

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

# THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

All redacted information  
exempt under b(1) and/  
or b(3) except where  
otherwise noted.

~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

UNITED STATES

AM 9:44

FOREIGN INTELLIGENCE SURVEILLANCE COURT

CLERK OF COURT

WASHINGTON, D.C.

Docket Number: PR/TT

APPLICATION FOR USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES  
FOR FOREIGN INTELLIGENCE PURPOSES

The United States of America, through the undersigned  
designee of the U.S. Government, hereby applies to this Court,  
pursuant to the Foreign Intelligence Surveillance Act of 1978  
(FISA or the Act), Title 50, United States Code (U.S.C.), §§  
1801-1811, 1841-1846, as amended, for renewed authority to  
install and use pen registers and trap and trace devices for  
investigations to protect against the international terrorism  
activities of the foreign powers listed and described in the  
Declaration of Michael E. Leiter, Director, National

~~TOP SECRET//COMINT//NOFORN~~

Classified by: Matthew G. Olsen, Acting Assistant  
Attorney General, NSD, DOJ

Reason: 1.4(c)

Declassify on: [REDACTED]



~~TOP SECRET//COMINT//NOFORN~~

Counterterrorism Center (NCTC) ("NCTC Declaration"), which has been filed with the Court at docket number [REDACTED] and is incorporated herein by reference, specifically [REDACTED]  
[REDACTED]

<sup>1</sup> For purposes of this Application, [REDACTED]  
[REDACTED]

~~TOP SECRET//COMINT//NOFORN~~



[REDACTED] (collectively, "Foreign Powers"), [REDACTED]  
[REDACTED] which are being conducted by the Federal Bureau of Investigation (FBI) under guidelines the Attorney General has approved pursuant to Executive Order 12333, as amended. (S)

This Application differs from the application that the Court approved in docket number PR/TT [REDACTED]. First, this application sets forth, in paragraph 6.H below, additional oversight mechanisms the Government will implement to ensure compliance with any order issued by the Court in this matter. Attached as Exhibit C is a memorandum detailing a meeting between NSA and the National Security Division (NSD). Second,

---

<sup>2</sup> For purposes of this Application, [REDACTED]

[REDACTED]



~~TOP SECRET//COMINT//NOFORN~~

the "Chief, Special Foreign Intelligence Surveillance Act Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, National Security Agency" has replaced as an approving official the "Signals Intelligence Directorate Deputy Program Manager for Counterterrorism Special Projects Analysis and Production" described in previous applications. Third, references to an "archive" have been deleted or replaced as appropriate. Fourth, to make clear that NSA technical personnel may access the data to perform processes to make the data usable by analysts, the Government had added footnote 11 to this Application and footnote 5 to the proposed Primary Order.

~~(TS//SI//NF)~~

The objective of the surveillance authority requested in this Application is to enable the NSA to uncover the communications and locations of the Foreign Powers and unknown persons in the United States and abroad affiliated with the Foreign Powers, and to disseminate such information to the FBI and other elements of the United States Intelligence Community as appropriate. The authority requested in this Application will allow [REDACTED] "metadata"<sup>3</sup> regarding certain

---

<sup>3</sup> "Metadata," as used in this Application, is the information appearing on the "to," "from," "cc," and "bcc" lines of a standard e-mail [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

electronic mail (e-mail) communications from [REDACTED]  
and then to place such information in a repository against which  
"queries" may be run to identify operatives of the Foreign  
Powers by looking for contacts with other individuals who are  
reasonably suspected to be operatives of one or more of the  
Foreign Powers and to reveal communications links between such  
operatives. (~~TS//SI//NF~~)

Specifically, the metadata will be stored in an NSA data  
repository, and the NSA will query the metadata using known e-  
mail [REDACTED] that meet a particular standard. The  
standard is that other investigation and analysis have revealed  
that, based on the factual and practical considerations of  
everyday life on which reasonable and prudent persons act, there

[REDACTED]

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

are facts giving rise to a reasonable, articulable suspicion that the e-mail [REDACTED] is associated with one or more of the Foreign Powers; provided, however, that an [REDACTED] [REDACTED] believed to be used by a U.S. person shall not be regarded as associated with a Foreign Power solely on the basis of activities that are protected by the First Amendment to the Constitution. The resulting analytical product from the queries made will be "leads" for the FBI and other elements of the United States Intelligence Community to follow to find suspected terrorists affiliated with the Foreign Powers, disrupt their activities, and prevent future terrorist attacks on the United States. (~~TS//SI//NF~~)

If authorized, of necessity this surveillance will collect metadata pertaining to [REDACTED] electronic communications, including metadata pertaining to communications of United States persons located within the United States who are not the subject of any FBI investigation.<sup>4</sup> The NSA has determined that such

[REDACTED]

4 [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

broad collection of information is necessary to develop a data repository that will enable the analysis the NSA needs to perform to find known operatives of the Foreign Powers and to identify unknown persons affiliated with the Foreign Powers, some of whom may communicate with United States persons, and many of whose communications transit the U.S. Internet infrastructure. (~~TS//SI//NF~~)

In support of this Application, the United States states as follows:

1. The Application. The federal officer seeking to use the pen registers and trap and trace devices covered by this Application is [REDACTED] Chief, Special Foreign Intelligence Surveillance Act (FISA) Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate (SID), NSA. Among other things, the NSA is responsible for collecting signals intelligence with respect to the activities of international terrorist groups and their agents, and disseminating intelligence product regarding such matters to the

---

[REDACTED]

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

United States Intelligence Community, including the FBI.

~~(S//SI//NF)~~.

Set forth below is the certification of Matthew G. Olsen, Acting Assistant Attorney General, National Security Division, United States Department of Justice, that the information likely to be obtained from this pen register and trap and trace surveillance is relevant to ongoing investigations to protect against international terrorism that are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution. (U)

The Act authorizes the Attorney General to approve applications for pen registers and trap and trace devices. The Attorney General's approval of this Application and finding that it satisfies the criteria and requirements for such applications is set forth below. (U)

2. Supporting documentation. This Application is supported by: (i) the Declaration of [REDACTED] Declaration"), attached as Exhibit A, describing the objective of the surveillance authority requested in this Application, the metadata sought, how the NSA will handle that metadata, and the [REDACTED] from which the metadata will be acquired; (ii) the NCTC Declaration, which has been filed with the Court at docket number [REDACTED] and is incorporated herein by reference, which

~~TOP SECRET//COMINT//NOFORN~~



describes the continued threat of terrorist attack faced by the United States from the Foreign Powers that could result in mass casualties, massive property loss, and disruption of the continuity of government; (iii) the report required by the Court's Order in docket number PR/TT [REDACTED] at pages 12-13, attached as Exhibit B; and (iv) the memorandum detailing a meeting between NSA and the NSD, attached as Exhibit C.<sup>5</sup>

~~(TS//SI//NF)~~

3. Predicated investigations. The Foreign Powers, and unknown persons in the United States and abroad who are affiliated with the Foreign Powers, are the subjects of numerous FBI predicated investigations being conducted under guidelines

<sup>5</sup> In its [REDACTED] filing in docket number PR/TT [REDACTED] the Government stated that:

[a]t least once before any future orders renewing the authorization granted in docket number PR/TT [REDACTED] expire, a meeting for the purpose of assessing compliance with this Court's orders will be held with representatives from NSD, NSA's OGC, and appropriate individuals from NSA's Signals Intelligence Directorate. The results of this meeting will be reduced to writing and submitted to the Court as part of any application to renew or reinstate this authority[.]

Mem. of the United States in Response to the Court's Order Dated [REDACTED] Docket Number PR/TT [REDACTED] at 7. NSA and NSD met on [REDACTED] to discuss a framework for these meetings and reports to the Court going forward. The results of the meeting are attached as Exhibit C. As set forth below, future applications for renewed authority will be accompanied by a similar exhibit.. ~~(TS//SI//NF)~~



approved by the Attorney General pursuant to Executive Order 12333, as amended. As of December 2008, the FBI had approximately [REDACTED] open predicated investigations targeting the Foreign Powers and leaders and agents of the Foreign Powers. Those investigations are being conducted on the basis of activities of the Foreign Powers and unknown persons in the United States and abroad affiliated with the Foreign Powers, and to the extent these subjects of investigation are United States persons, not solely on the basis of activities that are protected by the First Amendment to the Constitution. Additional facts regarding the threat to the United States posed by the Foreign Powers are set forth in the NCTC Declaration.

(S)

4. Previous applications. This is the [REDACTED] application to the Court targeting [REDACTED]  
[REDACTED]  
[REDACTED] at the facilities described as [REDACTED]  
[REDACTED]; the [REDACTED] application with respect to [REDACTED]; the [REDACTED] application with respect to [REDACTED] and the [REDACTED] application with respect to [REDACTED].<sup>6</sup>

<sup>6</sup> The Court's [REDACTED] Order extended authorization [REDACTED]  
[REDACTED]  
[REDACTED] The Court's [REDACTED] Order extended authorization [REDACTED]



The most recent prior application was in docket number

PR/TT [REDACTED] <sup>7</sup> ~~(S//SI)~~

5. Authority sought. The United States respectfully requests that the Court authorize the NSA to use pen registers and trap and trace devices to collect foreign intelligence information at the [REDACTED] described in detail in Tab 1 to the [REDACTED] Declaration (collectively, [REDACTED], which is incorporated herein by reference. ~~(TS//SI//NF)~~

This request is for pen register and trap and trace authority within the United States. All of the collection activity described above will occur in the United States, and will collect metadata from electronic communications that are: (1) between the United States and abroad; (2) between overseas locations; and (3) wholly within the United States. ~~(S)~~

With respect to the requested electronic communications surveillance authority, the applicant seeks Court orders authorizing the installation and use of pen registers and trap

[REDACTED]

~~(TS//SI//NF)~~

<sup>7</sup> The Court's [REDACTED] Order, Section 5(g), at pages 12-13, requires NSA to submit reports to the Court discussing queries that have been made against the data, as well as any changes in the description of the [REDACTED] described in the Order. Exhibit B, attached hereto, is NSA's third report in response to the above-stated requirement in that Order. ~~(S//SI)~~



and trace devices to collect all addressing and routing information reasonably likely to identify the sources or destinations of the electronic communications on the [REDACTED] including the "to," "from," "cc," and "bcc" fields for those communications [REDACTED]

[REDACTED]

As noted above, such addressing and routing information is referred to herein as "metadata." For the convenience of the Court, a fictitious example of e-mail metadata is set forth below:

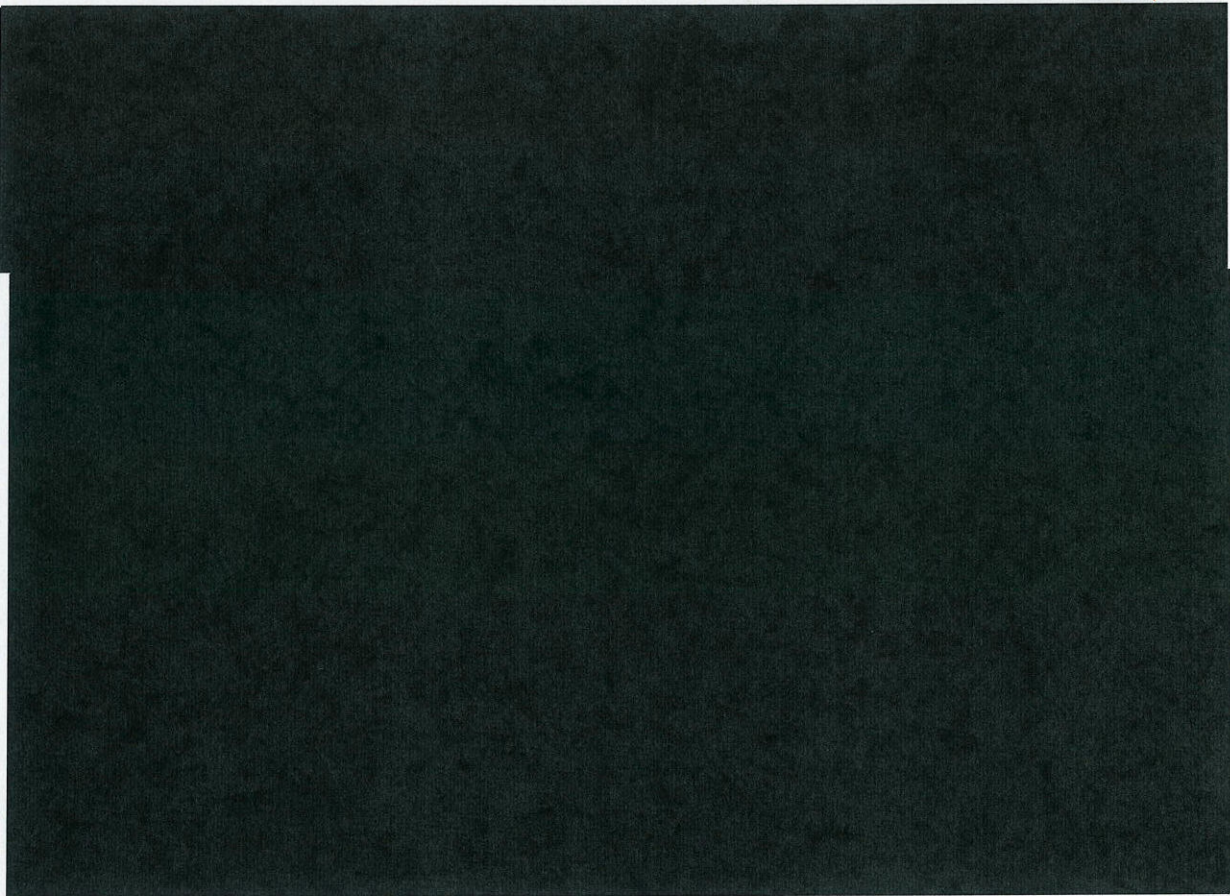
[REDACTED]



Data below the "bcc" line, including the subject line and the content of the message, are not metadata and will not be collected pursuant to the surveillance authority requested herein. ~~(S)~~

6. Additional description of surveillance methods. If this Application is approved, the NSA will employ the pen register and trap and trace surveillance authority sought herein as described below. ~~(S)~~

A. Collection of the metadata. The same technology will be used to extract the metadata from each of the [REDACTED]. [REDACTED]







B. Administration of the metadata repository.



The metadata will be stored and processed in secure private databases that the NSA exclusively will operate. The metadata will be stored on-line



on NSA database servers and access to the metadata will be restricted solely to individuals who are trained with regard to this authorization. The metadata will also be accessible to cleared technical personnel for the purpose of system administration. The data will not be commingled with data collected pursuant to other authorities.<sup>8</sup> Whenever the data is accessed, the user's login, IP address, date and time, and retrieval request will be logged for auditing capability.

~~(TS//SI//NF)~~

C. Procedures for making queries to the metadata. The NSA will use a software interface to limit access to the metadata to

8



As noted in the Court's Orders in this matter from docket number PR/TT [REDACTED] to docket number PR/TT [REDACTED] and as discussed in more detail in the Supplemental Declaration of [REDACTED] (attached to the Application in docket number PR/TT [REDACTED] as Exhibit C), NSA will place copies of the metadata in a database analytical tool known as [REDACTED]

[REDACTED] the metadata will be identified by a unique classification marking and access to it will be restricted by software controls to the specially-cleared NSA analysts discussed in paragraph B.

~~(TS//SI//NF)~~



specially cleared NSA analysts. The NSA currently is authorized to have [REDACTED] analysts perform queries of the metadata on a regular basis.<sup>9</sup> Docket Number PR/TT [REDACTED] Primary Order at 7. Access to the metadata will be controlled by user name and password by the cleared technical personnel. NSA's Office of General Counsel (OGC) will brief analysts concerning the authorization requested in this Application and the limited circumstances in which queries of the metadata are permitted. Queries of the metadata using contact chaining [REDACTED] [REDACTED] methods described on page 43 of the Court's July 14, 2004, Opinion and Order in docket number PR/TT [REDACTED] will be performed when they meet the following requirement: based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that a particular known [REDACTED] is associated with one or more of the Foreign Powers; provided, however, that an [REDACTED] [REDACTED] believed to be used by a U.S. person shall not be regarded as associated with a Foreign Power solely on the basis of activities that are protected by the First Amendment to the

---

<sup>9</sup> Personnel may, from time to time, be reassigned, resulting in some alterations to the list of analysts over time, but not the number of analysts authorized to perform queries of the metadata. (TS//SI//NF)



United States Constitution.<sup>10</sup> Queries must be approved by one of the following twenty-three people: the Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate (SID), NSA; the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. E-mail [REDACTED] that are the subject of Foreign Intelligence Surveillance Court (FISC) authorized electronic surveillance and/or physical search based on the FISC's finding of probable cause to believe that they are used by agents of one or more of the Foreign Powers, including those used by U.S. persons, will be deemed approved for metadata querying without approval of an NSA official due to the FISC authorization. The preceding sentence is not meant to apply to e-mail [REDACTED] under surveillance pursuant to any certification of the Director of National Intelligence and the Attorney General, pursuant to Section 105B of FISA as added by the Protect America Act of 2007, or Section 702 of FISA, as added by the FISA Amendments Act of 2008. Nor is it intended to apply to e-mail [REDACTED] under surveillance

---

<sup>10</sup> Further, all queries will be conducted in accordance with the [REDACTED] Orders of this Court (docket numbers PR/TT [REDACTED] PR/TT [REDACTED] and PR/TT [REDACTED]). (TS).



pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008. When the metadata is accessed, the user's login, IP address, date and time, and retrieval request will be logged for auditing purposes.<sup>11</sup> ~~(TS//SI//NF)~~

D. Minimization procedures. The NSA will apply the existing, Attorney General approved, guidelines in United States Signals Intelligence Directive 18 (Attachment D to the application in docket number PR/TT [REDACTED], to minimize the information reported concerning U.S. persons. Prior to disseminating any U.S. person information outside the NSA, the Chief of Information Sharing Services in the NSA's Signals Intelligence Directorate must determine that the information is related to counterterrorism information and is in fact necessary to understand the counterterrorism information or to assess its importance. ~~(TS//SI//NF)~~

Further, NSA has taken, and will continue to take, certain steps to ensure that the collection authorized by the Court has been, and continues to be, in strict compliance with the Court's Orders in this matter. Those steps are set forth in the [REDACTED]

---

<sup>11</sup> ~~(TS//SI//NF)~~ As set forth in the [REDACTED] Declaration at footnote 13, NSA technical personnel perform certain processes that are necessary for making the collected metadata usable by analysts. The restrictions on access are not meant to apply to those technical processes.



~~TOP SECRET//COMINT//NOFORN~~

Declaration and in the 30-day reports filed with the Court.

~~(TS//SI//NF)~~

E. The types of metadata that the NSA will collect pursuant to this authority. The devices will extract and collect [REDACTED] metadata:

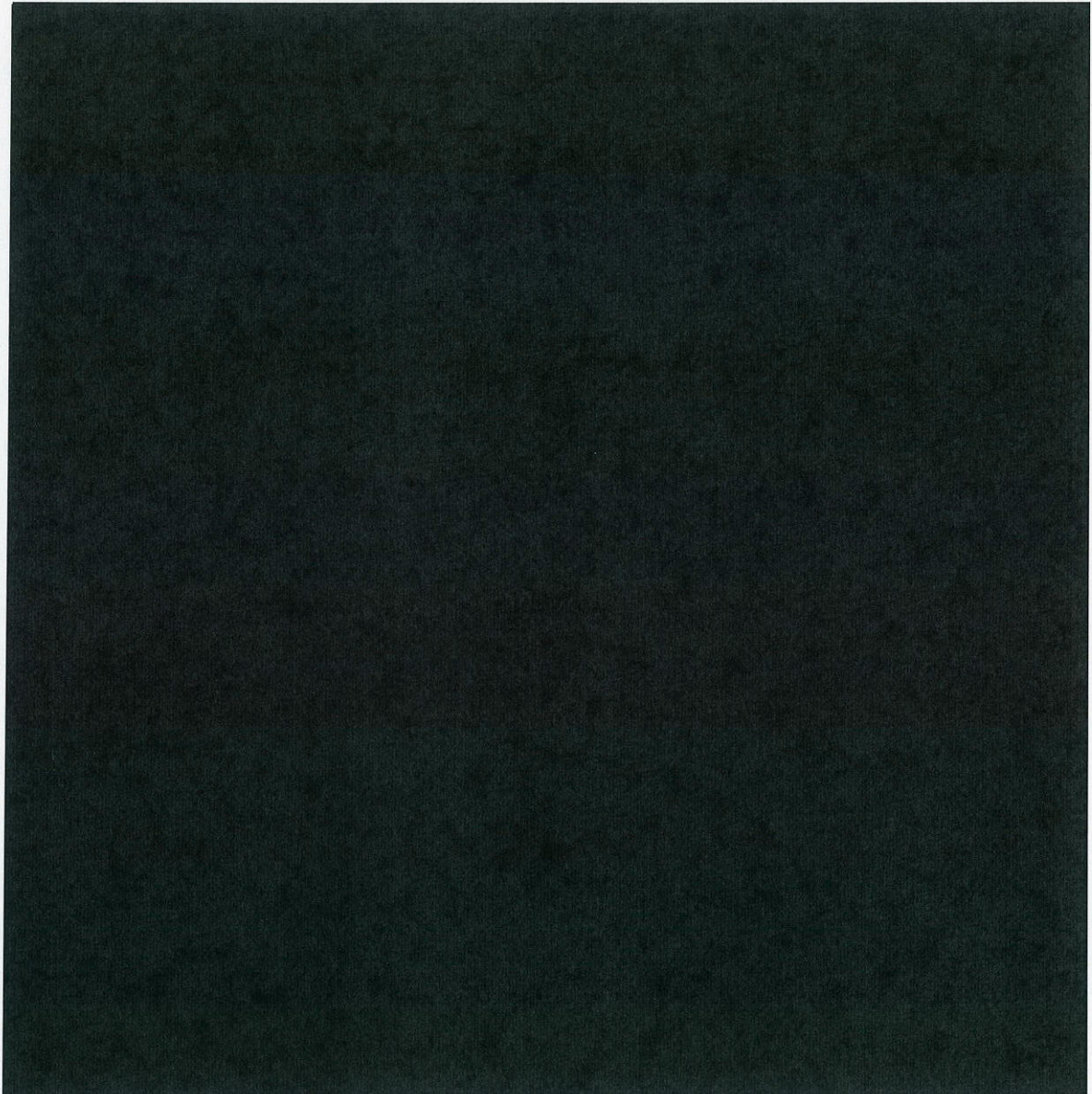
(1) For e-mail communications, the devices will extract the addresses contained in the "to," "from," "cc," and "bcc" lines. [REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//NOFORN~~





F. Maintenance of the metadata. NSA will store the metadata collected pursuant to the authority requested herein on an NSA secure private network and will keep the metadata online (that is, accessible for queries by cleared analysts) for four and one-half years (54 months). NSA will destroy the metadata



no later than four and one-half years after its initial collection.<sup>12</sup> ~~(TS//SI//NF)~~

G. Oversight. The following offices within the NSA will conduct oversight of the NSA's activities under this authority: the OGC, the Inspector General, and the Signals Intelligence Directorate Oversight and Compliance Office. NSA's OGC shall:

- i) ensure that analysts with access to such information receive appropriate training and guidance regarding the querying standard set out in paragraph C. above, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of such information;
- ii) monitor the designation of individuals with access to such information under paragraph B. above and the functioning of the automatic logging of auditing information required by paragraph C. above; and
- iii) ensure appropriate consideration of any First Amendment issues, review and approve proposed queries of metadata based on e-mail [REDACTED] used by U.S. persons. ~~(TS//SI//NF)~~

In addition, at least twice during the ninety-day authorized surveillance period, NSA's OGC will conduct random

---

<sup>12</sup> As noted in NSA's report to the Court, filed on [REDACTED] [REDACTED] NSA began destroying the first data obtained pursuant the Court's Orders on January 14, 2009. ~~(TS//SI//NF)~~



spot checks on each [REDACTED] to ensure that the collection is functioning as authorized by the Court. Such spot checks will require an examination of a sample of the metadata.

~~(TS//SI//NF)~~

H. Additional Oversight Mechanisms. As stated in its [REDACTED] filing in docket number PR/TT [REDACTED] in addition to the above minimization procedures, the Government will implement the following oversight mechanisms to ensure compliance with any order issued by the Court in this matter:

- NSA's OGC will consult with NSD on all significant legal opinions that relate to the interpretation, scope and/or implementation of the authorizations granted by the Court in this matter. When operationally practicable, such consultation shall occur in advance; otherwise NSD will be notified as soon as practicable.
- NSA's OGC will promptly provide NSD with copies of all formal briefing and/or training materials (including all revisions thereto) currently in use or prepared and used in the future to brief/train NSA personnel concerning the authorization granted by orders issued by the Court in this matter.
- At least once before the expiration of any authority granted herein, a meeting for the purpose of assessing compliance with this Court's orders will be held with representatives from NSA's OGC, NSD, and appropriate individuals from NSA's SID. The results of this meeting will be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.
- At least once before the expiration of any authority granted herein, NSD will meet with NSA's Office of Inspector General (OIG) to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders in this matter.



- Prior to implementation, all proposed automated query processes will be reviewed and approved by NSA's OGC and NSD.
- At least once every ninety days, NSA's OGC and NSD will review a sample of the justifications for querying the metadata, including e-mail [REDACTED] placed on an alert list.

~~(TS//SI//NF)~~

I. Reporting. Every thirty days during the authorized surveillance period, NSA will file with the Court a report that includes: (i) a discussion of queries made since the prior report to the Court and the NSA's application of the standard set out in paragraph 6.C. above to those queries; and (ii) any changes in the description of the [REDACTED] [REDACTED]

~~(S//SI//NF)~~

In addition, should the United States seek renewal of the authorities requested herein at that time it will file a report that includes: (i) detailed information regarding any new [REDACTED] proposed to be added to such authority; and (ii) any changes proposed in the collection methods, [REDACTED] [REDACTED] of the pen registers and/or trap and trace devices. ~~(S//SI//NF)~~

7. The Court is requested to authorize the installation and use of pen registers and trap and trace devices as described herein for a period of ninety days, and to direct that [REDACTED] [REDACTED] furnish the NSA with any information, facilities, or



~~TOP SECRET//COMINT//NOFORN~~

technical assistance necessary to accomplish the installation and operation of the pen registers and trap and trace devices, for purposes of targeting the Foreign Powers and unknown persons in the United States and abroad affiliated with one or more of the Foreign Powers in such a manner as will protect their secrecy and produce a minimum amount of interference with the services [REDACTED] are providing to their customers.

~~(S//SI//NF)~~

--- Remainder of page intentionally left blank. ---

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~


WHEREFORE, the United States submits that this Application satisfies the criteria and requirements of the Act, as amended, and therefore requests that this Court authorize the installation and use of the pen registers and trap and trace devices described herein, and enter the proposed orders that accompany this Application. (U)

Respectfully submitted,




MATTHEW G. OLSEN

Acting Assistant Attorney General  
National Security Division  
United States Department of Justice



Unit Chief  
National Security Division  
United States Department of Justice



National Security Division  
United States Department of Justice

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

VERIFICATION

I declare under penalty of perjury that the facts set forth  
in this Application are true and correct. Executed pursuant to  
Title 28, United States Code, § 1746, on

[REDACTED] (U)

[REDACTED]


Chief, FISA Oversight and Processing,  
Oversight and Compliance,  
Signals Intelligence Directorate  
National Security Agency

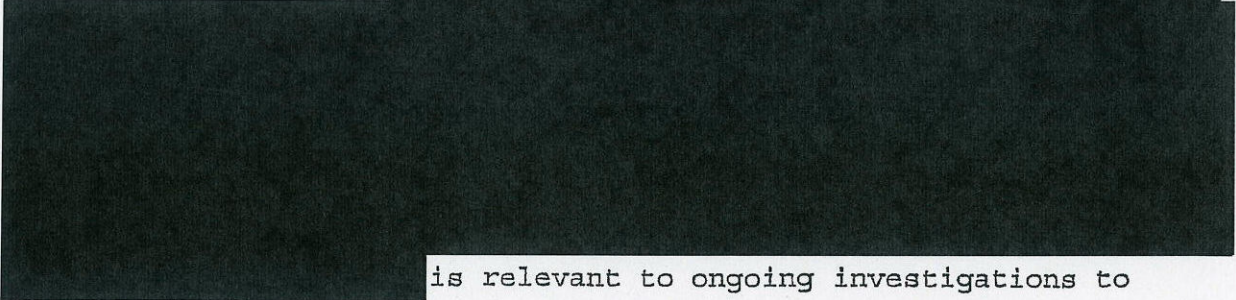
~~TOP SECRET//COMINT//NOFORN~~

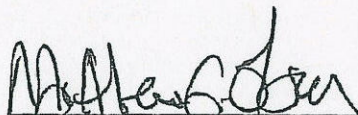


~~TOP SECRET//COMINT//NOFORN~~

CERTIFICATION

I certify that the information likely to be obtained from the pen registers and trap and trace devices requested in this Application regarding 

 is relevant to ongoing investigations to protect against international terrorism that are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution. ~~(S)~~



MATTHEW G. OLSEN


Acting Assistant Attorney General  
National Security Division  
U.S. Department of Justice


 \_\_\_\_\_  
Date

~~TOP SECRET//COMINT//NOFORN~~

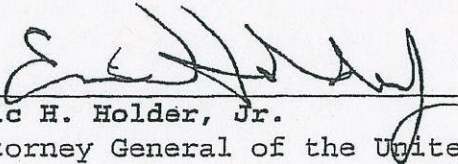


APPROVAL

I find that this Application regarding 



satisfies the criteria and requirements for such applications set forth in the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1811, 1841-1846, as amended, and hereby approve its filing with the Foreign Intelligence Surveillance Court. ~~(S)~~

  
Eric H. Holder, Jr.  
Attorney General of the United States

  
Date