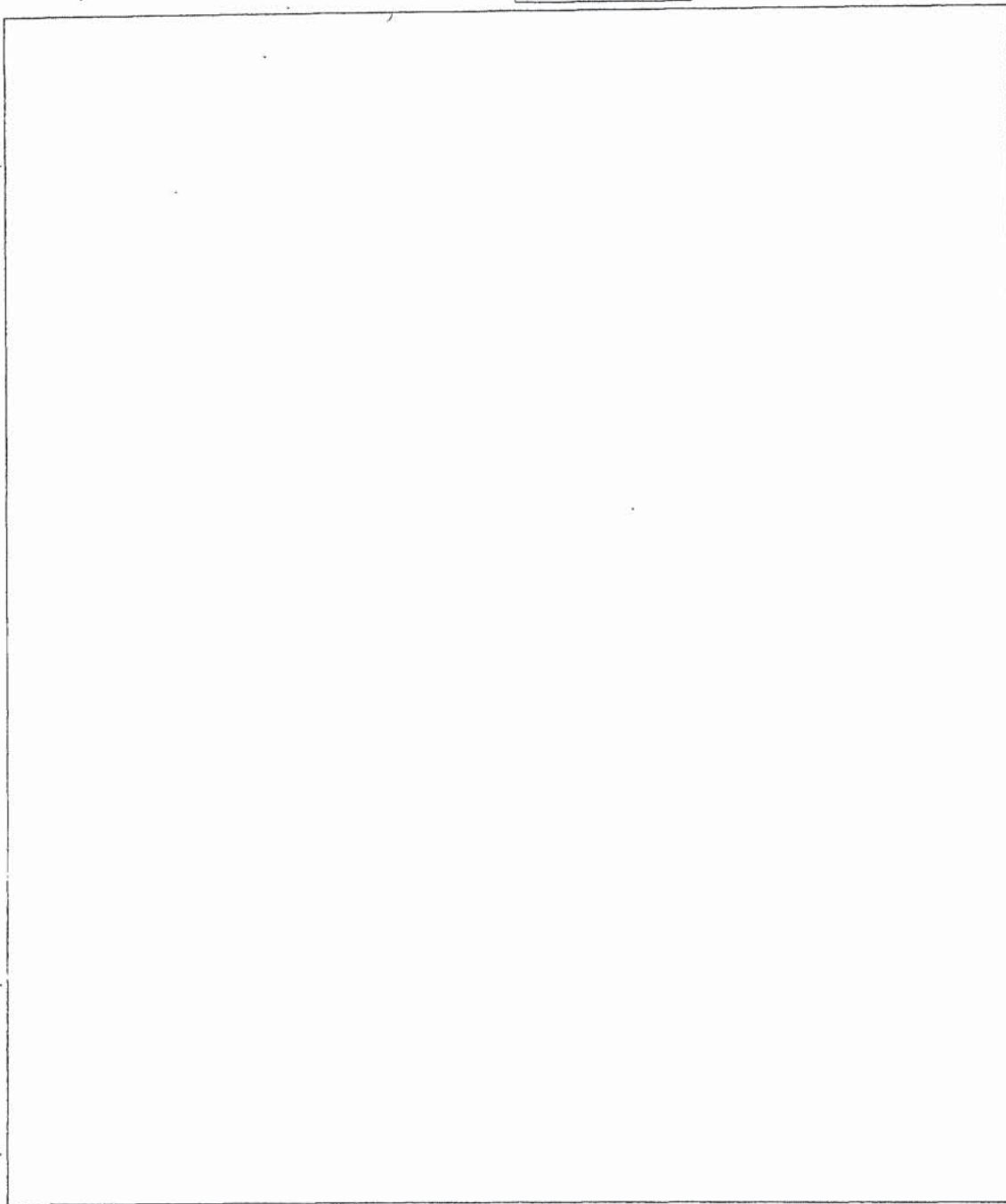
(U) Background Regarding June 22, 2008 Article by [REDACTED]

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] described his sources as "two dozen current and former American and foreign intelligence officers" and wrote that "[m]ost would speak of the highly classified program only on the condition of anonymity."

10. (S//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.

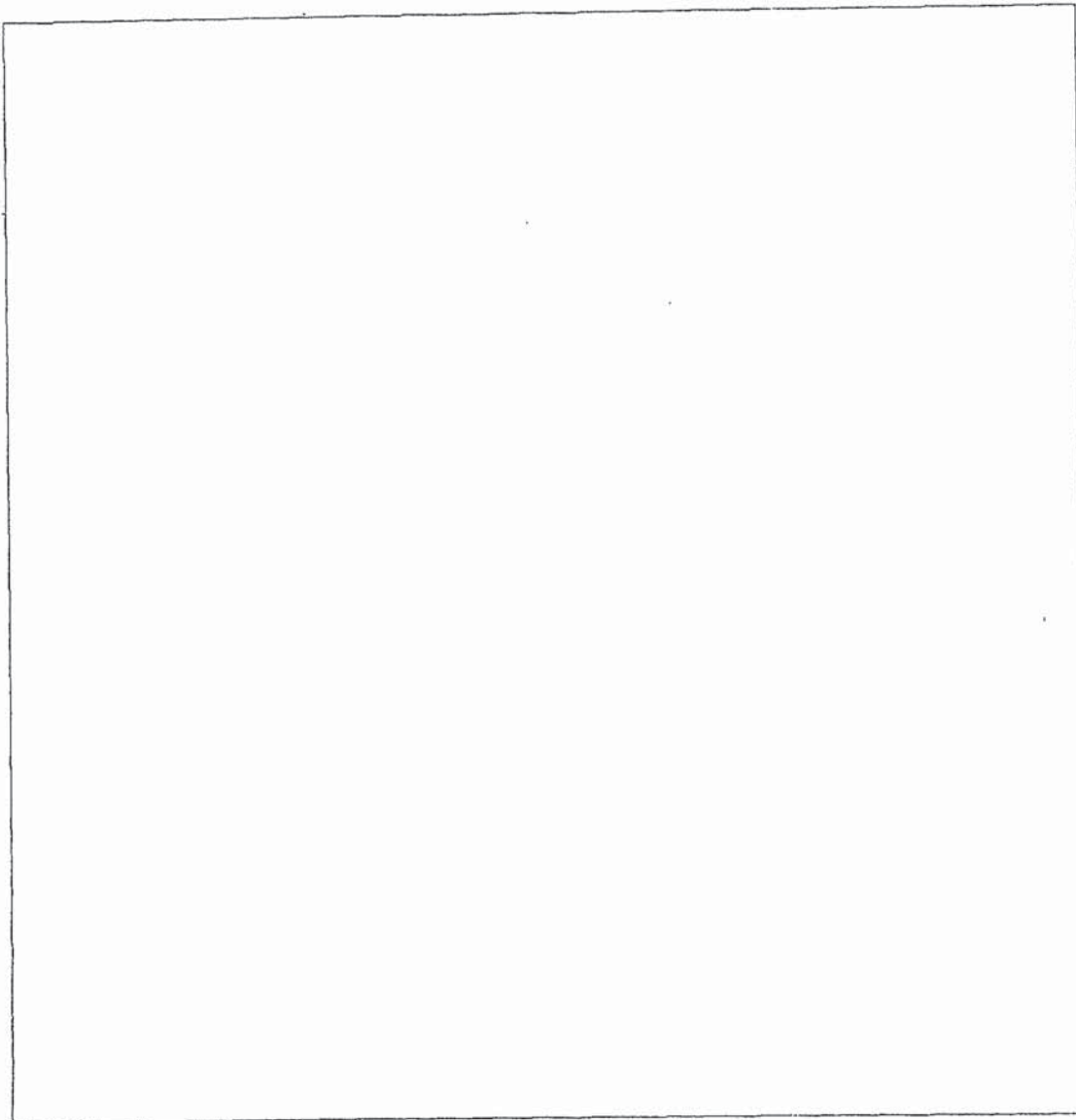
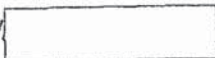
11. (S//NF) Among the classified information in [REDACTED] article identified by the CIA in its [REDACTED] report was the following (as stated in the report):

~~TOP SECRET~~ [redacted]

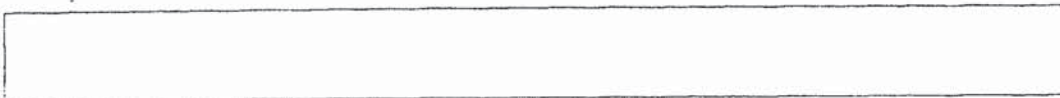


~~TOP SECRET~~ [redacted]

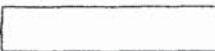
TOP SECRET/



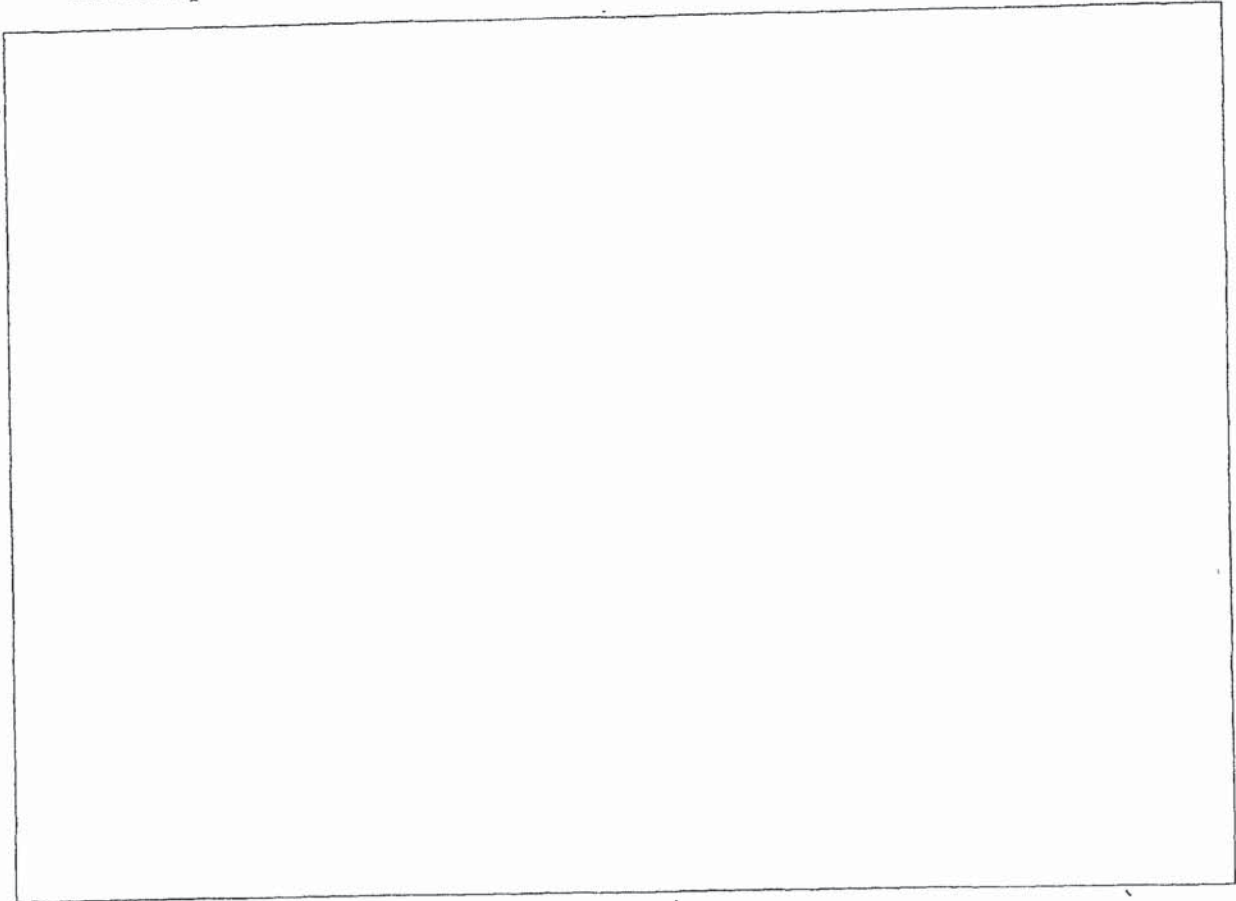
(U) Similarities in Style and Substance to Unattributed Information



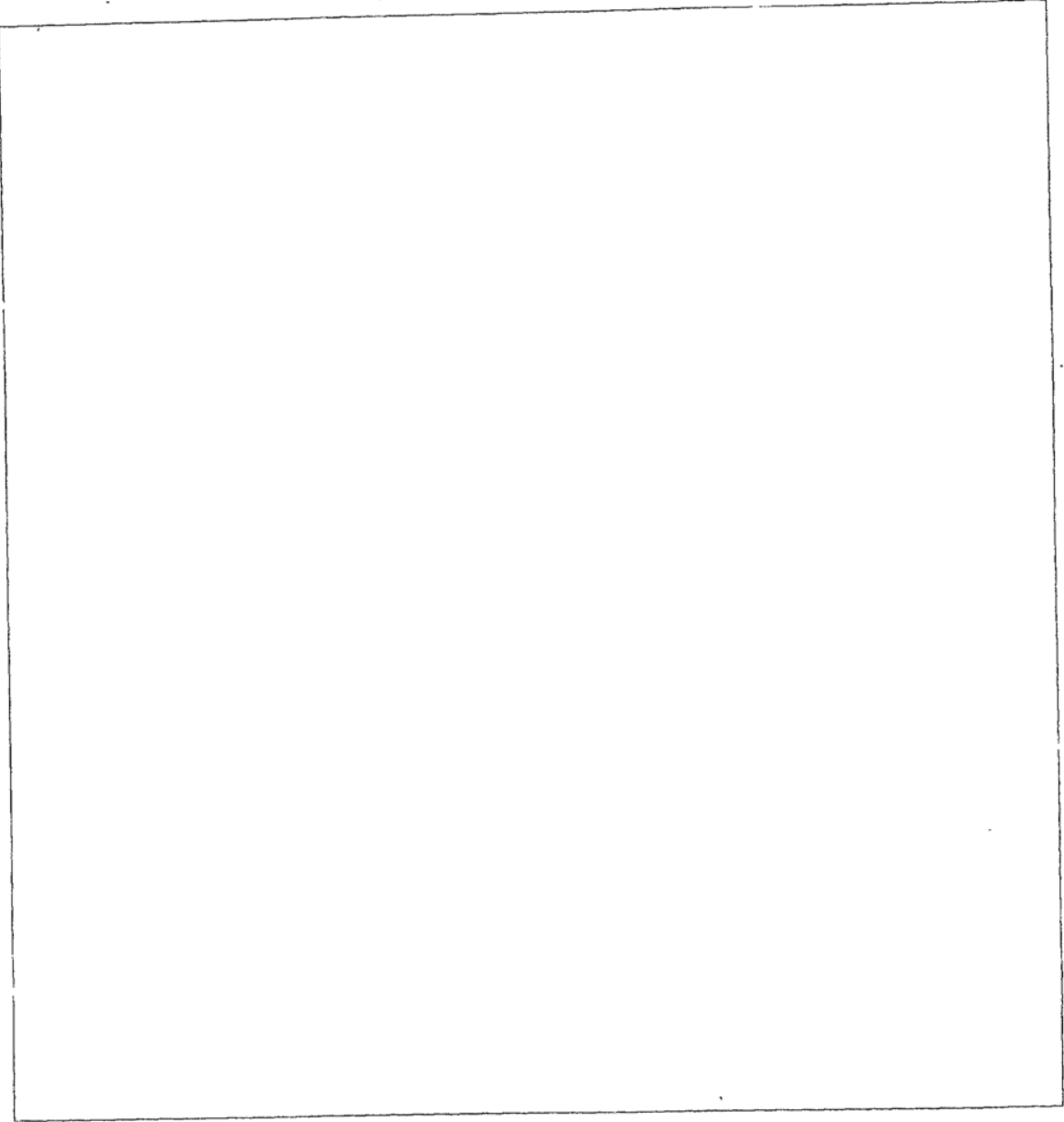
TOP SECRET/



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.⁵



⁵ (U) 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."²² 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.



⁶ (U) It is also noteworthy Kiriakou was an attributed source for a portion of the [redacted] article:

John C. Kiriakou, a former C.I.A. counterterrorism officer who was the first to question Abu Zubaydah, expressed such conflicted views when he spoke publicly to [redacted] and other news organizations late last year. In a December interview with [redacted] before being cautioned by the C.I.A. not to discuss

~~TOP SECRET~~ [redacted]

[redacted]

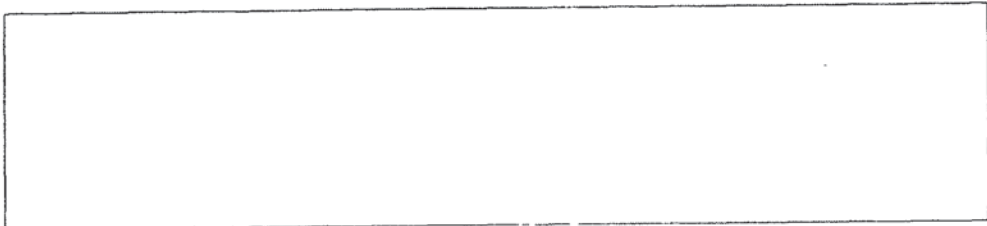
(TS//NF) "Magic Box"

[redacted]

classified matters, Mr. Kiriakou, who was not present for the waterboarding but read the resulting intelligence reports, said he had been told that Abu Zubaydah became compliant after 35 seconds of the water treatment.

"It was like flipping a switch," Mr. Kiriakou said of the shift from resistance to cooperation. He said he thought such "desperate measures" were justified in the "desperate time" in 2002 when another attack seemed imminent. But on reflection, he said, he had concluded that waterboarding was torture and should not be permitted. "We Americans are better than that," he said.

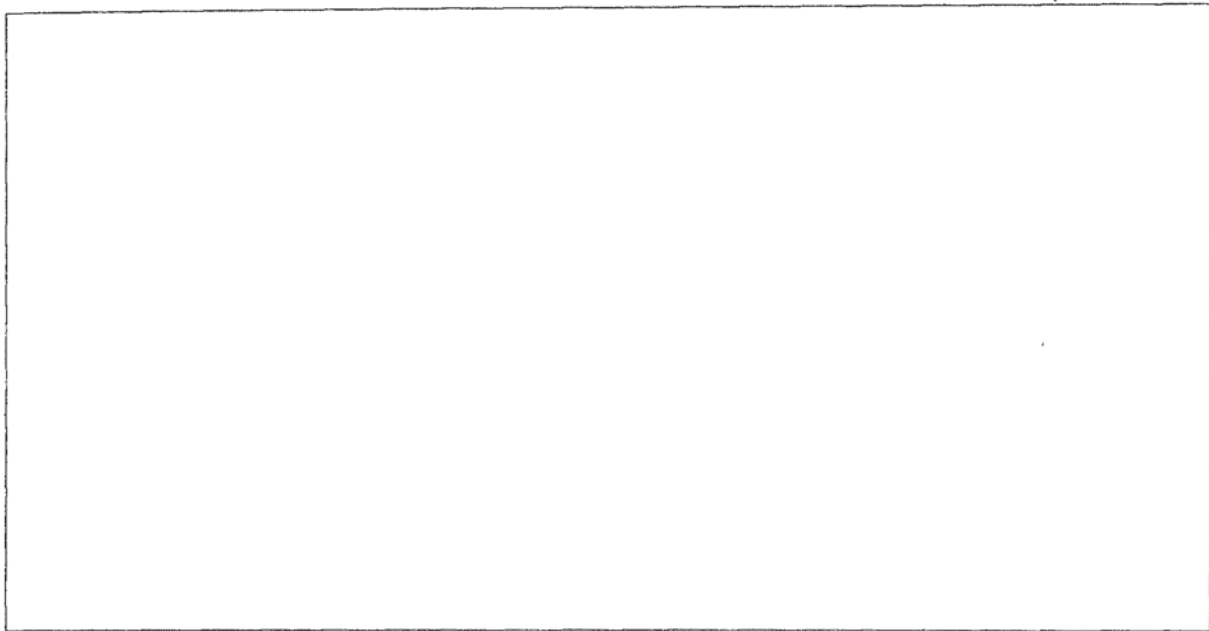
~~TOP SECRET~~ [redacted]



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

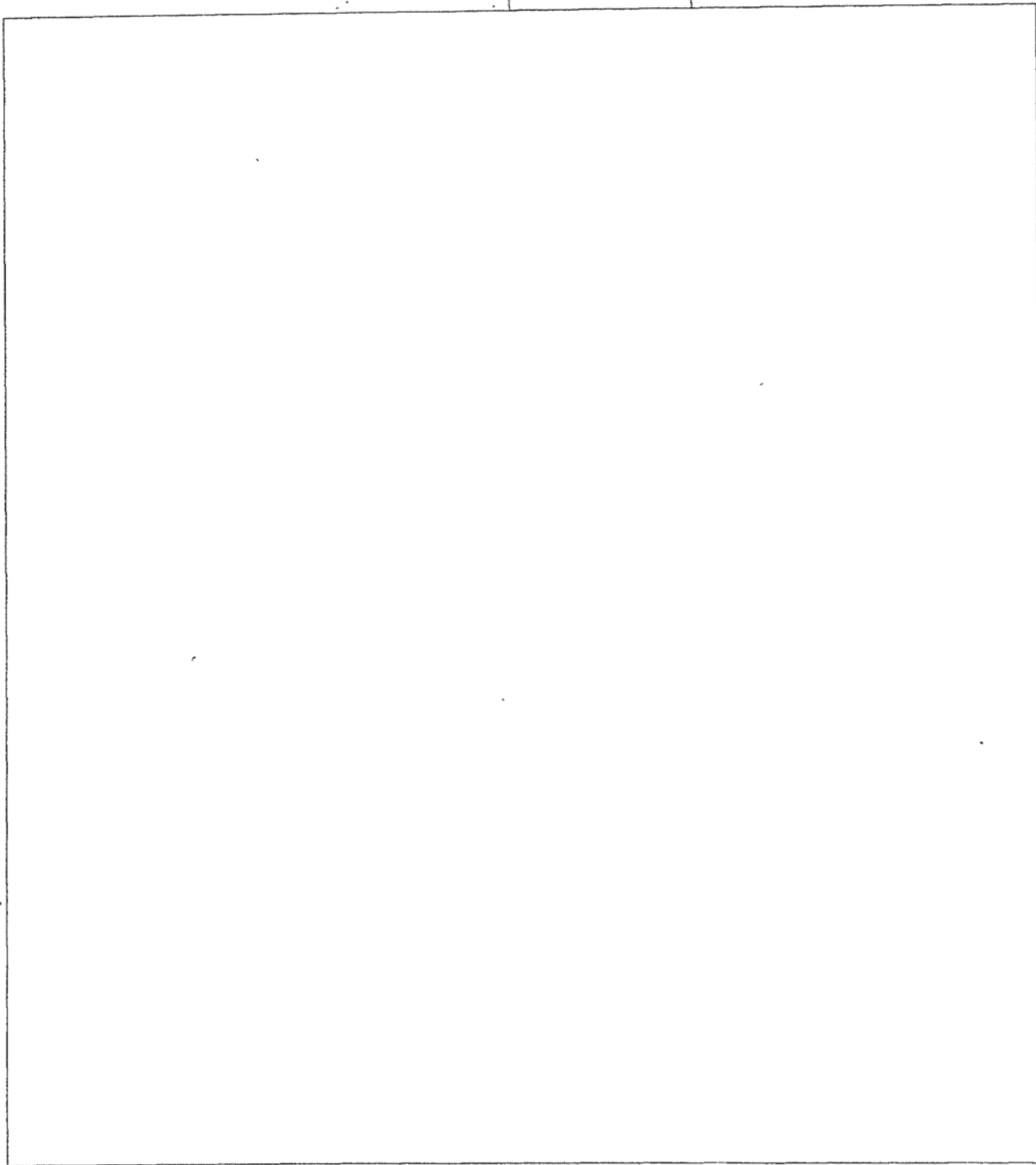
21. (TS//NF) Kiriakou wrote to the PRB on or about July 28, 2008 and stated that he had read about the term "magic box" in a New York Times article and sought to publish it in his book, stating: "The information in the [New York Times] article was clearly fabricated, as we used no such device. I am unaware 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:



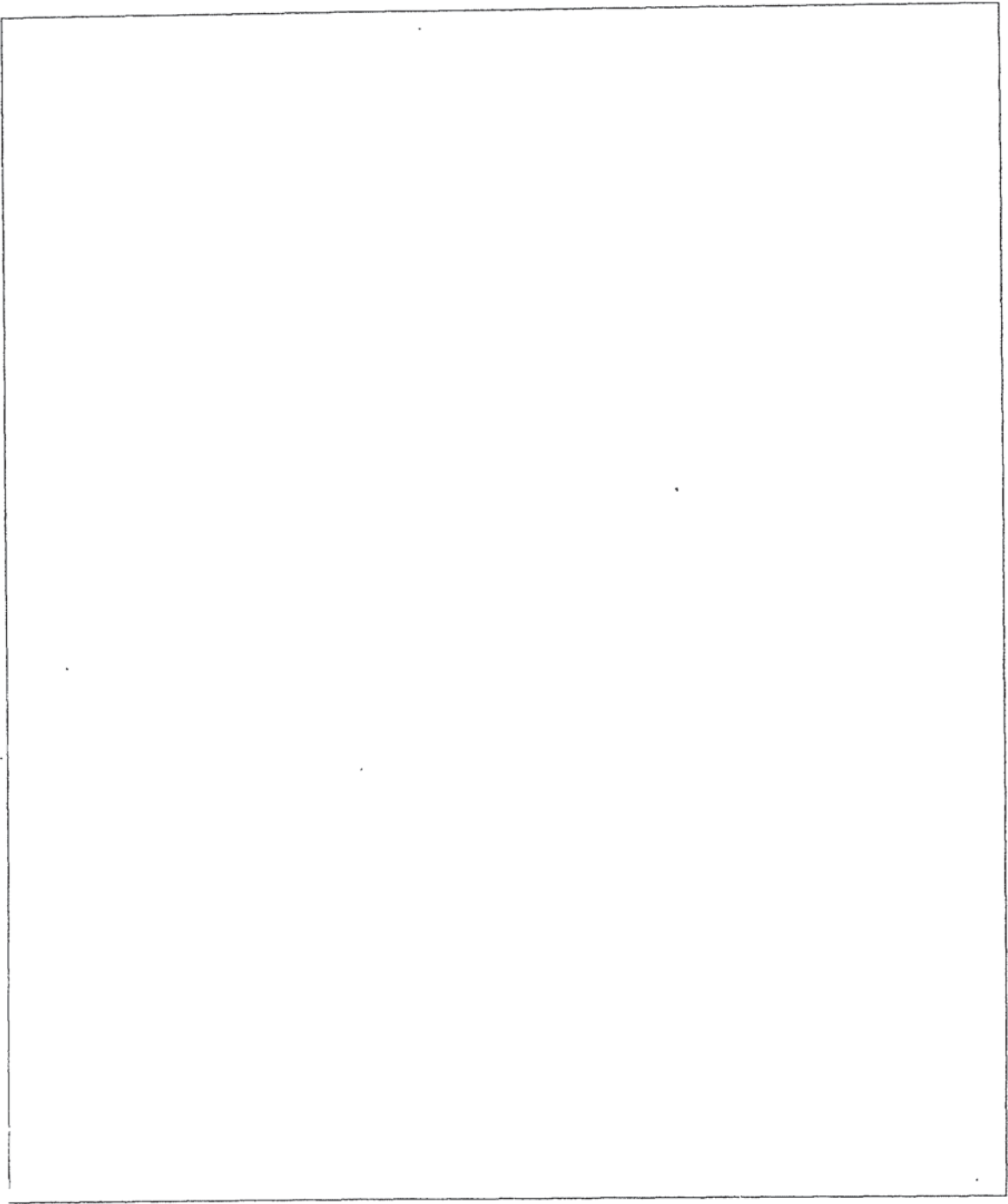
22. (TS//NF) The PRB denied Kiriakou's request on or about October 17, 2008 because the use of the magic box was considered classified [redacted]

~~TOP SECRET~~ [redacted]



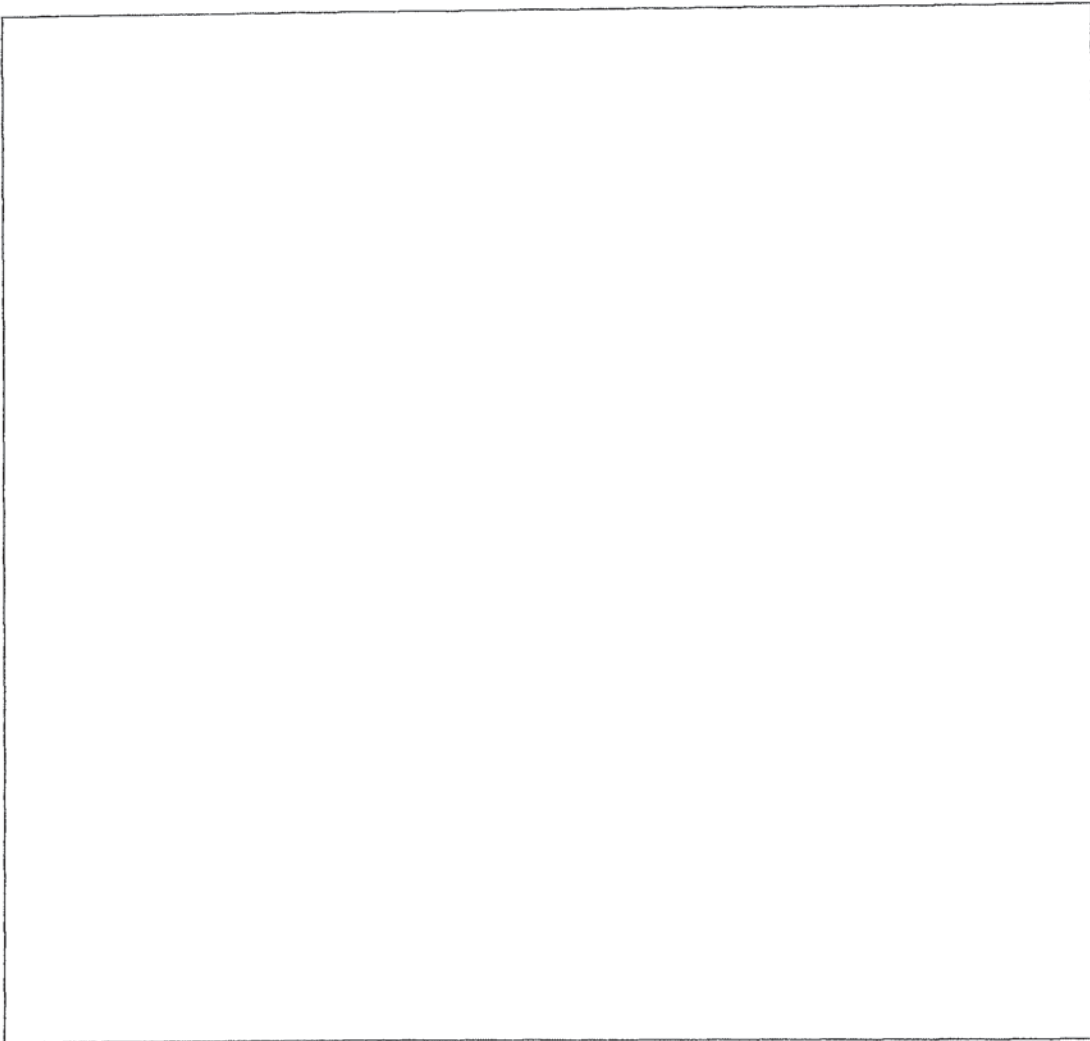
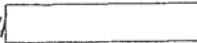
~~TOP SECRET~~ [redacted]

TOP SECRET// [redacted]



TOP SECRET// [redacted]

TOP SECRET//



(U) *Other*



TOP SECRET//



[redacted]

(U) 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. A classified Attachment to the Motion identifies numerous persons by name, alleges that those persons have direct knowledge and could testify about the detention and interrogation of [redacted] while in the HVD program, and makes factual claims regarding those persons' intelligence activities on behalf of the United States government.

[redacted]

[redacted]

~~TOP SECRET~~ [redacted]

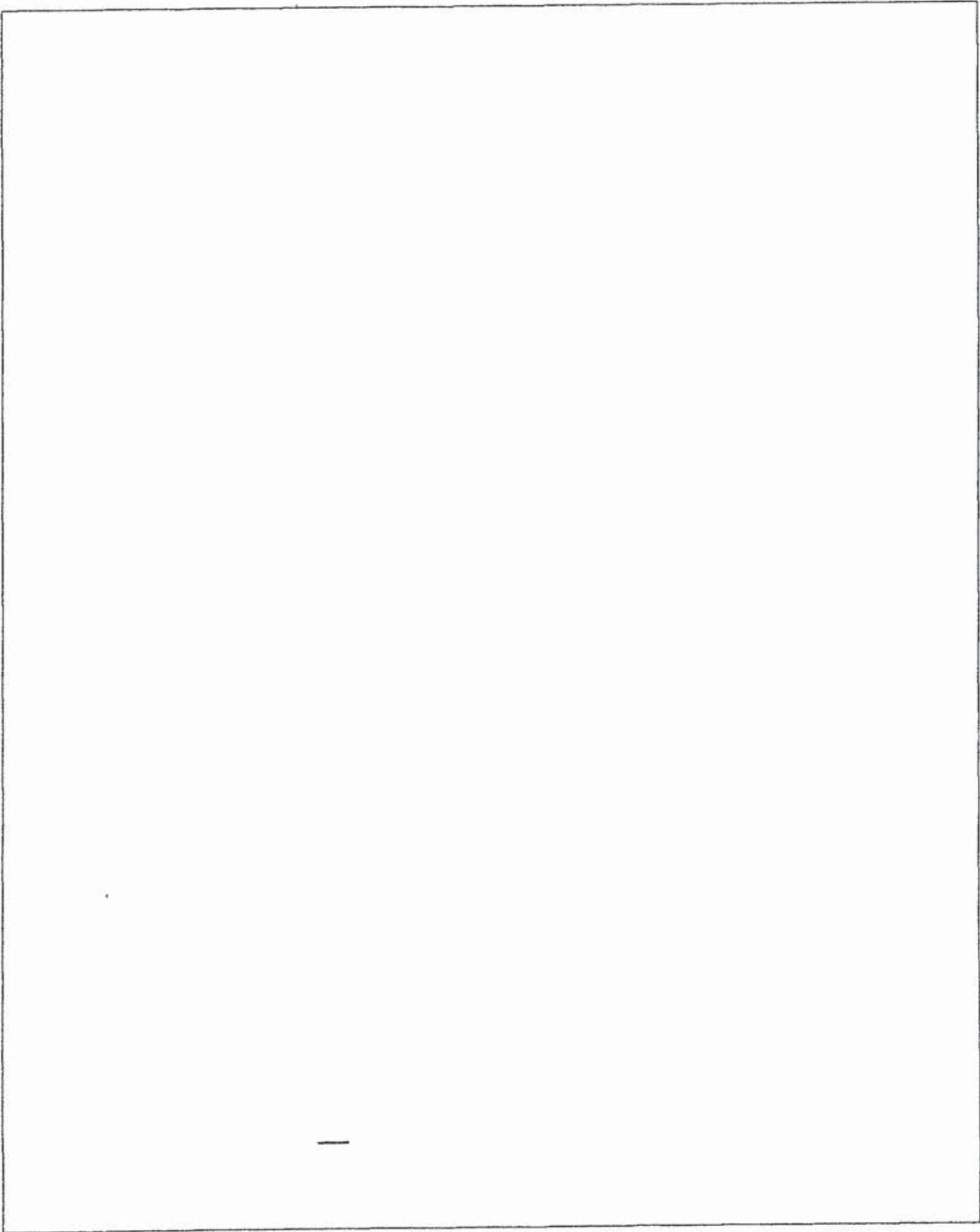
request by providing subscriber information and non-content email header information (i.e., sender, recipient, date, and time of email communications without email subject lines). Based on the subscriber information provided by Apple, the Mac Account was active and registered to John Kiriakou at [redacted] Arlington, VA [redacted] is Kiriakou's home address. The Mac Account had been active since June 5, 2005.

38. ~~(TS)~~ [redacted] ~~(NF)~~ As described further in paragraphs 39-57, *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] (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., [redacted] "Employee-2," "Employee-3," respectively). These colleagues were also identified in the Attachment to the Motion and are included in the group subsequently interviewed by CIA and FBI personnel, as referenced in paragraph 8, *supra*. I have reviewed reports memorializing the substance of these interviews and spoken with individuals who were present at the interviews.

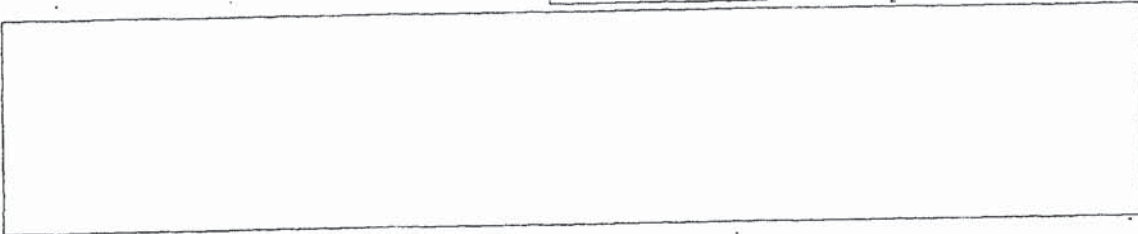
~~(S/NF)~~ [redacted]

~~TOP SECRET~~ [redacted]

~~TOP SECRET~~ [redacted]



~~TOP SECRET~~ [redacted]



47. (TS// [redacted] /NF) On June 30, 2008, approximately one week after the publication of the New York Times article, Kiriakou sent an email to [redacted]'s personal email address. The email, 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]'s 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.

48. (TS// [redacted] /NF) After the New York Times article was published, [redacted] recalls receiving an email not only from Kiriakou, but also from [redacted] and from [redacted]. [redacted] Based on [redacted]'s recollection, both [redacted]

TOP SECRET/ [redacted]

contacted [redacted]'s personal email address. As with [redacted] had not provided his email address to [redacted]

49. (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 [redacted]). From in or about December 2007 through in or about April 2008, there were at least 6 email contacts between Kiriakou and [redacted] (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 [redacted] direct telephone line at [redacted] was in contact with a phone number associated with John Kiriakou on or about May 15, 2008. Specifically, [redacted] phone called Kiriakou's phone, and the two spoke for approximately 5 minutes (303 seconds).

TOP SECRET/ [redacted]

51. (U) Prior to [redacted] March 18, 2009 email, Kirjakou and [redacted] 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).

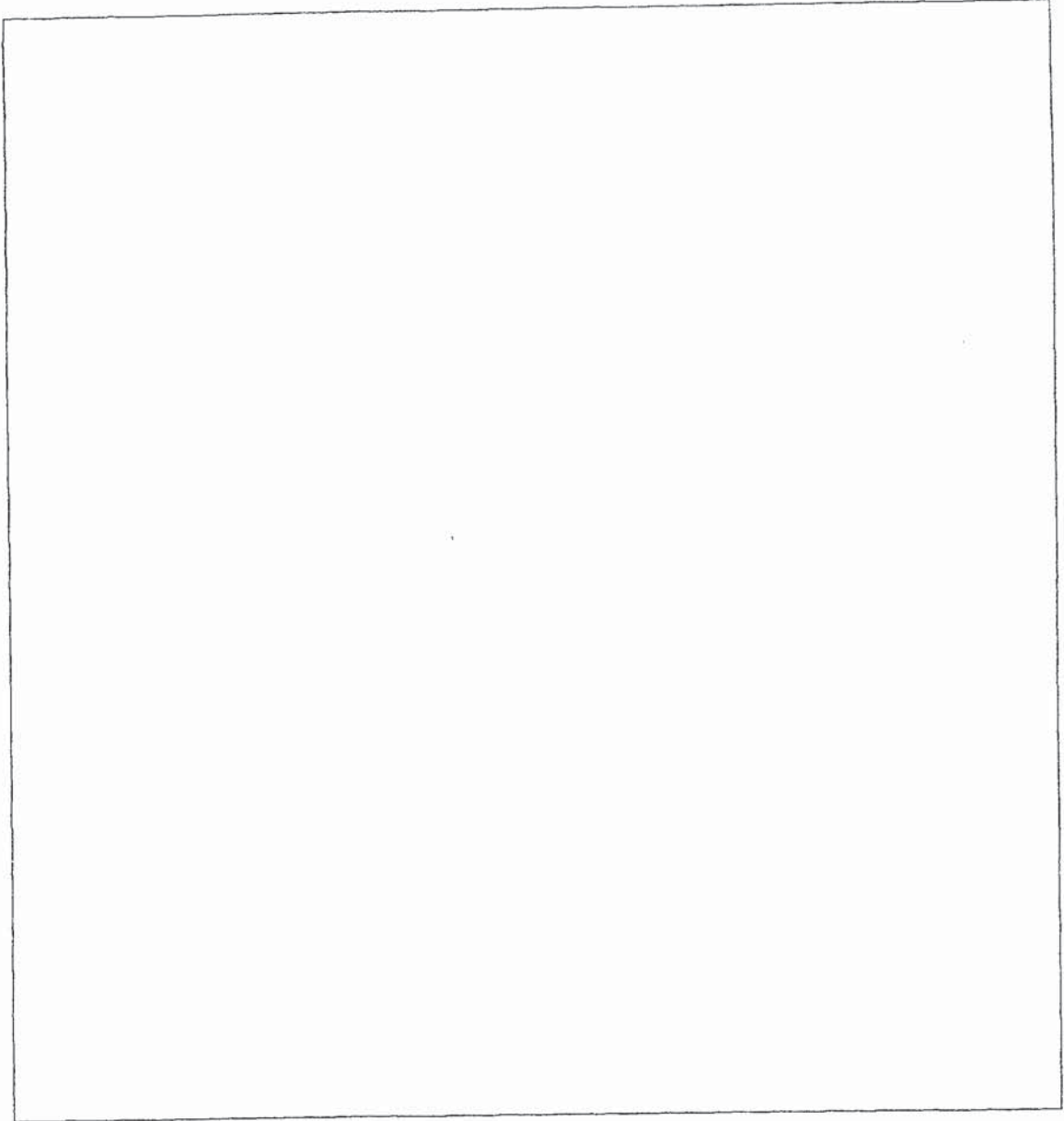
(U) Employee-2

52. (S//NF) Employee-2 [redacted]

[redacted] was contacted by three journalists in 2009, as

described further below. [redacted]

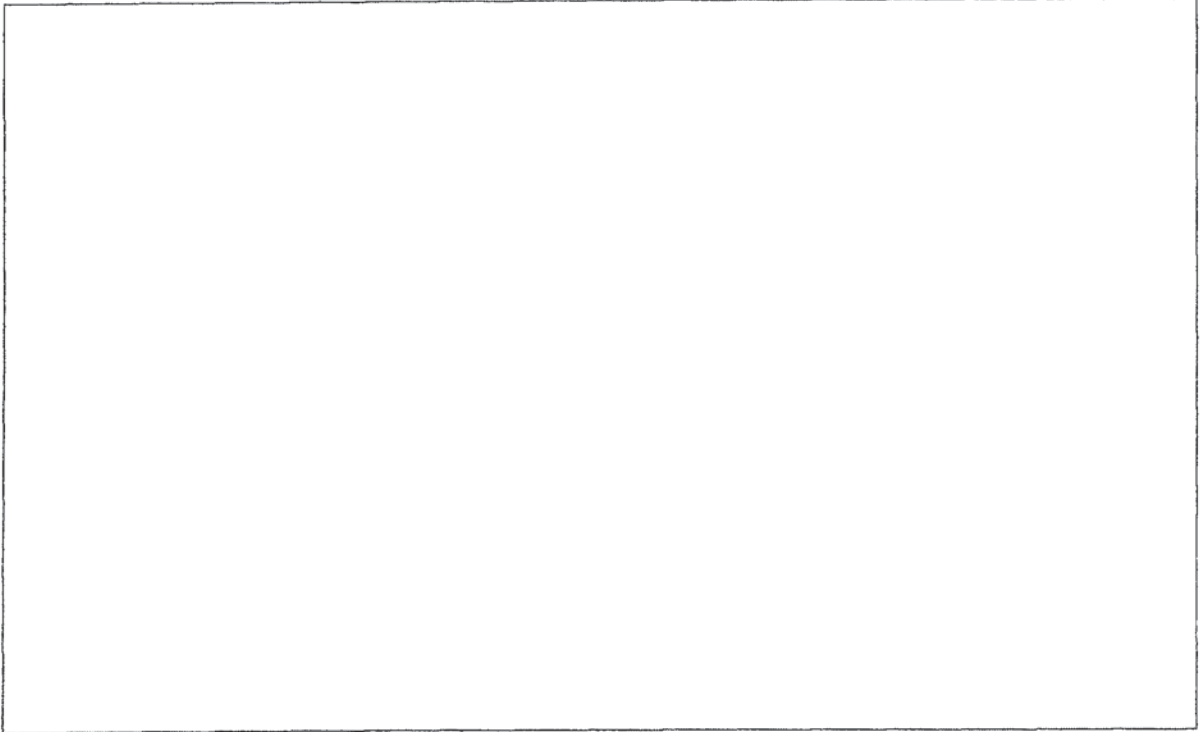
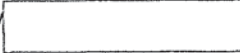
~~TOP SECRET~~ [redacted]



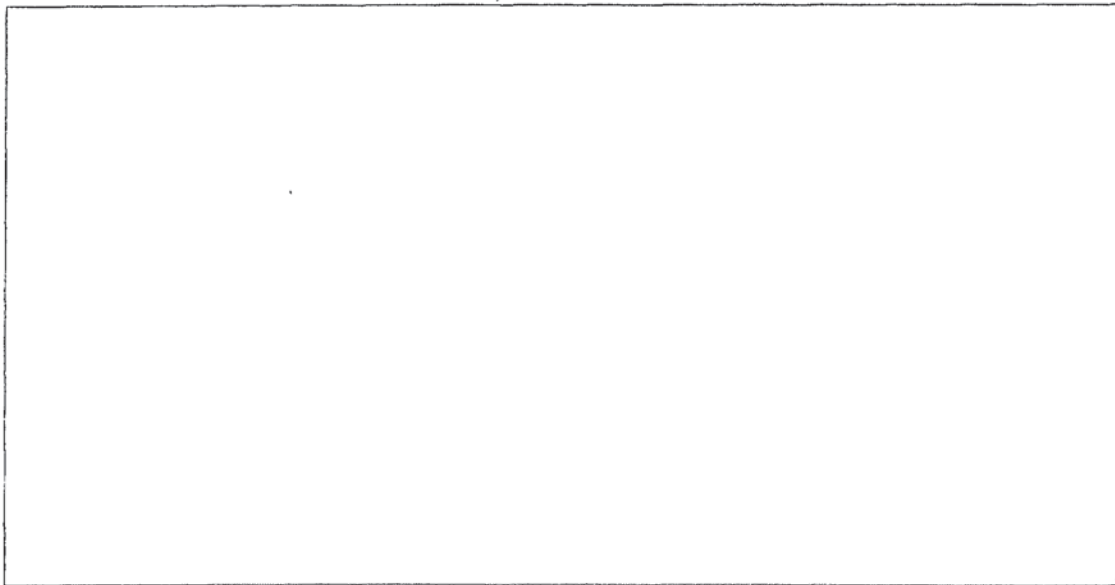
¹⁰ (U) It is noteworthy that, based on the Mac Account Emails, Kiriakou also served as an [redacted] consultant from approximately September 2008 through approximately March 2009, based on a review of Kiriakou statements in the media.

~~TOP SECRET~~ [redacted]

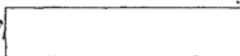
TOP SECRET//

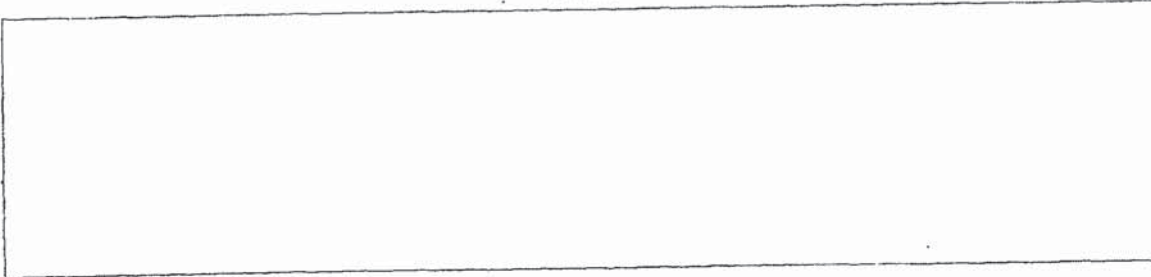


(U) Employee-3



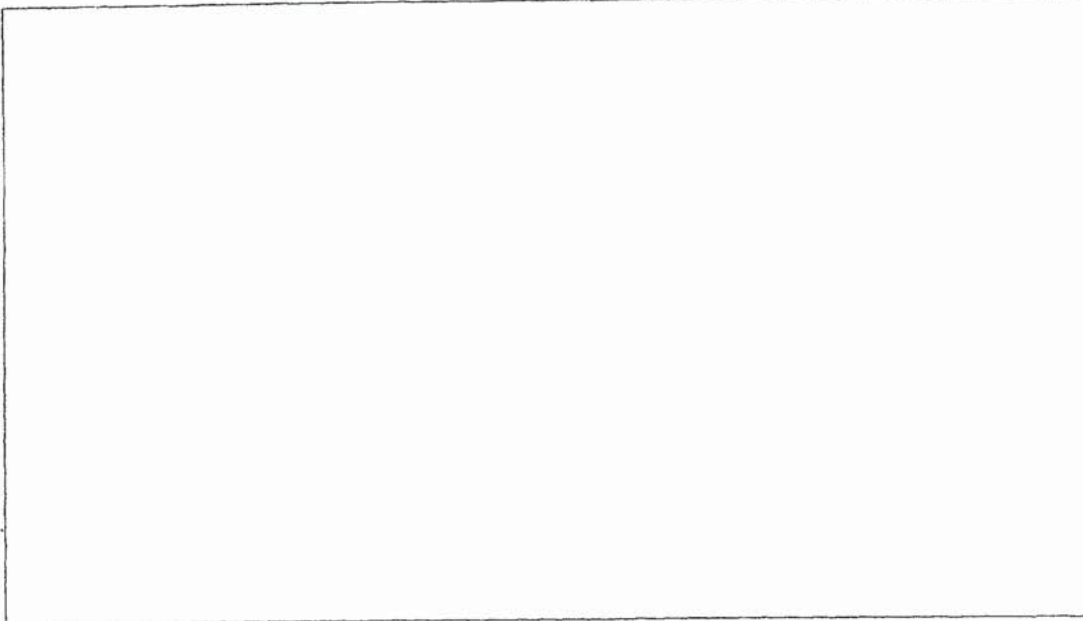
TOP SECRET





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

57. (S//NF) Other than [redacted] Employee-2, and Employee-3, who were both identified in the Attachment to the Motion and contacted by journalists, there were other former CIA colleagues of Kiriakou, who, although they were not contacted by journalists, were identified in the Attachment to the Motion and had contact with Kiriakou. [redacted]



58. (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.

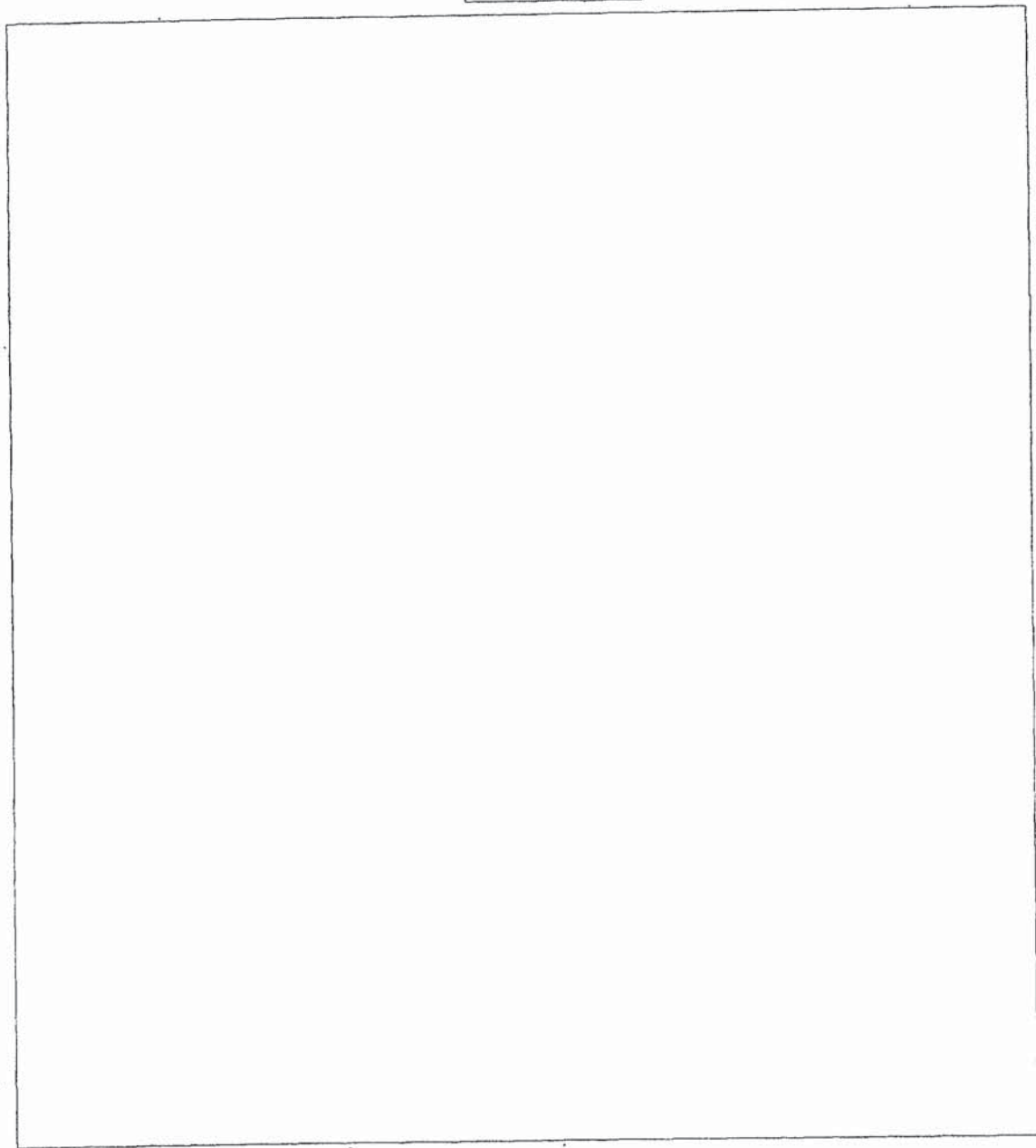
(U) Search of the Mac Account

59. (TS/ [redacted] NF) On or about November 19, 2010, the U.S. District Court for the District of Columbia issued a warrant authorizing the search of the contents of the Mac Account. Thereafter, Apple, Inc. provided the email contents for the Mac Account (the "Mac Account Emails"), selections of which are excerpted below. The CIA's classification review of the information contained within the emails is ongoing and not complete. However, as a general matter, I know that specific details regarding CIA operational activity, the identities and activities of covert CIA personnel, CIA sources and methods, and details relating to intelligence relationships with foreign governments, foreign officials, and human sources are often classified. In addition, in at least one instance, Kiriakou emailed photographs he described as "classified," *see infra* paragraph 59(a); in multiple instances Kiriakou emailed a photograph he described as

[redacted]

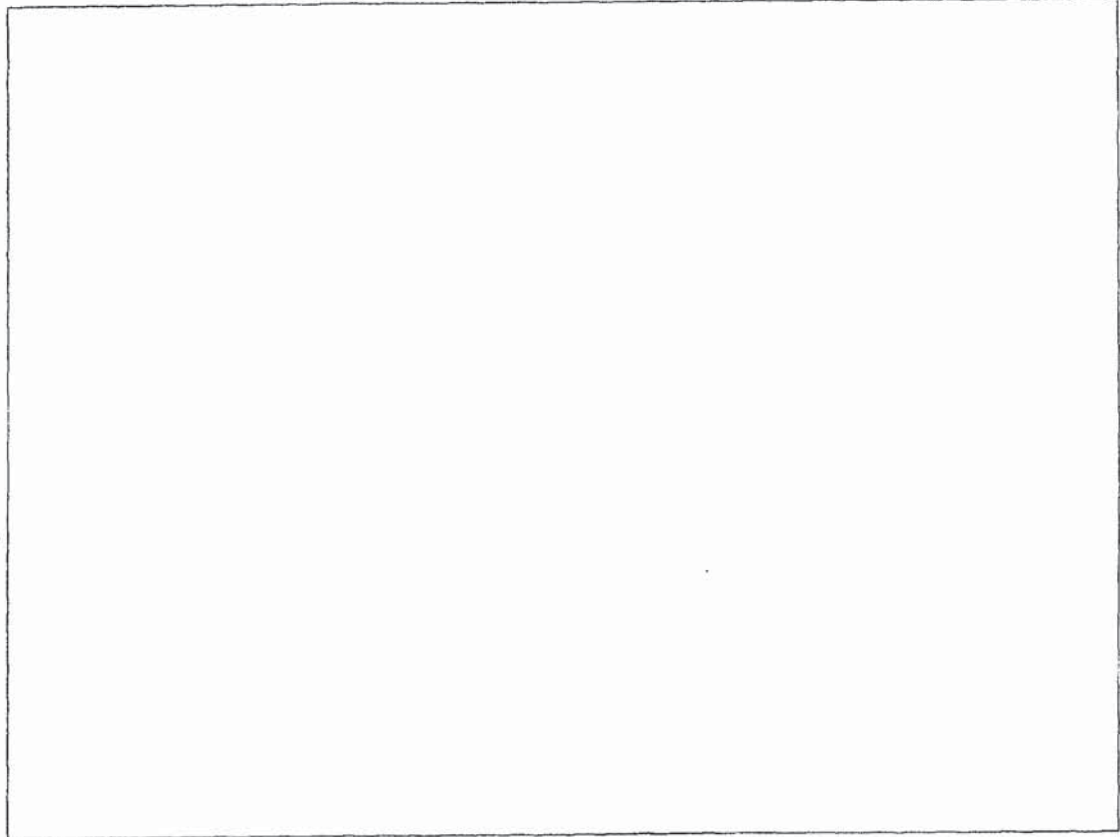
[redacted] *see infra* paragraph 59(b); and in at least two instances Kiriakou wrote about CIA personnel he described as being "under cover," *see infra* paragraph 59(g) and 60(e). These communications occurred using a commercial email account not approved for sensitive or classified communications and with persons not engaged in official government business, including reporters and Kiriakou's co-author. Among the emails discovered were the following:

~~TOP SECRET//~~ [redacted]



¹¹ (U) For approximately 24 years, until on or about November 12, 2008, [redacted] was a reporter for the [redacted]

~~TOP SECRET//~~ [redacted]



c. (U) *Correspondence with Book Coauthor* [REDACTED] On or about August 17, 2008, Kiriakou sent an email to [REDACTED] the co-author of his book *The Reluctant Spy*, and attached a copy of a letter to the PRB. In the email, Kiriakou admits to lying about the origin of information in his manuscript to PRB officials conducting his classification review. Specifically, Kiriakou wrote, "Here you go, [REDACTED] I laid it on thick. And I said some things were fictionalized when in fact they weren't. There's no way they're going to go through years of cable traffic to see if it's fictionalized, so we might get some things through. Enjoy. John." Further, in multiple emails, Kiriakou exchanged manuscript drafts with [REDACTED]

[redacted] which contained information that the PRB has advised Kiriakou is classified.

d. (TS/ [redacted] /NF) Correspondence with [redacted] Reporter [redacted]
[redacted] On or about April 21, 2008, [redacted] Reporter [redacted] informed Kiriakou that he "[d]rove around Va yesterday in the rain and stoped by [redacted]'s house. I couldn't figure it out-- two big dogs in the house, but no one around and a newspaper dated April 9 in front of the door. Also, the cell number on his [redacted] card seems not to work. Any further suggestions on how to find him most welcome" Kiriakou replied, "As for [redacted] I don't know what to make of it. The numbers I have are [redacted] (home) and [redacted] (cell). Is that what I gave you from the business card? His email is [redacted] It's very odd that the dogs were barking and that old paper was out . . . Please let me know if I can be of any further help." As of the date of the email correspondence, the contact info that Kiriakou provided for [redacted] [redacted] was accurate. On or about [redacted] May 29, 2008, [redacted] also emailed Kiriakou with contact information for "[redacted]" from a [redacted] [redacted] Web site link. In response, Kiriakou stated, "What an odd link this is! He was DEFINITELY in Pakistan when he did this."

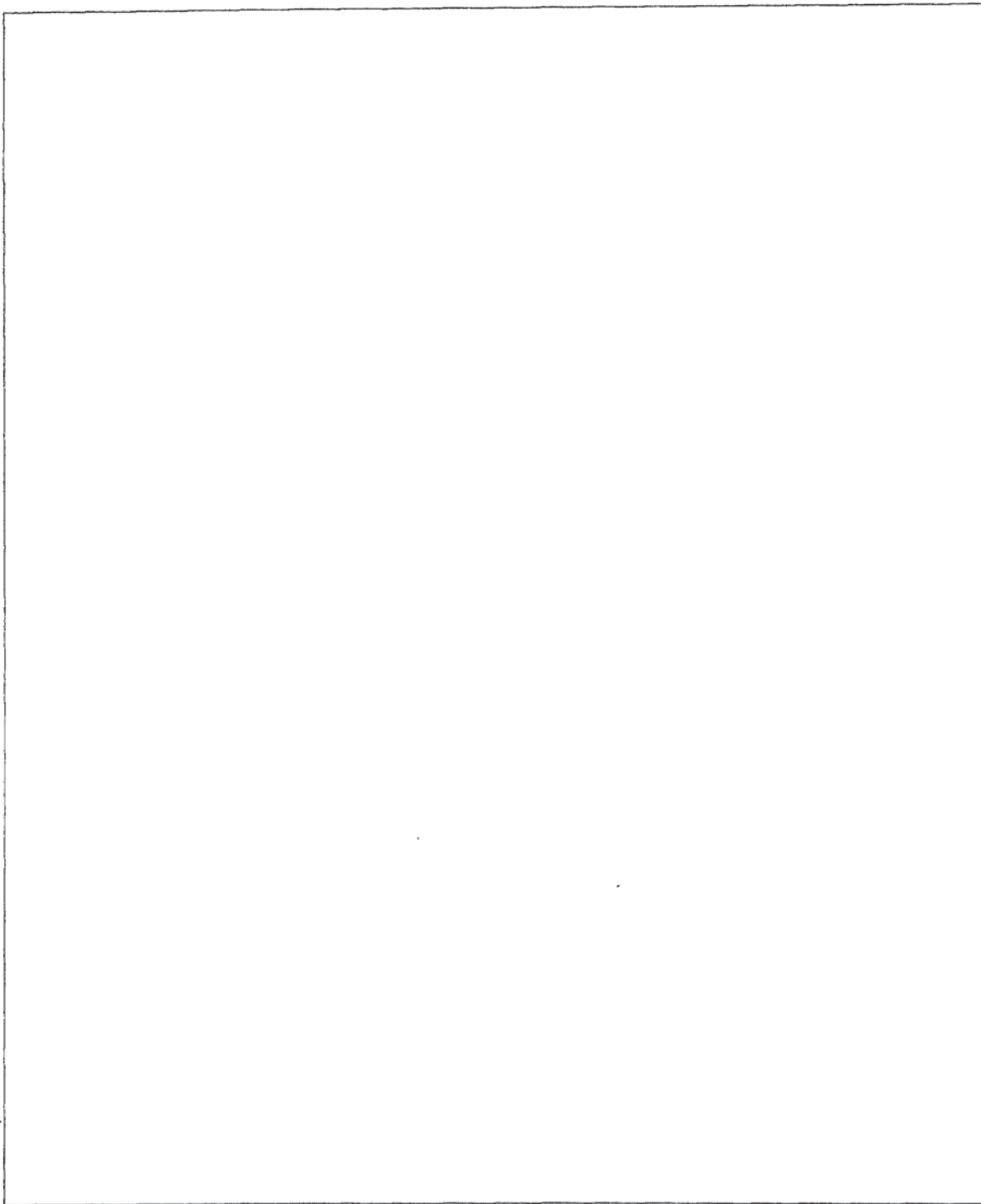
e. (FS/[redacted]/NF) *Correspondence with Reporter [redacted]* On or about November 08, 2007, [redacted] Reporter [redacted] stated to Kiriakou, "It was a pleasure to talk with you yesterday. I appreciate your candor and please know that I'm not newspaper journo [sic], so I'm just not interested in quotes et al. I won't burn you under any circumstances. . . . Thanks again for contacting [redacted] on my behalf. . . ."

f. (S/NF) *Correspondence with [redacted] Reporter [redacted]*

g. (S/NF) *Correspondence with [redacted] Reporter [redacted]* On or about

¹² (U) Based on a review of public source documents and email correspondence between [redacted] and Kiriakou, [redacted] has been a reporter with [redacted] since at least in or about June 2009.

~~TOP SECRET~~ [redacted]



~~TOP SECRET~~ [redacted]

[redacted]

60. (U) In addition, the Mac Account Emails revealed Kiriakou to have engaged in extensive discussions about information relating to persons associated with the CIA and, in some circumstances, identified in the Attachment to the Motion. For example:

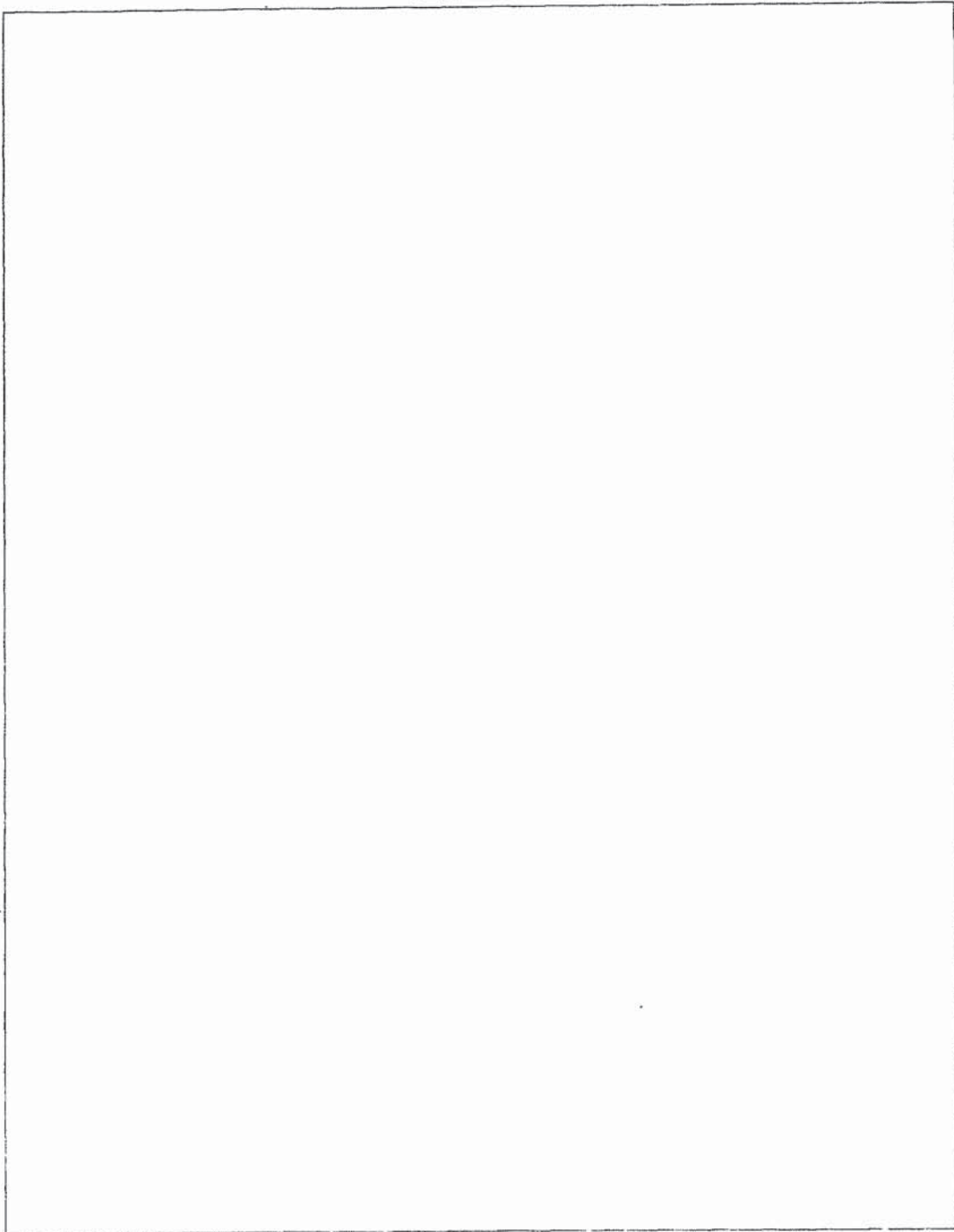
a. (S//NF) On or about January 6, 2010, [redacted] asked Kiriakou whether he had

[redacted]

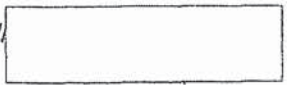
b. (TS// [redacted] NF) On or about January 29, 2010, [redacted] asked Kiriakou,

[redacted]

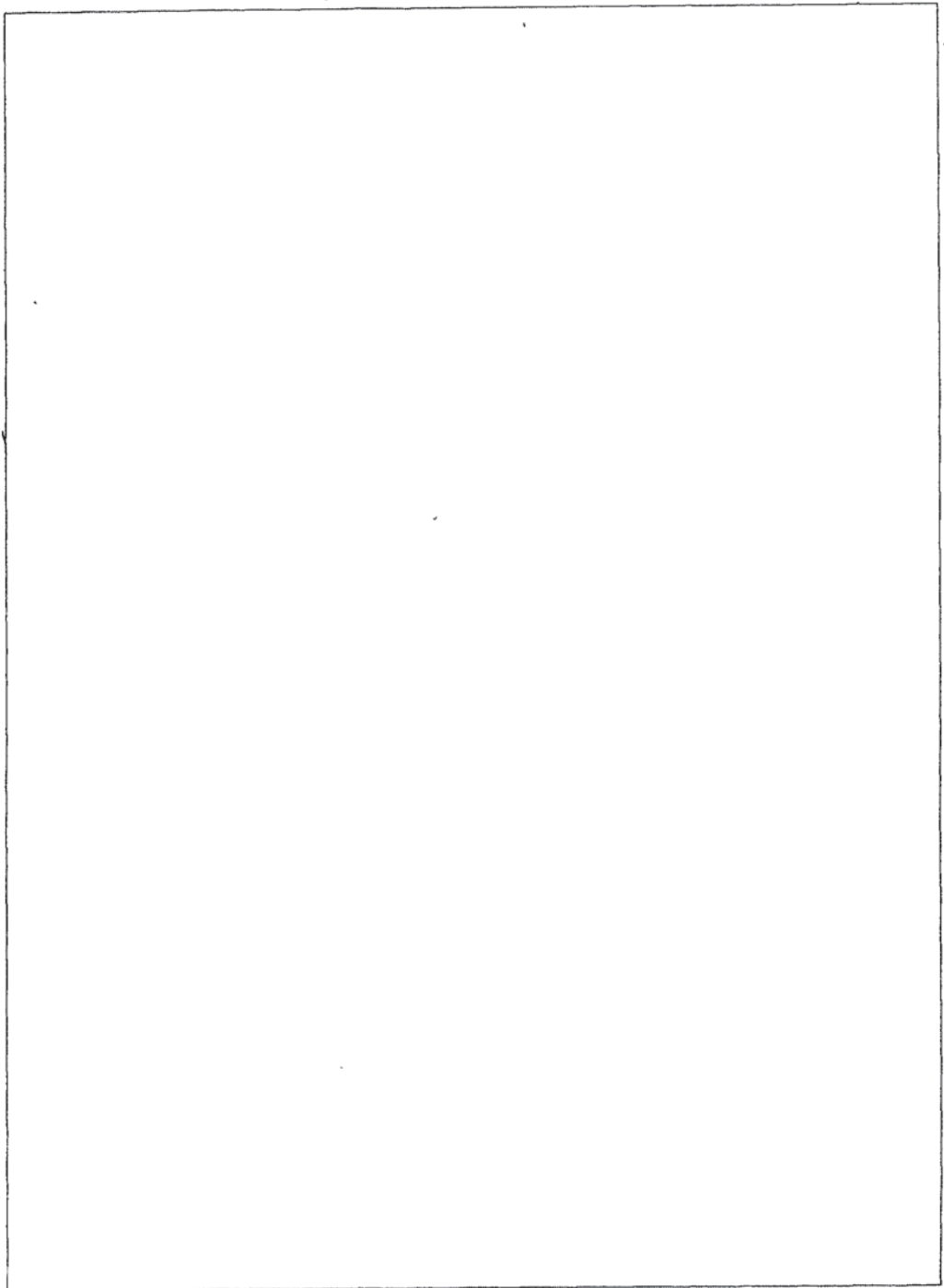
~~TOP SECRET~~



~~TOP SECRET~~



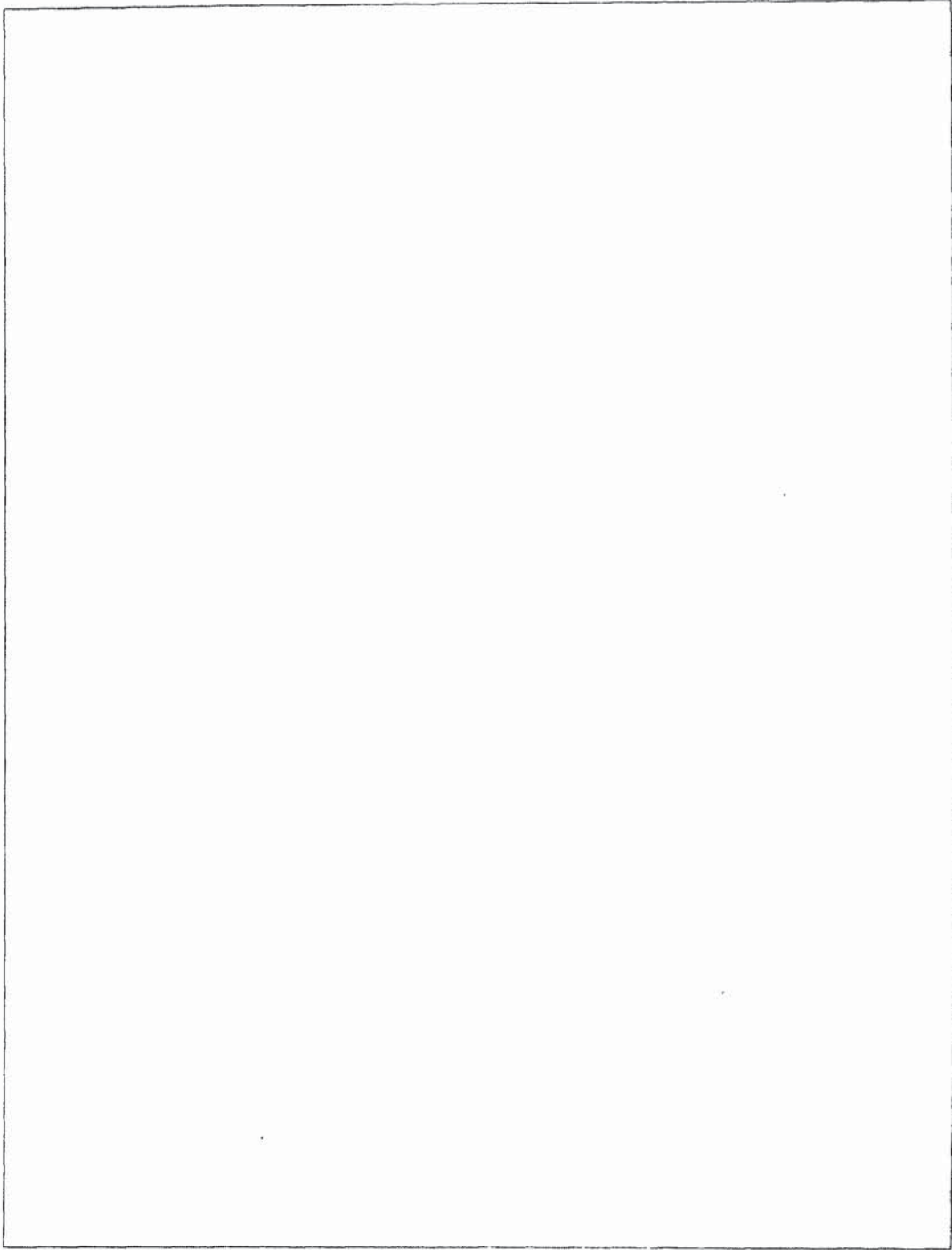
TOP SECRET



TOP SECRET



~~TOP SECRET~~ [redacted]



~~TOP SECRET~~ [redacted]

TOP SECRET/ [redacted]

[redacted]

k. (U) On or about February 10, 2009, [redacted] also asked, [redacted]

[redacted]

l. (S//NF) On or about January 7, 2010, [redacted] informed Kiriakou, [redacted]

[redacted]

m. (U) In summary, the emails establish that Kiriakou was engaged in ongoing communications relating to the identities of former and current CIA personnel.

(U) The Target Account

61. (U) Based on my review of the Mac Account Emails, I have also learned that Kiriakou maintains at least one additional email account from which he emails journalists and that may otherwise include relevant evidence. Specifically, I have learned the following:

TOP SECRET/ [redacted]

TOP SECRET// [REDACTED]

- a. (U) On October 23, 2009, Kiriakou received an email from journalist [REDACTED] [REDACTED] who stated, "Not sure if you got my reply to your very helpful email, or if it disappeared into the ether. If so let me know and I'll resend." Kiriakou replied on October 25 and stated, "Hi [REDACTED] I never received your second email. I even mentioned to [REDACTED] that I wasn't sure if I had been helpful because I hadn't heard from you. If you're having trouble sending to this email, try me also at [REDACTED]" On or about March 3, 2010, in an email from the Mac Account, Kiriakou informed [REDACTED] that he sent an email answering one of [REDACTED] questions "from my spam account."
- b. (U) The Mac Account Emails include multiple emails sent by Kiriakou from the Mac Account to [REDACTED] (the "Target Account"). For example, on or about July 26, 2008 Kiriakou forwarded to the Target Account a series of emails containing scanned pages from multiple books by former CIA officials. (From other correspondence, it appears that Kiriakou was seeking to determine what information the PRB had cleared for other authors, in order to predict what the PRB might approve in Kiriakou's case.) Similarly, on or about November 23, 2008, Kiriakou received an email at the Target Account with the subject line, Hosting Account Setup, from Godaddy.com. (Kiriakou used Godaddy.com to host the website for Rhodes Group, his consulting firm.) Kiriakou then forwarded the email to the Mac Account. He then forwarded the email from the Mac Account to an individual assisting him in designing the Web page.

TOP SECRET [REDACTED]

TOP SECRET [REDACTED]

- c. (U) The Mac Account Emails also include multiple received emails in which persons addressed the same email to both the Mac Account and the Target Account. For example, on or about October 27, 2009, [REDACTED] Reporter [REDACTED] [REDACTED] emailed Kiriakou at both the Mac Email Account and the Target Account with subject line "[REDACTED]"—see below. Am awake. R." and included a link to a news story. Similarly, on or about August 07, 2008, [REDACTED] also emailed Kiriakou at both accounts with subject line "PLEASE READ THIS," with a link to a Wikipedia entry on a criminal defendant, Aafia Siddiqui, arrested the preceding month in Afghanistan and the statement, "I have a lot of info I am just gathering and it may jibe with what you know." In addition, on or about August 11, 2007, and November 12, 2007, [REDACTED] sent an email to Kiriakou at both the Mac Account and the Target Account.¹³
- d. (U) In addition, the Mac Account Emails include sent emails in which Kiriakou included the Target Account as a cc: addressee. For example, on August 11, 2007, Kiriakou sent an email using the Mac Account to [REDACTED] and copied the Target Account, i.e., the [REDACTED] account. Based on this and other Mac Account Emails, [REDACTED] had conducted a recorded interview of Kiriakou to assist [REDACTED] in drafting the book, and these interviews were transcribed. In this August 11 email, Kiriakou responds to a question [REDACTED] had posed about whether

¹³ (U) Based on identifying information associated with the Target Account in both emails from [REDACTED] the Target Account is associated with an individual named "John Kiriakou."

TOP SECRET [REDACTED]

[redacted] should ask the woman who runs the transcription service to sign a non-disclosure agreement, given the sensitivity of the conversation that [redacted] characterized as covering "your life, career and adventures." Kiriakou replied, "And I have complete confidence in your transcription service. If [the woman operating the transcription service] is a friend of yours, that's good enough for me."

- e. (S// [redacted] /NF) Similarly, the Mac Account Emails include one or more emails in which Kiriakou received emails at the Mac Account, but also at the Target Account as a cc: recipient. [redacted]

- f. (U) The Mac Account Emails also included emails reflecting the fact that the Target Account was used as a general alternative email address for Kiriakou. On November 17, 2008, Kiriakou sent an email from the Mac Account to an acquaintance and stated, "Hi [redacted] Thanks for the Facebook invitation. Could you add me as a friend using my other email, which is [redacted] In addition, on October 15, 2008, Kiriakou sent an email to an individual assisting him in designing a website for his consulting firm, Rhodes Group. He referred this individual to his blog and stated that his "userid" is [redacted]

62. (U) On or about February 8, 2011, the Government served a request on Microsoft, the service provider for the Target Account, that the contents of the Target Account be preserved pursuant to 18 U.S.C. § 2703(f), for 90 days. Microsoft assigned preservation record number [redacted] to any data that may be in the Target Account.

(U) Email Records at Microsoft

63. (U) In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Microsoft allows subscribers to obtain e-mail accounts at the domain name hotmail.com, like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, e-mail transaction information, and account application information.

64. (U) In general, an e-mail that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely.

65. (U) When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Microsoft's servers, and then transmitted to its end destination.

Microsoft often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Microsoft server, the e-mail can remain on the system indefinitely.

66. (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 Microsoft but may not include all of these categories of data.

67. (U) An Microsoft 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 Microsoft.

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

69. (U) In general, e-mail providers like Microsoft 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).

70. (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 Microsoft'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.

71. (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.

72. (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.

73. (U) As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Microsoft 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 Microsoft for the relevant account and then to analyze the contents of that account on the premises of Microsoft. The impact on Microsoft'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 Microsoft, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Microsoft 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

74. (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 Microsoft 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

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

~~TOP SECRET~~ [REDACTED]

76. (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).

77. (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.

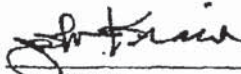
~~TOP SECRET~~ [REDACTED]

TOP SECRET/ [REDACTED]

(U) REQUEST FOR SEALING

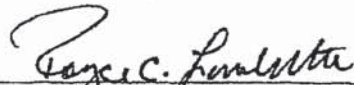
78. (U) I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



John Kralik
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
On March 9, 2011:



UNITED STATES DISTRICT JUDGE

TOP SECRET/ [REDACTED]

~~TOP SECRET~~ [REDACTED]

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with [REDACTED] that is stored at premises owned, maintained, controlled, or operated by Microsoft, a company headquartered at Redmond, Washington.

~~TOP SECRET//~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft

To the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft, Microsoft 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 Microsoft and any person regarding the account, including contacts with support services and records of actions taken.

~~TOP SECRET~~ [REDACTED]

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) 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.
- b. Communications and records relating to CIA personnel, operations, sources, and methods.
- c. Communications and records relating to communications with news organizations and journalists.
- d. Communications and records relating to who created, used, or communicated with the account and identifier, including records about their identities and whereabouts.

~~TOP SECRET~~ []

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

~~TOP SECRET~~ []