Case No. 07-MJ-515-AK

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, JASON W. LAWLESS, being duly sworn, depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") working at FBI Headquarters in Washington, D.C. I am currently assigned to an FBI Counterintelligence Squad. I have been an FBI Special Agent for five years, have completed FBI training in the proper handling of classified information, have investigated crimes involving the unlawful disclosure of national security information, and have been involved in the execution of search warrants and seizing evidence from residences and other locations. Before FBI employment, I worked for three years as a prosecuting attorney in Nashville, Tennessee.

2. I am currently assigned to a task force that is conducting an investigation into the unauthorized disclosure, or "leak," of classified information to two New York Times ("NYT") reporters, James Risen and Eric Lichtblau, who work in the NYT's Washington, D.C. Bureau, concerning alleged activities of the National Security Agency ("NSA"), including the Terrorist Surveillance Program ("TSP"). The investigation concerns potential violations of Title 18, United States Code (U.S.C.), Sections 793 (Unlawful Disclosure of Classified National Defense Information), 798 (Unlawful Disclosure of Classified Information) and 371 (Conspiracy To Commit an Offense Against The United States). As detailed below, the investigation to date has established probable cause to believe that William Edward Binney ("Binney"), Diane Sue Roark ("Roark"), Edward Francis Loomis ("Loomis"), John Kirk Wiebe ("Wiebe"), and Thomas Andrews Drake ("Drake"), have without authorization removed and retained

classified documents or materials at an unauthorized location, or created documents from memory that contained classified information in unauthorized space, that is, their respective homes, and disclosed such information to other persons not authorized to receive it, including at least one member of the media.

3. This affidavit is made in support of an application for warrant authorizing the search of an electronic mail (email) account controlled by EarthLink, Inc. ("EarthLink"), which is more fully described in Attachment A and provides email services for Thomas Andrews Drake, and the seizure of classified information and/or evidence establishing the unauthorized disclosure of classified documents or materials, in violation of one or more of the aforementioned statutes. A listing of items to be seized at the premises is described in Attachment B.

4. The facts set forth in this affidavit are those personally known to me, or communicated to me by other FBI Special Agents and personnel with knowledge of this investigation. Since this affidavit is being submitted for the limited purpose of securing search warrants, I have set forth only those facts which I believe are necessary to establish probable cause to believe that evidence, instrumentalities, or fruits of the above-specified offences will be located at the aforementioned premises.

II. COMPUTERS, THE INTERNET, AND EMAIL

5. I have spoken to FBI agents who have training and experience in the investigation of computer-related crimes. Based on these discussions, as well as my own law enforcement training, experience, and general knowledge, I know the following:

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. The term "computer," as used

herein, is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device. With a computer connected to the Internet, an individual computer user can make electronic contact with other computers around the world. This connection can be made by modem, local area network, wireless access, and other methods.

b. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. In order to send email, a computer user typically uses email service provided by a Service Provider, which operates a host computer system with Internet access. When the user sends email, the email originates at the user's computer, is transmitted to the subscriber's Service Provider's mail server, and is then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

6. Based upon my discussions with other FBI agents and law enforcement personnel, I have learned the following about RCN (the "Service Provider"):

a. The Service Provider has email services which are available to Internet users. Subscribers of the Service Provider obtain an account by registering with the Service Provider. The Service Provider requests subscribers to provide basic information, such as name (or company, if applicable), address, zip code and other identifying information.

b. The Service Provider maintains electronic records pertaining to the individuals and companies for which it maintains subscriber accounts. These records include account access information, email transaction information, and account application information.

c. Subscribers of the Service Provider may access their accounts on servers maintained and/or owned by the Service Provider from any computer connected to the Internet located anywhere in the world.

d. Any email that is sent to a subscriber of the Service Provider is stored in the subscriber's "mail box" on the Service Provider's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the Service Provider. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the Service Provider's servers indefinitely.

e. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to the Service Provider's servers, and then transmitted to its end destination. Subscribers of the Service Provider have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from Service Provider's server, the email can remain on the system indefinitely. The sender can delete the stored email message thereby eliminating it from the email box maintained at the Service Provider, but that message will remain in the recipient's email box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations.

U.S. JLC 4/17/07

f. A subscriber of the Service Provider can store files, including emails and image files, on servers maintained and/or owned by the Service Provider.

g. Emails and image files stored by a subscriber on a server maintained by the Service Provider may not necessarily be located in the subscriber's home or personal computer. The subscriber may store emails and/or other files on the Service Provider's servers for which there is insufficient storage space in the subscriber's computer and/or which the subscriber does not wish to maintain in the subscriber's computer. A search of the files in the subscriber's computer will not necessarily uncover the files that the subscriber has stored on the Service Provider's servers.

h. Computers located at the Service Provider may contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for a search warrant seek authorization solely to search the computer accounts and/or files using the procedures described herein and the Attachments.

III. RELEVANT STATUTORY PROVISIONS

7. Title 18, United States Code, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access" ("SCA"). Section 2703 of the SCA sets forth the procedure that federal and state law enforcement officers must follow to compel disclosure of various categories of stored records from network service providers. As shown from the following provisions of Section 2703, the government may compel disclosure of all stored content and records or other information pertaining to a customer or subscriber of an electronic communication service or remote computer service pursuant to a warrant issued using the procedures

described in the Federal Rules of Criminal Procedure.

a. Title 18, United States Code, Section 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant . . .
>
> (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service–
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a

subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. Title 18, United States Code, Section 2703(c) provides, in part:

The government may also obtain records and other information pertaining to a subscriber to or customer of electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(2). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(3).

IV. BACKGROUND

A. The Attacks of September 11

8. On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States – to kill the President, the Vice President or

Members of Congress. The attacks of September 11 resulted in approximately 3,000 deaths, the highest single-day death toll from hostile foreign attacks in the Nation's history. The attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy.

9. On September 14, 2001, the President declared a national emergency "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001). The same day, Congress passed a joint resolution authorizing the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11, which the President signed on September 18. Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541). Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and in particular recognized that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmbl. Congress emphasized that the attacks "continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States." *Id.* The United States also launched a large-scale military response, both at home and abroad. In the United States, combat air patrols were immediately established over major metropolitan areas and were maintained 24 hours a day until April

2002. The United States also immediately began plans for a military response directed at al Qaeda's base of operations in Afghanistan. Acting under his constitutional authority as Commander in Chief, and with the support of Congress, the President dispatched forces to Afghanistan and, with the assistance of the Northern Alliance, toppled the Taliban regime.

10. Against this unfolding background of events in the fall of 2001, there was substantial concern that al Qaeda and its allies were preparing to carry out another attack within the United States. Al Qaeda had demonstrated its ability to introduce agents into the United States undetected and to perpetrate devastating attacks, and it was suspected that additional agents were likely already in position within the Nation's borders. To counter this threat, the President authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. Press Conference of President Bush (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html. This activity – which subsequently was identified as the Terrorist Surveillance Program (TSP) – was "critical" to national security and was designed to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

B. **The Unauthorized Disclosure Of Classified Information Concerning The TSP**

11. In early October 2004, James Risen contacted Public Affairs officials in the Office of the Vice President, the National Security Council, the Central Intelligence Agency ("CIA") and the NSA about a news article he was writing. The Public Affairs

officials and other high-ranking Executive Branch officials have confirmed that during the ensuing days, Risen engaged in a series of email communications, conversations and meetings with the officials regarding the story. In substance, Risen represented that he had obtained information about a warrantless electronic surveillance program that he said was known to only a few officials within the United States Government. Ultimately, Risen's inquiries led to a meeting on October 25, 2004, at The White House, involving other representatives of The New York Times and high-ranking Executive Branch officials. This was followed by another meeting about ten days later at the Department of Justice involving Risen, Lichtblau, a third NYT representative, and several high-ranking Executive Branch officials. Subsequent to this meeting, NYT representatives elected not to publish Risen's story without first conferring further with the high-ranking Executive Branch officials. As a result, no story regarding the TSP was published in 2004.

12. Approximately one year later, in the fall of 2005, NYT representatives again contacted high-ranking Executive Branch officials and advised that they were considering publishing the story. In that regard, it was represented that additional "sources" had come forward and raised concerns about the surveillance activities. A number of meetings ensued between representatives of the NYT, high-ranking Executive Branch officials, and Members of Congress. Despite these ongoing discussions, the NYT published its story on its website the evening of December 15, 2005. The story, titled *Bush Lets U.S. Spy on Callers Without Courts*, was authored by Risen and Lichtblau and appeared in the next day's edition of the newspaper. This article was followed by a series of NYT articles, written or co-authored by Risen and/or Lichtblau describing a range of alleged NSA activities and related circumstances, including:

a. *Spy Agency Mined Vast Data Trove, Officials Report*, Dec. 24, 2005, by James Risen and Eric Lichtblau;

b. *Defense Lawyers in Terror Cases Plan Challenges Over Spy Efforts*, Dec. 28, 2005, by James Risen and Eric Lichtblau;

c. *Justice Deputy Resisted Parts of Spy Program*, Jan. 1, 2006, by James Risen and Eric Lichtblau; and

d. *Spy Agency Data After Sept. 11 Led FBI to Dead Ends*, Jan. 17, 2006, by Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta, Jr.

13. In early January 2006, Risen published a book, titled State of War: The Secret History of the CIA and the Bush Administration. Chapter 2 of the book was entitled, "The Program," and dealt entirely with alleged NSA activities, including the warrantless surveillance program described in the Risen and Lichtblau articles.

14. Since publication of the aforementioned articles and book, there have been numerous additional stories in various media, including but not limited to newspapers, magazines, television, radio and the internet, regarding the TSP and related matters. As set forth below, one such article, which appeared in

suggests that one or more of the five subjects discussed herein disclosed highly classified information concerning the NSA and its activities, sources and methods, to unauthorized persons.

V. INVESTIGATION OF THE LEAK OF CLASSIFIED INFORMATION CONCERNING THE TSP

15. Shortly after the first TSP article, in late December 2005, the DOJ and the FBI initiated an investigation concerning the unauthorized disclosure of classified

information contained in that article. That investigation has been continuing since that time and has involved interviews of in excess of 1,000 individuals, issuance of more than 200 grand jury subpoenas, principally for telephone and email records, and review of thousands of pages of documents, including telephone and email records for approximately 60 individuals.

A. Background Regarding Five Subjects Of The Investigation

16. Through that process, the following individuals, among others, have been identified as subjects of the investigation: (a) William Binney, a former senior operations officer for the NSA, who now resides in Severn, Maryland; (b) Diane Roark, a former staff member on the U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI), who now resides in Stayton, Oregon; (c) Edward Loomis, a former cryptologic computer scientist at NSA, who now resides in Baltimore, Maryland; (d) John Wiebe, a former acting division chief at NSA, who now resides in Westminster, Maryland; and (e) Thomas Drake, a current NSA Senior Executive Staff member, who now resides in Glenwood, Maryland.

17. Binney is a former senior operations officer for the NSA who retired on October 31, 2001, after 36 years of service. Since 2004, Binney has worked as a contractor for the NSA and, until July 26, 2007, had entered NSA facilities approximately two times a year. After retiring, Binney started a three-person contracting firm on December 3, 2001, with Loomis and Wiebe. The company is called Entity Mapping LLC (Entity). According to Binney, the company has done work for NSA, Boeing, and the Department of Homeland Security. In addition to being a partner in Entity, Binney worked for Eagle Alliance from October 2001 to October 2002; Zytel Corporation

(General Dynamics sub-contractor) from November 22, 2002, to May 5, 2004; Diversified Development Corporation from July 2002 to the present; and Entegra Systems, Inc. from October 2005 to the present. While working at the NSA, Binney was the program manager of a program called Additionally, he had regular contact with Roark while she was serving as a HPSCI staff member. At no time during or subsequent to his employment at the NSA has Binney been authorized to possess NSA classified documents or data at his home or on his personal computer.

18. Roark is a former Congressional staff member who worked for seventeen years on the HPSCI until she retired in April 2002. At the HPSCI, Roark assisted in oversight of various compartmentalized intelligence programs at the NSA, as well as related Congressional budget approval issues. After Roark left the HPSCI, she stayed in the Washington, D.C., area until early 2003, when she moved to Oregon. At no time during or subsequent to her service on the HPSCI has Roark been authorized to possess NSA classified documents or data at her home or on her personal computer.

19. Loomis is a former cryptologic computer scientist for the NSA who retired in November 2001 after twelve years of service. Since the end of 2002, Loomis has worked as a contractor for the NSA and, until July 26, 2007, entered NSA facilities on a regular basis. After retiring, Loomis started Entity, the above mentioned three-person contracting firm, with Binney and Wiebe. The company's corporate headquarters is located at 515 Overdale Road, Baltimore, Maryland, which is also Loomis' home address. In addition to being a partner in Entity, Loomis worked for Eagle Alliance from November 2001 to October 2002; GTE Tactical Systems (General Dynamics sub-contractor) from November 2002 to present; and Diversified Development Corporation

from October 2002 to the present. At no time during or subsequent to his employment at the NSA has Loomis been authorized to possess NSA classified documents or data at his home or on his personal computer.

20. Wiebe is a former acting division chief for the NSA who retired in October 2001 after approximately 26 years of service. After Wiebe retired from the NSA, he continued to work as a contractor for the NSA and, until July 26, 2007, regularly entered NSA facilities. On December 3, 2001, Wiebe started Entity with Binney and Loomis. In addition to being a partner in Entity, Wiebe worked for Eagle Alliance from October 2001 to November 2002; Diversified Development Corporation from September 2002 to the present; and GTE Tactical Systems (General Dynamics sub-contractor) from April 2003 to present. At no time during or subsequent to his employment at the NSA has Wiebe been authorized to possess NSA classified documents or data at his home or on his personal computer.

21. Drake was hired at NSA as the Chief of the Signal Intelligence Directorate (SID) Change Leadership and Communications Office on September 10, 2001. Prior to being hired at NSA, Drake was acquainted with Roark through professional affiliations, and was employed at Booz Allen Hamilton and Integrated Computer Concepts Inc. as a fully cleared NSA contractor. In August 2006, Drake began working as the NSA Chair for the Industrial College of the Armed Forces (ICAF), National Defense University (NDU), Fort McNair, Washington, D.C. At no time during his employment at the NSA has Drake been authorized to possess NSA classified documents or data at his home or on his personal computer.

L.C. JCW 12/17/07

22. On July 26, 2007, search warrants were executed at the residences of Binney, Wiebe, and Roark, and a consent search was executed at the Loomis residence. A District of Maryland search warrant was obtained for Loomis' home computer(s), but was not executed as Loomis consented to a search of his home, as well as his home computer.[1] As described more fully below, this request for issuance of search warrants relating to Drake is based, in part, on evidence obtained during the Binney, Wiebe and Loomis searches.

B. The Subjects' Unlawful Disclosure Of Classified NSA Information

1. Roark, Binney And Wiebe Disclose To Unauthorized Persons

23. According to NSA officials who have been interviewed in connection with this investigation, in the mid to late 1990s, Binney, Loomis and Wiebe worked on several programs that collected and analyzed data at the NSA. One of these collection programs, which Binney claimed during an FBI interview that he developed,[2] was called . According to Binney, was a pre-cursor to the . Moreover, Binney believed that was less costly to implement and operate than the , and believed that it included features purportedly designed to address concerns associated with NSA activities.

[1] On July 25, 2007, the U.S. Magistrate Judge on duty at the U.S. District Court for the District of Maryland approved search warrants for the residences of Wiebe (case no. 07-2351 JKS) and Binney (case no. 07-2352 JKS) and sealed the application materials. The next day, the court authorized a search warrant for the computer(s) located in Loomis's home (case no. 07-2360 JKS) and sealed the affidavit. On July 25, 2007, the U.S. Magistrate Judge on duty at the U.S. District Court for the District of Oregon approved a search warrant for the residence of Roark (case no. 07MC9169-A) and similarly sealed the affidavit. All of the search warrant applications remain sealed.

[2] Binney has been interviewed by the FBI on three occasions during this investigation: October 19, 2006, March 21, 2007, and June 28, 2007. Additionally, Binney made additional statements to the FBI on July 26, 2007, during the court-authorized search of his residence. Unless otherwise noted, the statements attributed to Binney in this affidavit were made during one or more of three interviews, not in connection with the July 26 search.

24. After 9/11, Binney, Wiebe, and Loomis immediately started packaging as a solution to some of the problems exposed by what they perceived as the way of doing business at the NSA. Similarly, review of Drake's classified email from 2001 forward shows that Drake shared their view, was pushing NSA senior officials to keep operational and funded, and was reporting back to Binney, Wiebe, and Loomis (now former NSA employees) on sensitive NSA information being discussed in the high-level NSA meetings he was attending.

25. Both before and after 9/11, Binney, as the project manager, provided Roark, as the HPSCI staff member with NSA responsibilities, with information regarding . According to Binney, Roark was a strong proponent of the program and worked hard to ensure that it was funded. However, according to Binney and several other NSA employees who were interviewed during this investigation, Roark did not have an accurate understanding of and believed it was

26. Binney explained to the FBI that after 9/11, the NSA decided to scale back the program. By his own admission, Binney was extremely upset about this decision. Moreover, at or about the same time, Binney learned that the TSP was being implemented. Significantly, Binney admitted that he was never "read in" to the TSP program – that is, he was never authorized to receive information concerning the program. He also has admitted, however, that he learned of its existence, its covername (which remains unpublished today) and its basic outlines, from an NSA contractor who

was not authorized to provide Binney this classified information.

27. Binney advised the FBI that because he was upset at NSA's decision to scale back [redacted] in favor of the [redacted] he went to Roark, his contact on the HPSCI. According to Binney, in late 2001, while Roark was still with the HPSCI, Binney met her at her home in Hyattsville, Maryland, outside of normal channels and in an unsecure facility, and told her what he knew about the TSP, a highly classified program. According to NSA officials, Roark also had not been read in to the TSP (indeed, she has never been read in). Nevertheless, Binney informed the FBI that he and Roark then discussed various actions they could take to bring their concerns about the TSP to the attention of people within and outside the United States Government.

28. According to Binney, one step that he and Roark took was to disclose the existence of the TSP to Dale Griffiths, another NSA contractor who, according to NSA officials, was not read in to the TSP. According to Binney, Griffiths was a friend of the daughter of a U.S. Supreme Court Justice, and Binney and Roark hoped that Griffiths could facilitate a meeting with the Justice through the daughter. Binney told the FBI that this effort failed. Binney further stated that at or about the same time, Roark told him that she had called the presiding judge of the Foreign Intelligence Surveillance Court (FISC), Judge Colleen Kollar-Kotelly, to arrange a meeting; however, after an exchange of telephone calls with a court secretary, Roark was told to convey any concerns she had to the DOJ.

29. According to Binney, in late 2001 or early 2002, Roark arranged for him and Wiebe to brief a member of the HPSCI about the TSP. According to NSA officials, that member was not read in to the TSP. Roark also told Binney that she went to the

Chairman of the HPSCI, who was read in to the TSP, to discuss the TSP. According to the Chairman, who has been interviewed during the investigation, he told Roark to speak with General Michael Hayden, then the Director of the NSA, regarding her concerns. According to Binney, Roark told him that she spoke with General Hayden regarding her concerns about the TSP, as well as her belief that | was a superior program. Roark subsequently told Binney that as far as she was aware, no action was taken by the NSA after her discussion with General Hayden.

2. Binney, Roark, Loomis, Wiebe and Drake Disclose Classified NSA Information Without Authorization

30. During his interview(s) with the FBI, including an interview on July 26, 2007 when the search warrant was executed at his residence, Binney stated that in 2002, after he had left the NSA, he, Roark, Loomis and Wiebe created a thirteen-page summary of the technology on his home computer. The idea to create the document originated with Roark, who wrote the first draft. According to Binney, he, Wiebe, and Loomis subsequently wrote technical parts of the summary which the four subjects then emailed back and forth to one another from their home computers. The investigation has further determined that Drake was copied on those emails and, at a minimum, was involved in reviewing drafts of the summary. The subjects wrote the document as part of their effort to market technology solutions to potential customers, including government agencies, in connection with their fledgling contracting business, and to memorialize their views regarding the superiority of | vs. .

31. During his FBI interviews, Binney stated that when the final summary was completed in May 2002, Binney and Loomis, who are not NSA classification authorities, and were not even NSA employees at the time, conducted their own "classification

review" and decided that the document was unclassified. Notably, Binney stated that no effort was made to submit the summary for classification review by appropriate authorities at the NSA. Binney told the FBI that they based their decision not to submit the document for classification review on their view that there was "far worse" on the internet as other contractor firms were far more open with their information than was the summary and, if it was acceptable for other firms to be open about their classified or sensitive information, it was acceptable for them.

32. On March 25, 2007, after his Binney's second FBI interview, Binney voluntarily emailed to the FBI the thirteen-page summary which he originally had helped create in 2002. On May 10, 2007, the FBI provided that document to the NSA and requested that it conduct a thorough classification review of the summary. On June 26, 2007, NSA officials advised the FBI that the summary is a classified document at the level. As noted herein, this document was created, edited and emailed by and between Binney, Roark, Loomis, Wiebe, and Drake. Thus, it appears that a document, classified drafts of the document, and/or classified information contained in or relating to the document and , were and are located on or in the personal computers, email accounts, and/or residence of Drake.

33. This is further corroborated by the results of the search of Binney's residence on July 26, 2007. At that time, two documents were seized which established that Roark had emailed the classified summary to Loomis, Wiebe, Binney, and Drake on May 31, 2002. These documents were sent to Drake at tadrake@earthlink.net, his personal email address, and the document so transmitted

contained information that the NSA has classified as . As stated above, Drake is not authorized to have classified information in his home, his personal computer, and/or in his personal email account. Additionally, Drake's contact information was located in Weibe's address book, which was seized during the search of Weibe's residence. Finally, printed emails from Drake were recovered at the homes of Binney, Wiebe, and Loomis.

34. In connection with this and other investigations in which I have participated, I have learned that individuals who hold security clearances typically sign agreements that they will safeguard classified information, report violations of security rules, and not disseminate classified information to uncleared persons. This matter is no exception. On August 28, 2001, Drake signed a security agreement with the NSA governing his obligations regarding "protected information," which is defined in the agreement as "information obtained as a result of my relationship with NSA which is classified or in the process of a classification determination." The security agreement, a copy of which has been obtained and reviewed, states, in pertinent part:

> I understand that all Protected Information to which I may obtain access hereafter, is and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law.... I agree not to discuss matters pertaining to Protected Information except when necessary for the proper performance of my duties and only with persons who are currently authorized to receive such information and have a need-to-know... I understand the burden is upon me to determine whether information or materials within my control are considered by the NSA to be protected information, and whether the person(s) to whom disclosure is to be made is/are authorized to receive it.

In the agreement, Drake also acknowledged that the unauthorized disclosure of

"protected information" may constitute a violation of one or more of the following statutes – Sections 793, 794, 798, or 952 of Title 18, United States Code, and sections 421 through 426 and 783(b) of Title 50, United States Code.

35. The security agreement also contained a provision regarding the return of "protected information," underscoring its contraband nature if it is maintained in an uncleared space such as a person's home, personal computer, and/or unsecured personal email account:

> I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that upon demand by an authorized representative of the NSA or upon the conclusion of my authorized access to Protected Information, I shall return all material concerning such Protected Information in my possession, or for which I am responsible because of such access. I understand that failure to return such items may be a violation of Section 793 of Title 18, United States Code, and may constitute a crime for which I may be prosecuted.

3. The Unauthorized Disclosure Of Classified NSA Information To A Member Of The Media

36. On 2006, an article was published in , titled by which over the During an interview of a former high-ranking FBI official in connection with this investigation, that official stated that before publication of the 2006 story, contacted her and asked for information about specifically identifying it by the initials of the covername for Although the article itself did not contain classified information, the questions asked the FBI official and the information set forth below strongly suggest that

source or sources for story related classified information to

37. In that regard, Binney explained to the FBI that shortly before publication of the 2006 article, Roark called Binney from her home in Oregon and told him she was talking to and that was working on an article about . According to Binney, Roark further explained that the article was going to highlight assertion that was cheaper than and had features that did not have – issues that Roark previously had raised with HPSCI members and General Hayden. Roark also asked Binney if he would talk to but he declined.

38. Binney has further advised the FBI that during the same conversation, Roark asked him if the he had done on the program occurred in and Binney confirmed that it had. Roark concluded the conversation by asking Binney to email her the thirteen-page summary of that she, Binney, Loomis, Wiebe, and Drake had created in 2002 and which contained details about the architecture of According to Binney, he still had the document on his computer and emailed it from Binney3@verizon.net, his personal email address on his home computer, to Roark's personal email address on her home computer, with copies to Loomis and Wiebe at their personal email addresses on their home computers. On July 26, 2007, during the court-authorized search of his residence, Binney also advised the FBI that before the summary was sent to Roark in May 2006, he, Roark, and Wiebe exchanged additional email communications, using their respective personal email accounts, about Roark's request and the summary.

12/7/07

39. When asked about the 2006 article by the FBI, Binney admitted that his answer to Roark's question about in appeared in the article. Likewise, he admitted that the article's discussion of seems to be directly lifted from the thirteen-page summary he provided to Roark. I believe that this suggests, at a minimum, that Roark read portions of the summary to Moreover, she may have provided the entire document to by hand, fax or email. According to Binney, before he sent the summary to Roark, she asked if he and Loomis would review the document to confirm it was unclassified. Binney then confirmed that he and Loomis believed it was unclassified. While this facially suggests that Roark was sensitive to classification issues, it is worth noting that she, Binney and Loomis were no longer employed by the federal government, were not classification authorities, were fully aware of the appropriate procedure for seeking classification determinations, and never sought review of the document by the NSA before transmitting it through unsecure channels and sharing it with an uncleared member of the media.

40. As noted previously, Drake appears to share Roark's views regarding the differences between In that regard, on November 21, 2005, Drake sent an email to the Director of NSA, General Keith Alexander, in which he outlined his views on the injustices that had occurred regarding and how easy it would be to put back into action. Drake pleaded for "top cover" and admitted he was going outside of his management chain in writing the email. General Alexander replied to Drake's email saying that was tested and

found "wanting." After this communication, Drake was reassigned to the NDU, a transfer that he has told others he believes was punishment for his criticism of

41. In addition to the foregoing, evidence adduced during the investigation suggests that Drake has encouraged Roark to disseminate her views regarding classified programs to members of the media without clearing her submissions through classification review channels. In that regard, on August 22, 2006, Drake was involved with Roark, Binney, Wiebe, and Loomis in an email exchange, a copy of which was obtained and reviewed pursuant to the July 26, 2007 searches, on whether Roark needed to meet her duty to submit a draft op ed to the pre-publication boards at CIA and NSA for a classification review. Drake's response to Roark was "you really want to get tied up in the whole review process?! Potentially could take months!" Drake then added that NSA could block it out of spite, and said "... there are 'other' ways of getting this truth out if CIA/NSA balk." In another exchange with Roark, Drake wrote, "Diane, Are you absolutely bound to have this go through formal CIA or even NSA review, PRIOR to publication in the ? If so, who says you HAVE to?" (emphasis in original). Notably, NSA has conducted a classification review of the Roark draft op ed emailed to Drake, Binney, Wiebe, and Loomis, and determined it to be classified at the level.

42. Evidence also indicates that there is probable cause to believe that Drake himself is in regular contact with and is sharing classified and/or sensitive NSA information with During an investigative interview of a former high ranking intelligence community official who was contacted by the official stated that had generally described NSA source to the official, noting that "he" was an

W.S. J.L. 12/17/07

"insider" who had access to Director's Messages and Agency-All notifications, which are sent via internal NSA email to those with access to NSA computer systems. Drake fits this description. Additionally, during another investigative interview of a second former high-ranking intelligence community official who had been contacted by , the second official stated that showed him/her NSA documents that appeared as if classified portion markings, which typically are noted as headers and footers on classified documents, had been cut off, scanned, and then emailed.

43. Although Drake does not have remote access to NSA computer systems from his offices at NDU, between at least April and June 2007, he returned to NSA to access computer systems and review messages, the substance of which were reported by in various media stories. For example, on 2007, the Director of NSA sent a Director's Message concerning that was released to NSA employees via internal email. The investigation has determined that on that day, Drake was logged on to TOP SECRET and UNCLASSIFIED computer systems, viewed the Director's message, and printed off an untitled two-page word document, as well as thirteen emails. Given these facts and circumstances, there is probable cause to believe that Drake cut and pasted portions of other titled documents, which may be classified, into an unclassified document he either created or received. Moreover, in my experience, the removal of header and footer classification markings, or otherwise obscuring the classification of a document, is a classic indicia of mishandling classified information and/or espionage.

44. It also has been determined that the next day, 2007, Drake viewed and printed an internal NSA document concerning

and four-minutes later printed the NSA Security Policy regarding unauthorized disclosures to the media. On 2007, printed another article, written by Similarly, on 2007, printed another article, written by The article reflects that it was based on NSA information from a brief This article was subsequently reviewed and by NSA. The investigation also has determined that only individuals accessed, via internal NSA internet, all documents that used to write article, and Drake was one of the

45. On 2007, published a story on the web site that is the publisher of The investigation has determined that only individuals accessed, via internal NSA internet, the internal documents used by to publish story, and Drake was one of those individuals. Additionally, Drake was the only individual who accessed both the documents and the documents used for the blog by

46. The investigation has further determined that Drake continues to use his personal email account, tadrake@earthlink.net, to engage in email exchanges about NSA-related programs with Binney, Wiebe, Roark, and Loomis. In fact, on June 27, 2007, Drake emailed Binney, Wiebe, Roark, Loomis, and another former NSA employee and disclosed that the name of an existing NSA program had been changed. That email also

was obtained and reviewed pursuant to the aforementioned searches.

47. More recently, since the July 26, 2007 searches, Drake has been observed engaging in additional suspicious behavior when he visits NSA. For example, on August 3 and August 13, 2007, Drake logged on to NSA classified and unclassified computer systems and printed several emails and documents. Thereafter, on September 10, 2007, after logging onto a classified computer system, he was again observed printing several documents from his NSA computer, although the investigation has determined that these documents were not classified. Drake was then seen rolling up the documents, walking out of the NSA office space to his car, and placing the documents in the glove box of his vehicle, where they would not be visible to others.

VI. PREMISES TO BE SEARCHED AND ITEMS TO BE SEIZED

48. Computers and related electronic media, along with hardcopies of emails and other printed materials, were seized from the locations searched on July 26, 2007. The investigation has since determined that Drake's contact information was located in the email address books of Roark and Wiebe. Printed emails from Drake were also recovered at the respective homes of Binney, Wiebe, Loomis, and Roark during the aforementioned searches. Furthermore, the searches establish that Drake was on the "cc" line of a May 2002 email sent from one of Binney's unsecure personal email accounts to unsecure personal email accounts used by Wiebe and Loomis. Drake was copied at the email address tadrake@earthlink.net. That message disseminated the classified collaboration paper, although Drake is not authorized to retain, disseminate, or discuss classified information at his home or via his personal email.

49. Drake has also had numerous email contacts with Roark, Binney, Wiebe and Loomis, which have involved reviewing documents for their business, and Drake has also hosted private companies with Roark, Binney, Wiebe and Loomis, in an effort to market technology to the private sector. As noted above, Binney, Roark, Wiebe and Loomis conduct business out of their respective homes, and emails concerning the technology were recovered either in hardcopy format from some of the search locations, or in electronic format from several personal computers seized during the searches. Moreover, although Drake has an office where he conducts NSA business, items recovered from the recent searches reflect that Drake also helps Roark, Binney, Wiebe, and Loomis with their business using unofficial email addresses and computers, including Drake's personal email address, tadrake@earthlink.net, which relevant email provider log-in records reflect was accessed from Drake's home until approximately July 6, 2007, shortly after investigators spoke to Binney on June 28, 2007 about the investigation.

50. In addition to the foregoing, Drake has been observed carrying a lap top computer bag to and from his NDU work office and home. The investigation has also confirmed that NDU issued Drake a lap top computer, and his NDU office space has a docking station for his lap top computer when he is at the office. NDU security officials have advised that on one very recent occasion when Drake was not at work Drake's lap top computer was observed in his office in a docking station on his work desk. The lap top docking station provides internet access by cable modem.

51. Through grand jury subpoenas issued to EarthLink, as well as discussions with EarthLink representatives, Drake's account activity for the personal email account

"tadrake@earthlink.net" was obtained and reviewed for the period Monday, October 22, 2007, through Friday, November 2, 2007. According to the EarthLink representative and the documents obtained, Drake has not logged on from his home EarthLink dial-up service since early July of this year, approximately a few weeks before the above-described search warrants were executed. However, it appears that Drake has nonetheless continued to check his EarthLink emails from work, using the laptop computer he brings to NDU from home. This is confirmed by Drake's EarthLink account login records for the following recent, representative time periods:

Date	Drake EarthLink Email Account Login Times
Monday, October 22, 2007	11:41 am, 3:32 pm
Tuesday, October 23, 2007	no logins (Drake was scheduled to teach a class from 1:30pm – 3:25 pm)
Wednesday, October 24, 2007	1:26 pm, 3:58 pm (Drake scheduled to teach class from 1:30 pm – 3:25 pm)
Thursday, October 25, 2007	no logins
Friday, October 26, 2007	11:44 am, 4:07 pm, 10:57 pm
Saturday, October 27, 2007	no logins
Sunday, October 28, 2007	no logins
Monday, October 29, 2007	12:44 pm, 12:55 pm, 1:18 pm
Tuesday, October 30, 2007	1:34 pm, 1:40 pm, 2:10 pm (Drake was scheduled to teach a class from 3:35 pm – 5:30 pm)
Wednesday, October 31, 2007	no logins (Drake was scheduled to teach a class from 3:35 pm – 5:35 pm)

Date	Drake EarthLink Email Account Login Times
Thursday, November 1, 2007	7:47 am, 7:52 am, 8:03 am, 8:17 am, 8:34 am, 3:31 pm, 3:36 pm
Friday, November 2, 2007	7:40 am, 7:45 am, 7:52 am, 8:25 am, 8:30 am, 8:39 am, 8:52 am, 9:02 pm

As these representative log-in records suggest, during the work week, Drake may be routinely and frequently checking his EarthLink email from his NDU office space, using the internet access NDU provides there, except when he is either away from the office, or engaged in teaching responsibilities.

52. Given these things, I submit that there is probable cause to believe that a document, classified drafts of the document, and/or classified information contained in or relating to the document, were and may continue to exist and be located in the personal email account used by Drake. Accordingly, based upon my experience and the information obtained to date during this investigation, I believe there is probable cause to believe that email servers or premises associated with Drake's personal email account, tadrake@earthlink.net, will contain evidence establishing his unauthorized disclosure of classified documents or materials, in violation of one or more of the aforementioned statutes.

53. More specifically, based upon my experience, my discussions with other law enforcement officers, and my familiarity with the practices and methods of persons committing violations of the aforementioned statutes by communicating through email, I believe there is probable cause to believe that the email servers or premises will contain:

a. Stored email and other stored content information presently contained in, or on behalf of, the following email account: tadrake@earthlink.net.

12/7/07

b. Printouts from original storage of all of the email described above in subparagraph a.

c. Transactional information of all activity of the email addresses and/or individual account described above in subparagraph a, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.

d. Business records and subscriber information, in any form kept, pertaining to the email address described above in subparagraph a, including applications, the subscriber's full name, all screen names associated with the subscriber and/or account, all account names associated the subscriber, methods of payments, telephone numbers, addresses, and detailed billing records, if applicable.

e. Records indicating the services available to the subscriber of the email address and/or individual account described above in paragraph a.

VII. SEARCH PROCEDURES

54. In order to ensure that agents search only the computer email account or premises described in Attachment A, this affidavit and application for search warrant seek authorization to permit employees of the Service Provider to assist agents in the execution of this warrant. The search warrant will be faxed to the Service Provider's personnel who will be directed to produce those email accounts and files.

VIII. CONCLUSION

55. Based upon the evidence set forth herein, which I believe to be truthful and reliable, as well as my investigative experience, I believe that probable cause exists to believe that Thomas Andrews Drake has engaged in the unauthorized disclosure of classified documents or materials to other persons not authorized to receive it, including

at least one member of the media, in violation of Title 18, United States Code, Sections 793 (Unlawful Disclosure of Classified National Defense Information), 798 (Unlawful Disclosure of Classified Information), and 371 (Conspiracy To Commit An Offense Against The United States). I further believe that a search of the above-described email account or premises will result in the seizure of items listed in Attachment B that may constitute the evidence, instrumentalities, or fruits of these offenses.

Jason W. Lawless, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on this 17th day of December, 2007

The Hon. William Connolly
United States Magistrate Judge
District of Maryland

Attachment A

Property to be Searched at EarthLink, Inc.

1. All stored electronic mail ("email") and other stored content information presently contained in, or on behalf of, the following email address or account:

   tadrake@earthlink.net

2. All existing printouts from original storage of all of the email described in Paragraph 1.

3. All transactional information of all activity of the email described in Paragraph 1, including log files, dates, times, methods of connection, ports, dial-ups, and/or locations.

4. All business records and subscriber information, in any form kept, pertaining to the email address described in Paragraph 1, including applications, the subscriber's full names, all screen names associated with the subscriber and/or account, all account names associated with the subscriber, methods of payment, telephone numbers, addresses, and detailed billing records.

5. All records indicating the services available to the subscriber of the email address described in Paragraph 1.

Attachment B

Items to be Seized

Any items which constitute evidence, instrumentalities, or fruits of violation of Title 18, United States Code (U.S.C.), Sections 371 (Conspiracy To Commit An Offense Against The United States), 793 (Unlawful Disclosure of Classified National Defense Information), and 798 (Unlawful Disclosure of Classified Information), including specifically:

1. U.S. government documents, classified documents (including classified documents missing headers and footers), national defense intelligence documents and papers, and other documents relating to the National Security Agency (NSA), the program, the Terrorist Surveillance Program or other classified U.S. Government programs.

2. Papers or documents relating to the transmittal by electronic mail of U.S. government documents, national defense and classified intelligence to representatives of the news media, or individuals not authorized to receive the information;

3. Any electronic mail communications which reflect or relate to any communications or contacts of any kind with or any other reporter, journalist, employee or representative of