



U.S. Department of Justice

National Security Division

---

Washington, D.C. 20530

EMAIL: [savage@nytimes.com](mailto:savage@nytimes.com)

NSD FOIA/PA #16-148  
September 29, 2017

Mr. Charlie Savage  
The New York Times  
1627 I Street, N.W.  
Washington, D.C. 20006

*Charlie*  
Dear Mr. Savage:

This is our final response to your Freedom of Information Act (FOIA) request dated May 10, 2016, for "previously unreleased documents from the Foreign Intelligence Surveillance Court docket for the case that resulted in Judge John Bates' October 3, 2011, and November 30, 2011, rulings, both of which were declassified and made public in August 2013 but with their docket number and case name redacted." Your request was received on May 10, 2016.

In response to your request, we conducted a search of the National Security Division Office of Intelligence (NSD/OI), and we have located responsive records. We have processed documents for today's response under the FOIA, and enclose here 12 documents with portions withheld in part pursuant to one or more of the following FOIA exemptions set forth in 5 U.S.C. 552(b):

(1) which permits the withholding of information properly classified pursuant to Executive Order No. 13526; and

(3) which permits the withholding of information specifically exempted from disclosure by statute, including but not limited to Section 102(d)(3) of the National Security Act of 1947;

(6) which permits the withholding of information when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy."; and

(7)(C) which permits the withholding of records or information compiled for law enforcement purposes the release of which could "could reasonably be expected to constitute an unwarranted invasion of personal privacy."

Additional documents responsive to the May 10, 2016 FOIA request are exempt from disclosure in their entirety pursuant to one or more of these FOIA exemptions. To describe these

documents in any more detail would disclose information that is exempt from disclosure under the FOIA.

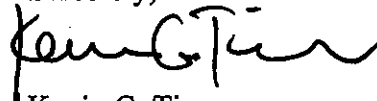
For your information, Congress excluded three discrete categories of law enforcement information and national security records from the requirements of the FOIA. See 5 U.S.C. §552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

Although this request is now the subject of litigation, we are including the following information on FOIA mediation and administrative appeals.

You may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, or at [ogis@nara.gov](mailto:ogis@nara.gov), or 202-741-5770, or toll free at 1-877-684-6448, or facsimile at 202-741-5769. Or you may contact our Public Liaison at 202-233-0756.

If you are not satisfied with this response, you may administratively appeal by writing to the Director, Office of Information Policy, U.S. Department of Justice, 1425 New York Avenue, N.W., Suite 11050, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA portal by creating an account at: <https://foiaonline.regulations.gov/foia/action/public/home>. Your appeal must be postmarked or transmitted electronically within 90 days of the date of my response to your request. If you submit an appeal by mail, both the letter and envelope should be clearly marked, "Freedom of Information Act Appeal."

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin G. Tiernan", with a stylized flourish at the end.

Kevin G. Tiernan  
Records and FOIA



~~SECRET//ORCON,NOFORN~~

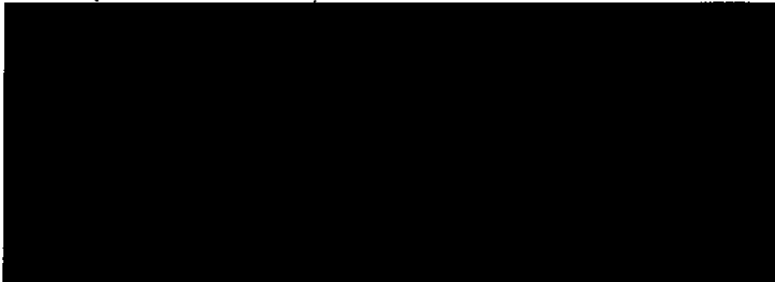
UNITED STATES

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

FOREIGN INTELLIGENCE SURVEILLANCE COURT APR 22 AM 11:03

WASHINGTON, D.C.

LEE ANN FLYNN HALL  
CLERK OF COURT



UNDER SEAL

**GOVERNMENT'S EX PARTE SUBMISSION OF REAUTHORIZATION  
CERTIFICATION AND RELATED PROCEDURES, EX PARTE SUBMISSION OF  
AMENDED CERTIFICATIONS, AND REQUEST FOR AN ORDER APPROVING  
SUCH CERTIFICATION AND AMENDED CERTIFICATIONS ~~(S)~~**

In accordance with subsection 702(g)(1)(A) of the Foreign Intelligence  
Surveillance Act of 1978, as amended ("the Act"), the United States of America, by and  
through the undersigned Department of Justice attorney, hereby submits ex parte the  
attached certification, DNI/AG 702(g) Certification [REDACTED] This certification  
reauthorizes DNI/AG 702(g) Certification [REDACTED] which expires on [REDACTED] 2011.  
Attached as Exhibits A, B, C, D, and E to DNI/AG 702(g) Certification [REDACTED] are the  
targeting and minimization procedures to be used under the certification. ~~(S//OC,NF)~~

~~SECRET//ORCON,NOFORN~~

Classified by:

~~Tashina Gauhar, Deputy Assistant Attorney  
General, NSD, DOJ~~

Reason:

~~1.4 (c)~~

Declassify on:

~~18 April 2036~~

The National Security Agency (NSA) targeting procedures and Federal Bureau of Investigation (FBI) minimization procedures attached to the certification as Exhibits A and D, respectively, previously have been submitted to and approved by this Court,

[REDACTED]

The NSA and Central Intelligence Agency (CIA) minimization procedures attached as Exhibits B and E, respectively, as well as the FBI targeting procedures attached as Exhibit C, were submitted to this Court on April 20, 2011 [REDACTED]

[REDACTED]

[REDACTED], the NSA and CIA minimization procedures, as well as the FBI targeting procedures, are similar to, but differ in certain substantive respects from, procedures previously approved by this Court. ~~(S//OC,NF)~~

In addition, the above-captioned certification also includes amendments to the certification being reauthorized, DNI/AG 702(g) Certification [REDACTED] and its predecessors, DNI/AG 702(g) Certifications [REDACTED]. Specifically, these amendments authorize the use of the NSA and CIA minimization procedures attached as Exhibits B and E, respectively, to DNI/AG 702(g) Certification [REDACTED] in connection

~~SECRET//ORCON,NOFORN~~

with foreign intelligence information acquired in accordance with DNI/AG 702(g)

Certifications [REDACTED]<sup>1</sup> (~~S//OC,NF~~)

### Conclusion (U)

DNI/AG 702(g) Certification [REDACTED] contains all of the elements required by the Act, and the targeting and minimization procedures included with the certification are consistent with the requirements of the Act and the Fourth Amendment to the Constitution of the United States. Accordingly, the Government respectfully requests, pursuant to subsection 702(k)(2) of the Act, that this Court review ex parte and in camera DNI/AG 702(g) Certification [REDACTED] and supporting documents, which are submitted herewith. The Government further requests that this Court enter an order pursuant to subsection 702(i)(3)(A) of the Act approving: DNI/AG 702(g) Certification [REDACTED] the use of the targeting and minimization procedures attached thereto as Exhibits A, B, C, D, and E in connection with acquisitions of foreign intelligence information in accordance with that certification; and the use of the minimization procedures attached as Exhibits B and E to DNI/AG 702(g) Certification [REDACTED] in

---

<sup>1</sup> The FBI minimization procedures attached to the above-captioned certification as Exhibit D are identical to the FBI minimization procedures that already have been approved for use by this Court in connection with foreign intelligence information acquired in accordance with DNI/AG 702(g) Certifications [REDACTED]. Thus, with respect to the FBI minimization procedures currently approved for use under those certifications, no amendments are necessary. (~~S//OC,NF~~)

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

connection with foreign intelligence information acquired in accordance with DNI/AG

702(g) Certifications [REDACTED] (S//OC,NF)

Respectfully submitted,

[REDACTED]

Attorney-Advisor  
National Security Division  
United States Department of Justice

~~SECRET//ORCON,NOFORN~~

~~SECRET~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED]

ORDER

This matter having come before this Court pursuant to the Government's ex parte submission of the above-referenced certification in accordance with subsection 702(g)(1)(A) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and request for an order approving such certification and the use of the targeting and minimization procedures attached thereto, and full consideration having been given to the matters set forth therein, the Court finds that the above-captioned certification submitted in accordance with 50 U.S.C. § 1881a(g) contains all the required elements, and that the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States.

~~SECRET~~

Derived From:

~~Submission to the USFISC  
in Docket Number captioned above~~

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such certification and the use of such procedures are approved.

Entered this \_\_\_\_ day of [REDACTED] 2011, at \_\_\_\_\_ Eastern Time.

---

Judge, United States Foreign  
Intelligence Surveillance Court

~~SECRET~~

~~SECRET//NOFORN~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED]

Docket No. 702(i) 08-01

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, "contains all the required elements" and that the revised National Security Agency and Central Intelligence Agency minimization procedures submitted with the amendment "are consistent with the requirements of [Section 1881a(e)] and with the fourth amendment to the Constitution of the United States."

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such amendment and the use of such procedures are approved.

Entered this \_\_\_\_ day of [REDACTED] 2011, at \_\_\_\_\_ Eastern Time.

\_\_\_\_\_  
Judge, United States Foreign  
Intelligence Surveillance Court

~~SECRET//NOFORN~~

Derived From:

~~Submission to the USFISC  
in Docket Number captioned above~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED] [REDACTED]

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, "contains all the required elements" and that the revised National Security Agency and Central Intelligence Agency minimization procedures submitted with the amendment "are consistent with the requirements of [Section 1881a(e)] and with the fourth amendment to the Constitution of the United States."

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such amendment and the use of such procedures are approved.

Entered this \_\_\_\_ day of [REDACTED] 2011, at \_\_\_\_ Eastern Time.

\_\_\_\_\_  
Judge, United States Foreign  
Intelligence Surveillance Court

~~SECRET//NOFORN~~

Derived From:

~~Submission to the USFISC  
in Docket Number captioned above~~



UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED] [REDACTED]

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, "contains all the required elements" and that the revised National Security Agency and Central Intelligence Agency minimization procedures submitted with the amendment "are consistent with the requirements of [Section 1881a(e)] and with the fourth amendment to the Constitution of the United States."

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such amendment and the use of such procedures are approved.

Entered this \_\_\_\_ day of [REDACTED] 2011, at \_\_\_\_\_ Eastern Time.

\_\_\_\_\_  
Judge, United States Foreign  
Intelligence Surveillance Court

~~SECRET//NOFORN~~

Derived From: Submission to the USFISC  
in Docket Number captioned above

~~SECRET//ORCON,NOFORN~~

U.S. FOREIGN  
INTELLIGENCE

11:03

**DNI/AG 702(g) Certification**

LEEANN FLYNN HALL  
CLERK OF COURT

In accordance with subsection 702(g) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and based on the representations made in the supporting affidavits of John C. Inglis, Acting Director of the National Security Agency (NSA), Robert S. Mueller, III, Director of the Federal Bureau of Investigation (FBI), and Leon E. Panetta, Director of the Central Intelligence Agency (CIA), in the above-referenced matter, the Director of National Intelligence and the Attorney General, being duly sworn, hereby certify that:<sup>1</sup> (S//OC,NF)

(1) there are procedures in place that have been approved<sup>2</sup> or will be submitted with this certification for approval by the Foreign Intelligence Surveillance Court<sup>3</sup> that are reasonably designed to --

- a. ensure that an acquisition authorized pursuant to subsection 702(a) of the Act is limited to targeting persons reasonably believed to be located outside the United States; and

~~(S//OC,NF)~~

<sup>2</sup> Specifically, the NSA targeting procedures attached herewith as Exhibit A were most recently approved by the Court on [REDACTED] 2010, in connection with Amendment 1 to DNI/AG 702(g) Certification [REDACTED]. (S//OC,NF)

<sup>3</sup> Specifically, the FBI targeting procedures attached herewith as Exhibit C are being submitted for approval by the Court. ~~(S//OC,NF)~~

~~SECRET//ORCON,NOFORN~~

Classified by: The Attorney General  
Reason: ~~1.4(c)~~  
Declassify on: ~~11 April 2036~~

~~SECRET//ORCON,NOFORN~~

- b. prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States;
- (2) the minimization procedures with respect to such acquisition --
  - a. meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act; and
  - b. have been approved<sup>4</sup> or will be submitted with this certification for approval by the Foreign Intelligence Surveillance Court;<sup>5</sup>
- (3) guidelines have been adopted in accordance with subsection 702(f) of the Act to ensure compliance with the limitations in subsection 702(b) of the Act and to ensure that an application for a court order is filed as required by the Act;
- (4) the procedures and guidelines referred to in sub-paragraphs (1), (2), and (3) above are consistent with the requirements of the fourth amendment to the Constitution of the United States;
- (5) a significant purpose of the acquisition is to obtain foreign intelligence information;
- (6) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
- (7) the acquisition complies with the limitations in subsection 702(b) of the Act. ~~(S)~~

On the basis of the foregoing, the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, as

<sup>4</sup> Specifically, the FBI minimization procedures attached herewith as Exhibit D were most recently submitted to the Court for approval in connection with Amendment 1 to DNI/AG 702(g) Certification [REDACTED] on [REDACTED] 2010, and were most recently approved by the Court on [REDACTED] 2010. ~~(S//OC,NF)~~

<sup>5</sup> Specifically, the NSA and CIA minimization procedures attached herewith as Exhibits B and E, respectively, are being submitted for approval by the Court. ~~(S//OC,NF)~~

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

described above, is authorized, and such authorization shall be effective on [REDACTED], 2011, or on the date upon which the Foreign Intelligence Surveillance Court issues an order concerning this certification pursuant to subsection 702(i)(3) of the Act, whichever is later. Such targeting is authorized for a period of one year from the effective date of this authorization. This authorization reauthorizes DNI/AG 702(g) Certification [REDACTED]

[REDACTED]

which became effective on [REDACTED] 2010. ~~(S//OC,NF)~~

**Amendment 4 to DNI/AG 702(g) Certification [REDACTED]  
Amendment 3 to DNI/AG 702(g) Certification [REDACTED] and  
Amendment 2 to DNI/AG 702(g) Certification [REDACTED]**

Furthermore, in accordance with subsection 702(i)(1)(C) of the Act, DNI/AG 702(g) Certifications [REDACTED] are hereby amended. Specifically, the use of the NSA and CIA minimization procedures attached herewith as Exhibits B and E, respectively, in connection with foreign intelligence information acquired in accordance with DNI/AG 702(g) Certifications [REDACTED] is authorized.<sup>7</sup> Such authorization, as amended, shall be effective on [REDACTED], 2011, or on the date upon which the FISC issues an order concerning these amendments pursuant to subsection 702(i)(3) of the Act, whichever is later. All other aspects of Certifications [REDACTED] as amended, remain unaltered and are incorporated herein. ~~(S//OC,NF)~~

<sup>6</sup> DNI/AG 702(g) Certification [REDACTED] was first amended by the Attorney General and the Director of National Intelligence in [REDACTED] 2009. This amendment related only to modifications to the FBI's targeting procedures. Amendments to DNI/AG 702(g) Certification [REDACTED] in [REDACTED] 2010 and [REDACTED] 2010, which related only to modifications to the minimization procedures for NSA, FBI, and CIA, were incorrectly specified as Amendment 1 and Amendment 2, respectively, to DNI/AG 702(g) Certification [REDACTED]. The amendments in July and August 2010 should have been specified as Amendment 2 and Amendment 3, respectively. ~~(S//OC,NF)~~

<sup>7</sup> As certified above, these minimization procedures meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act, will be submitted for approval by the FISC, and are consistent with the requirements of the Fourth Amendment to the Constitution of the United States. ~~(S//OC,NF)~~

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

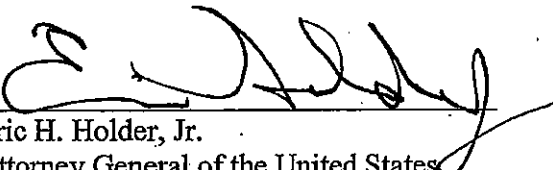
**VERIFICATION (U)**

I declare under penalty of perjury that the facts set forth in the foregoing certification in

[REDACTED]

[REDACTED] DNI/AG 702(g) Certification [REDACTED], are true and correct to the best of my knowledge and belief. I further declare under penalty of perjury that the facts set forth in the foregoing amendments to DNI/AG 702(g) Certifications [REDACTED] are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746

on April 11, 2011. (S)

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

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

VERIFICATION (U)

I declare under penalty of perjury that the facts set forth in the foregoing certification in

[REDACTED]

[REDACTED] DNI/AG 702(g) Certification [REDACTED] are true and correct to the best of my knowledge and belief. I further declare under penalty of perjury that the facts set forth in the foregoing amendments to DNI/AG 702(g) Certifications [REDACTED] are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746

on 13 April, 2011. (S)



James R. Clapper, Jr.  
Director of National Intelligence

~~SECRET//ORCON,NOFORN~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE ACT

**AFFIDAVIT OF JOHN C. INGLIS, ACTING DIRECTOR,  
NATIONAL SECURITY AGENCY**

2011 APR 22 AM 11:03

[REDACTED]

**DNI/AG 702(g) Certification** [REDACTED]

~~(S)~~ Pursuant to subsection 702(g)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and in support of DNI/AG 702(g) Certification [REDACTED] I affirm that the following is true and accurate to the best of my knowledge and belief:

1. ~~(S//NF)~~ There are reasonable procedures in place that the National Security Agency (NSA) will use to ensure that any acquisition under this certification is limited to targeting non-United States persons reasonably believed to be located outside of the United States. In addition, these targeting procedures are reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. These targeting procedures, which are attached herewith as Exhibit A, were most recently submitted for approval to the Foreign Intelligence Surveillance Court (FISC) in connection with Amendment 1 to DNI/AG 702(g) Certification [REDACTED] on [REDACTED] 2010, and were most recently approved by the FISC on [REDACTED] 2010.
2. ~~(TS//SI//NF)~~ As described below, NSA's acquisition of foreign intelligence information pursuant to this certification involves obtaining foreign intelligence information from or with the assistance of electronic communication service providers, as that term is defined in subsection 701(b)(4) of the Act.
3. ~~(TS//SI//NF)~~ NSA seeks to acquire foreign intelligence information [REDACTED]

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

[REDACTED]

4. ~~(TS//SI//NF)~~ Furthermore, NSA seeks to acquire foreign intelligence information [REDACTED]

[REDACTED]

5. ~~(TS//SI//NF)~~ Pursuant to the above-referenced certification, NSA seeks to acquire foreign intelligence information concerning [REDACTED]

~~TOP SECRET//COMINT//NOFORN//20320108~~



~~TOP SECRET//COMINT//NOFORN//20320108~~

[REDACTED]

A list [REDACTED] is attached herewith as Exhibit F. NSA believes that the non-United States persons reasonably believed to be located outside the United States who will be targeted for collection under this certification possess, are expected to receive, and/or are likely to communicate foreign intelligence information concerning [REDACTED]. Thus, a significant purpose of the acquisition is to obtain:

- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against --
  - a. actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
  - b. sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
  - c. clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to --
  - a. the national defense or the security of the United States; or
  - b. the conduct of the foreign affairs of the United States.

If NSA seeks to acquire foreign intelligence information concerning [REDACTED] NSA may target under this certification non-United States persons reasonably believed to be located outside the United States who possess, are expected to receive, and/or are likely to communicate foreign intelligence information concerning [REDACTED] provided that NSA notifies the Attorney General and Director of National Intelligence within five business days of implementing such targeting. Such notification will include a description of the factual basis for NSA's determination that the [REDACTED]

6. ~~(S//NF)~~ With respect to the information NSA acquires pursuant to the above-referenced certification, NSA will follow the minimization procedures attached herewith as Exhibit B.

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

7. ~~(S//SI//NF)~~ NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to the above-referenced certification. CIA will identify to NSA the targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with the CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.
8. ~~(S//SI)~~ NSA may provide to the Federal Bureau of Investigation (FBI) unminimized communications acquired pursuant to the above-referenced certification. The FBI will identify to NSA the targets for which NSA may provide unminimized communications to the FBI. The FBI will process any such unminimized communications received from NSA in accordance with the FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

*----- The remainder of this page intentionally left blank -----*

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

(U) I declare under penalty of perjury that the foregoing is true and correct.

Signed this 8<sup>th</sup> day of April, 2011.

  
\_\_\_\_\_  
JOHN C. INGLIS  
Acting Director  
National Security Agency

~~TOP SECRET//COMINT//NOFORN//20320108~~

**AFFIDAVIT OF ROBERT S. MUELLER, III**  
**DIRECTOR, FEDERAL BUREAU OF INVESTIGATION**

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE ACT  
2011 APR 22 AM 11:03

**DNI/AG 702(g) Certification**

(S) Pursuant to subsection 702(g)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and in support of DNI/AG 702(g) Certification [REDACTED], I affirm the following is true and accurate to the best of my knowledge and belief:

1. (S) The National Security Agency (NSA) has represented to the Federal Bureau of Investigation (FBI) that, in accordance with the NSA targeting procedures attached herewith as Exhibit A, NSA may identify certain electronic communications [REDACTED] that are used by non-United States persons reasonably believed to be outside the United States and which are reasonably believed to contain foreign intelligence information [REDACTED]
2. (S) The FBI's acquisition of [REDACTED] pursuant to NSA's request is consistent with Section 702 of the Act because, *inter alia*: the acquisition will be conducted in compliance with the limitations set forth in subsection 702(b) of the Act; the acquisition will involve obtaining foreign intelligence information [REDACTED] electronic communication service providers; and a significant purpose of the acquisition is to obtain foreign intelligence information.
3. (S) In conducting the acquisition of [REDACTED] as requested by NSA, the FBI will use the procedures attached herewith as Exhibit C to determine that the requested acquisition targets non-United States persons reasonably believed to be located outside the United States.
4. (S//NF) The FBI will convey any [REDACTED] it acquires pursuant to the above-referenced certification to NSA in unminimized form without performing any further processes or procedures to ensure that the user of the [REDACTED] is a non-United States person reasonably believed to be located outside the United States. If directed by NSA, the FBI will also convey the [REDACTED] of specified [REDACTED] from the electronic communication service provider to the Central

~~Derived From: Multiple Sources~~  
~~Declassify On: April 4, 2036~~

~~SECRET//NOFORN~~

Intelligence Agency (CIA) in unminimized form without performing any further processes or procedures to ensure that the user of the [REDACTED] is a non-United States person reasonably believed to be located outside the United States. NSA and CIA shall process any [REDACTED] received from the FBI in accordance with the NSA and CIA minimization procedures, respectively, adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

5. ~~(S)~~ The minimization procedures that the FBI will use with respect to any [REDACTED] it acquires pursuant to the above-referenced certification are attached herewith as Exhibit D. These minimization procedures were most recently submitted for approval to the Foreign Intelligence Surveillance Court (FISC) in connection with Amendment 1 to DNI/AG 702(g) Certification [REDACTED] on [REDACTED], 2010, and were most recently approved by the FISC on [REDACTED] 2010.
6. ~~(S)~~ NSA may acquire, pursuant to the above-referenced certification, unminimized communications as those communications are transmitted. Such unminimized communications may contain foreign intelligence information relating to the lawful functions and responsibilities of the FBI's counterterrorism, counterintelligence, and national security activities. Accordingly, the FBI may request and receive such unminimized communications from NSA. The FBI will identify to NSA the targeted selectors for which the FBI seeks the dissemination of unminimized communications. The minimization procedures that the FBI will use with respect to any unminimized communications it receives from NSA are attached herewith as Exhibit D.


*---- The remainder of this page intentionally left blank ----*

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

I declare under penalty of perjury that the foregoing is true and correct.

Signed this 8<sup>th</sup> day of April 2011.

  
\_\_\_\_\_  
ROBERT S. MUELLER, III  
Director, Federal Bureau of Investigation

~~SECRET//NOFORN~~

~~TOP SECRET//NOFORN~~

U.S. FEDERAL  
INTELLIGENCE  
SURVEILLANCE ACT

**AFFIDAVIT OF THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY**

2011 APR 22 AM 11:01

**DNI/AG 702(g) Certification**

CLERK OF COURT

~~(TS//NF)~~ Pursuant to subsection 702(g)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and in support of DNI/AG 702(g) Certification [REDACTED], I affirm the following is true and accurate to the best of my knowledge and belief:

1. ~~(S)~~ As Director of the Central Intelligence Agency (CIA), I am responsible for the collection of foreign intelligence through human sources and by other appropriate means. These functions are carried out by and through CIA. The mission of CIA includes the collection, production, and dissemination of foreign intelligence and counterintelligence, including information not otherwise obtainable. This includes the conduct of clandestine espionage or counterintelligence activities abroad.

2. ~~(TS//NF)~~ Pursuant to the above-referenced certification, the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) may acquire unminimized communications, [REDACTED]

3. ~~(TS//NF)~~ [REDACTED]

4. ~~(TS//NF)~~ [REDACTED]

~~TOP SECRET//NOFORN~~

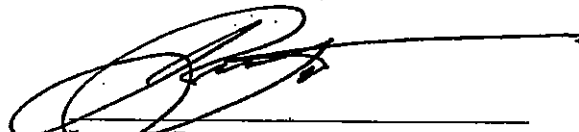
~~TOP SECRET//NOFORN~~



5. ~~(TS//NF)~~ I have reviewed the minimization procedures attached herewith as Exhibit E. CIA will follow these minimization procedures with respect to communications acquired pursuant to the above-referenced certification.

I declare under penalty of perjury that the foregoing is true and correct.

Signed this 6<sup>th</sup> day of April 2011.



\_\_\_\_\_  
Leon E. Panetta  
Director, Central Intelligence Agency

~~TOP SECRET//NOFORN~~



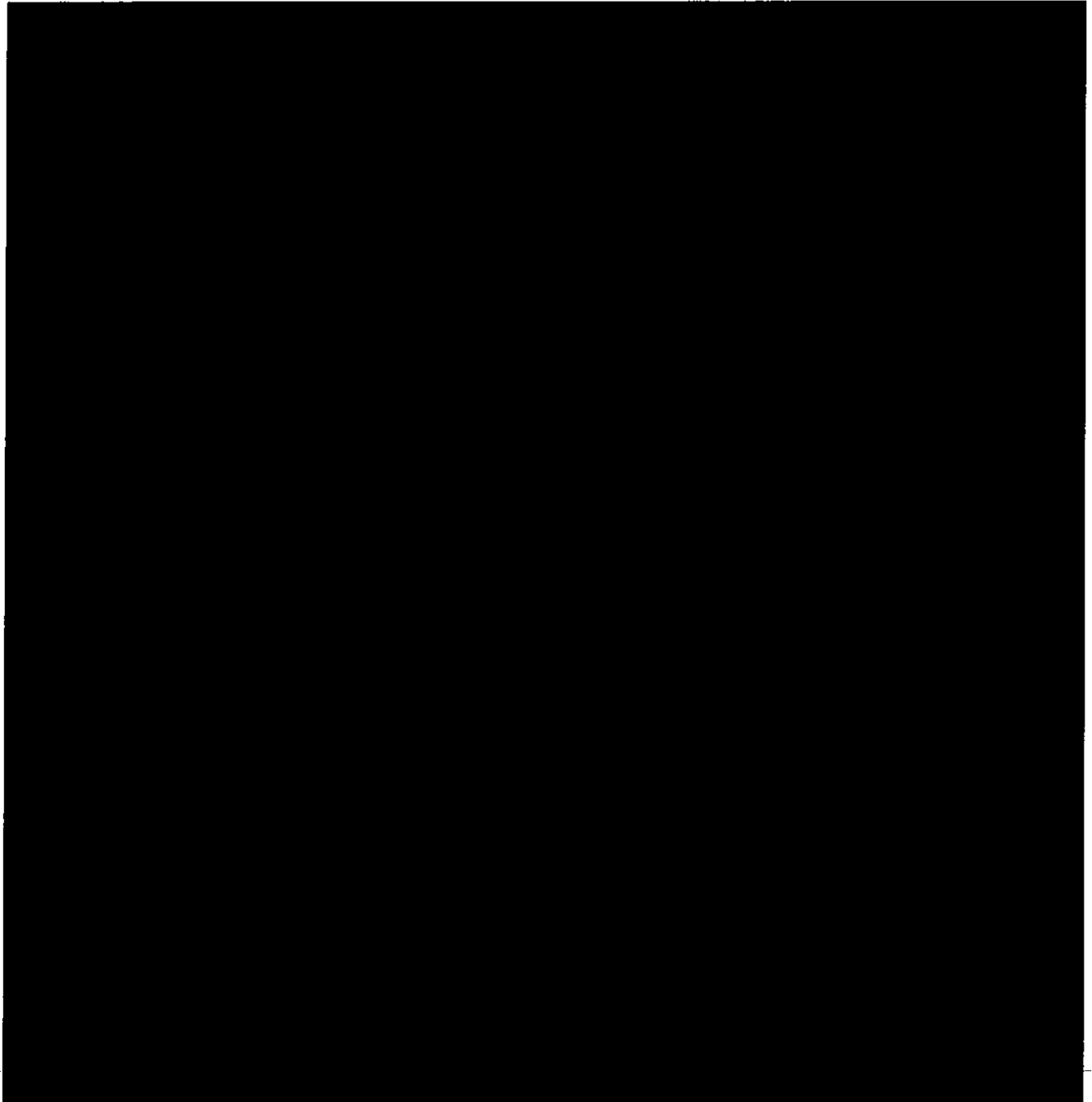
~~TOP SECRET//COMINT//NOFORN//20320108~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

EXHIBIT A

PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING  
NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED  
OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE  
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE  
SURVEILLANCE ACT OF 1978, AS AMENDED

2009 JUL 29 PM 3:14  
CLERK OF COURT



Derived From: NSA/CSSM 1-52

Dated: 20070108

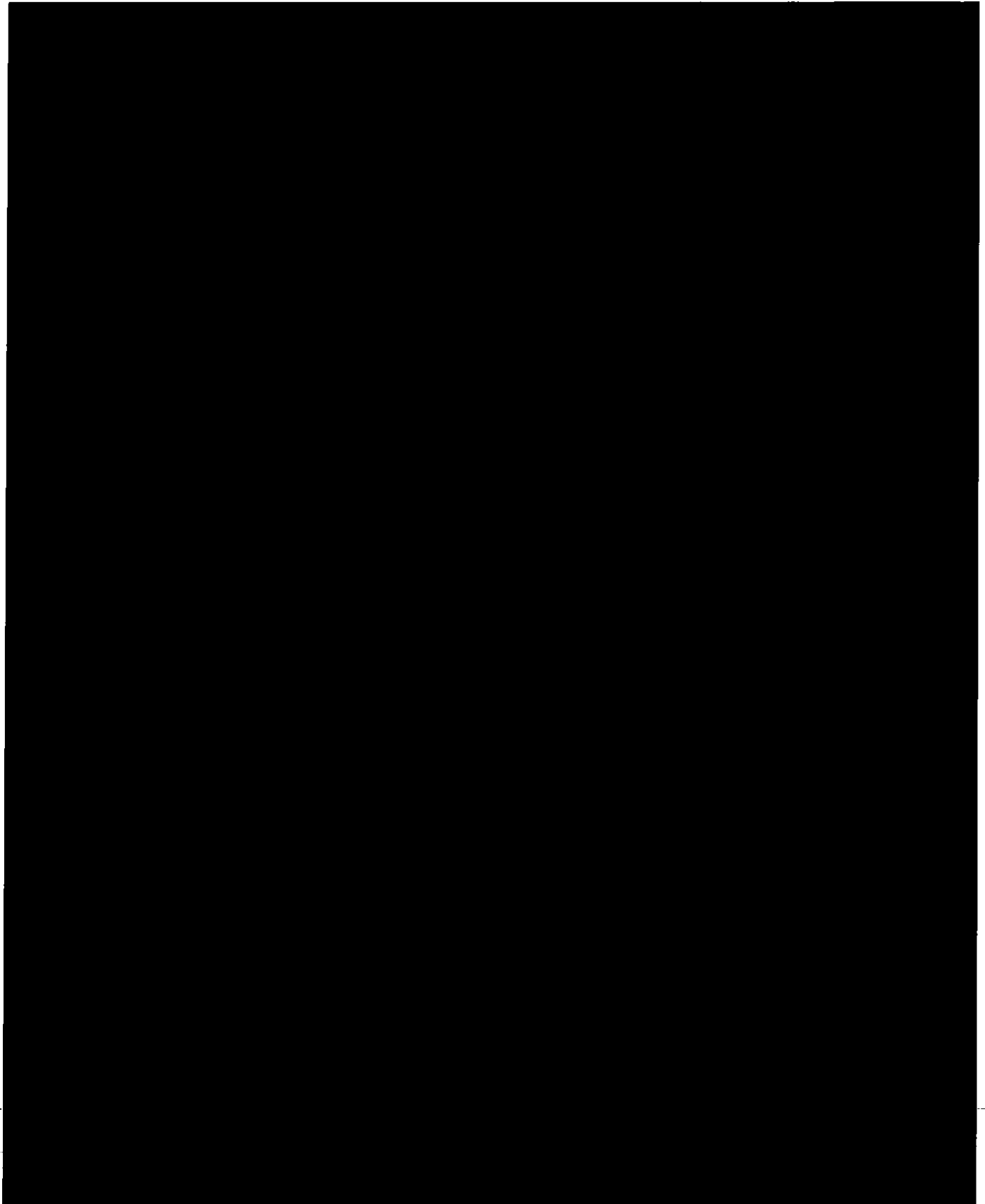
Declassify On: 20320108

~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

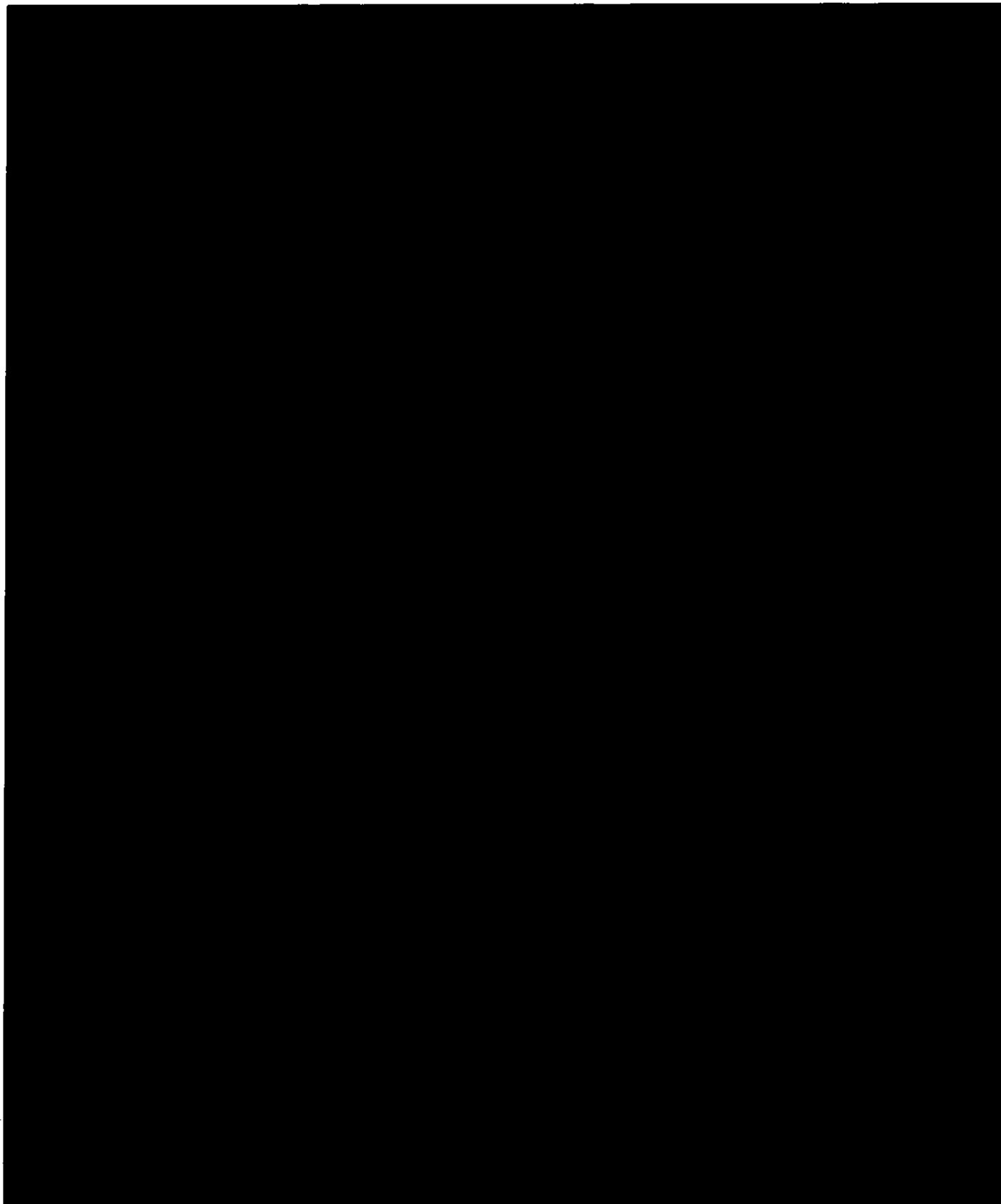


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

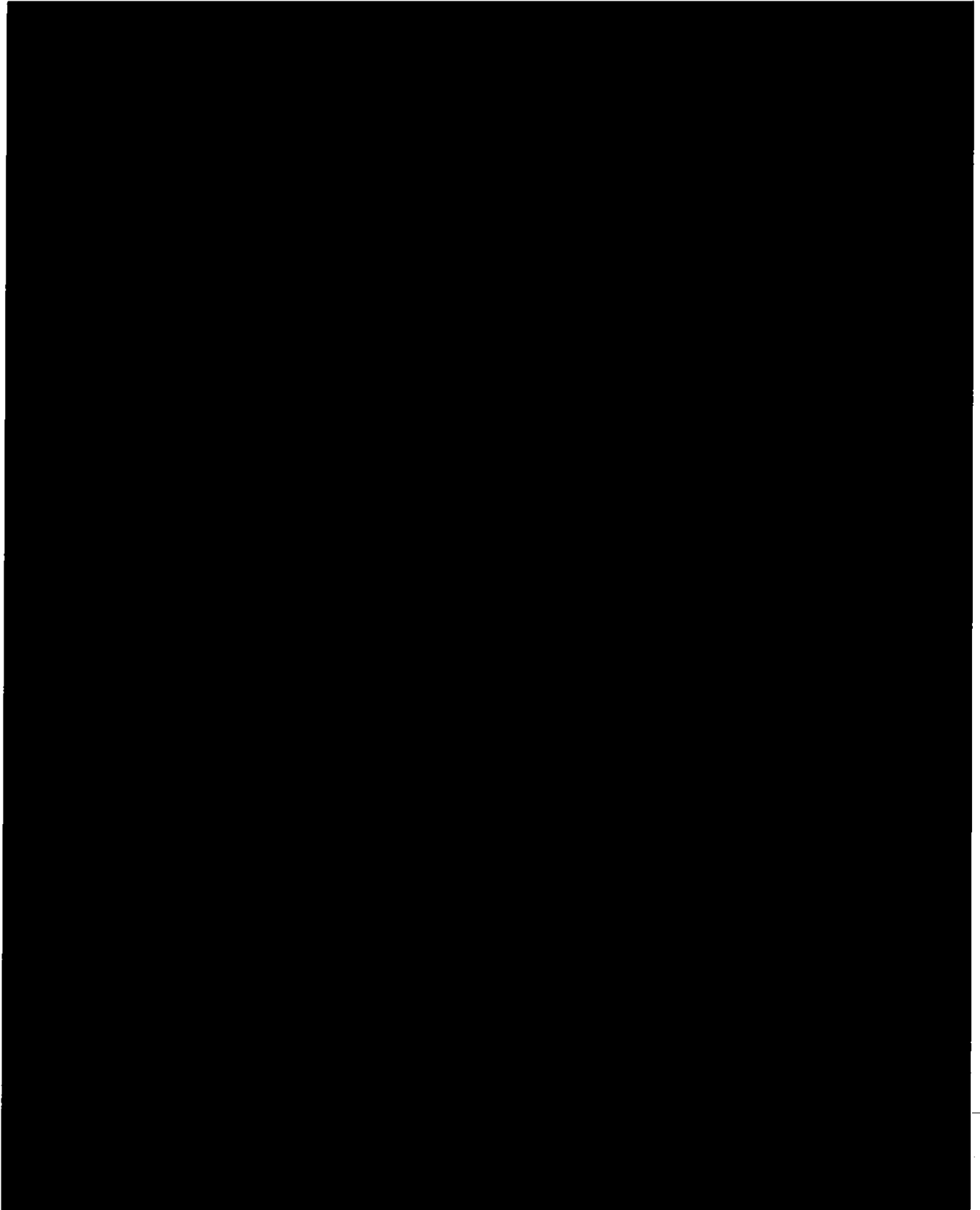


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

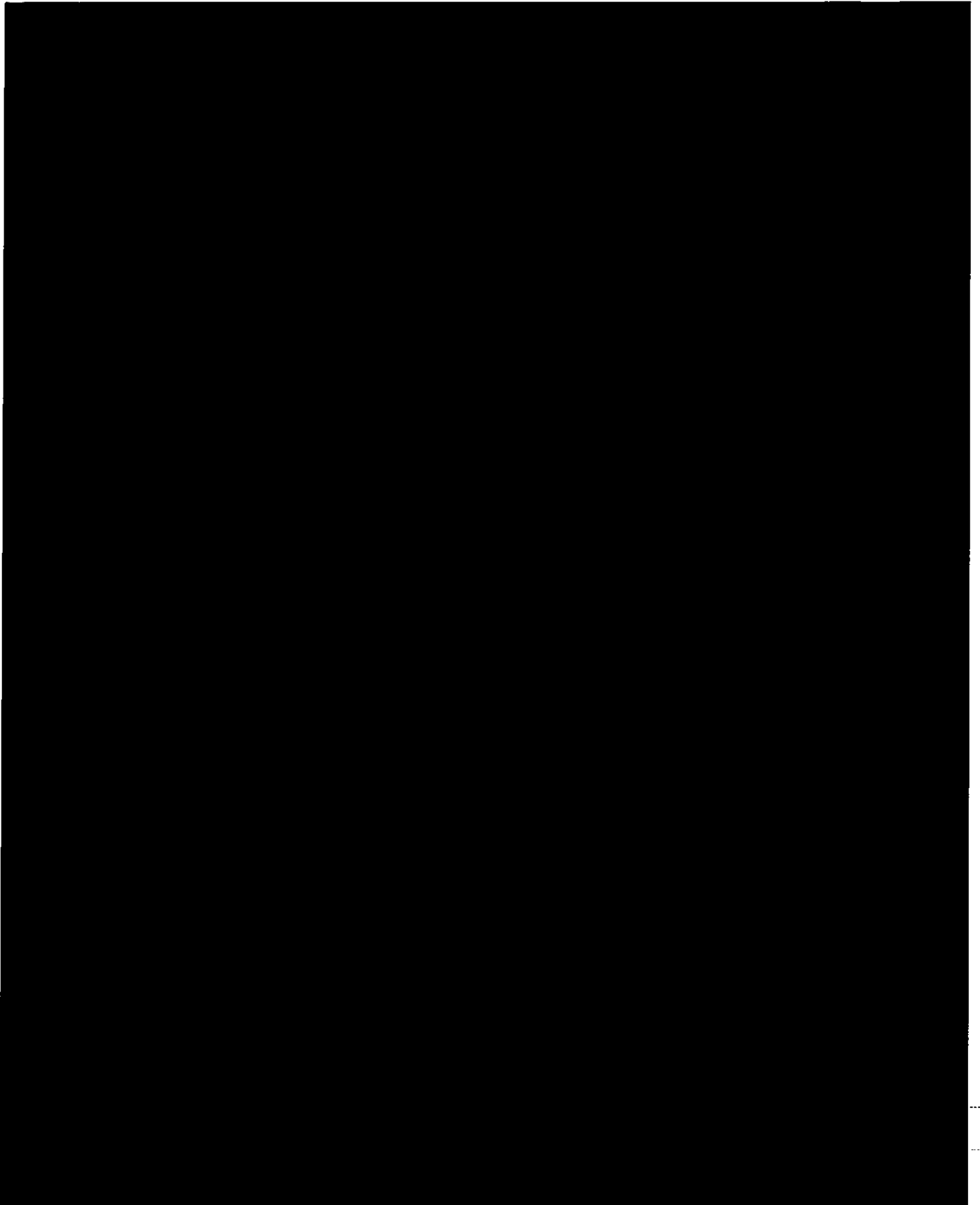


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~



~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

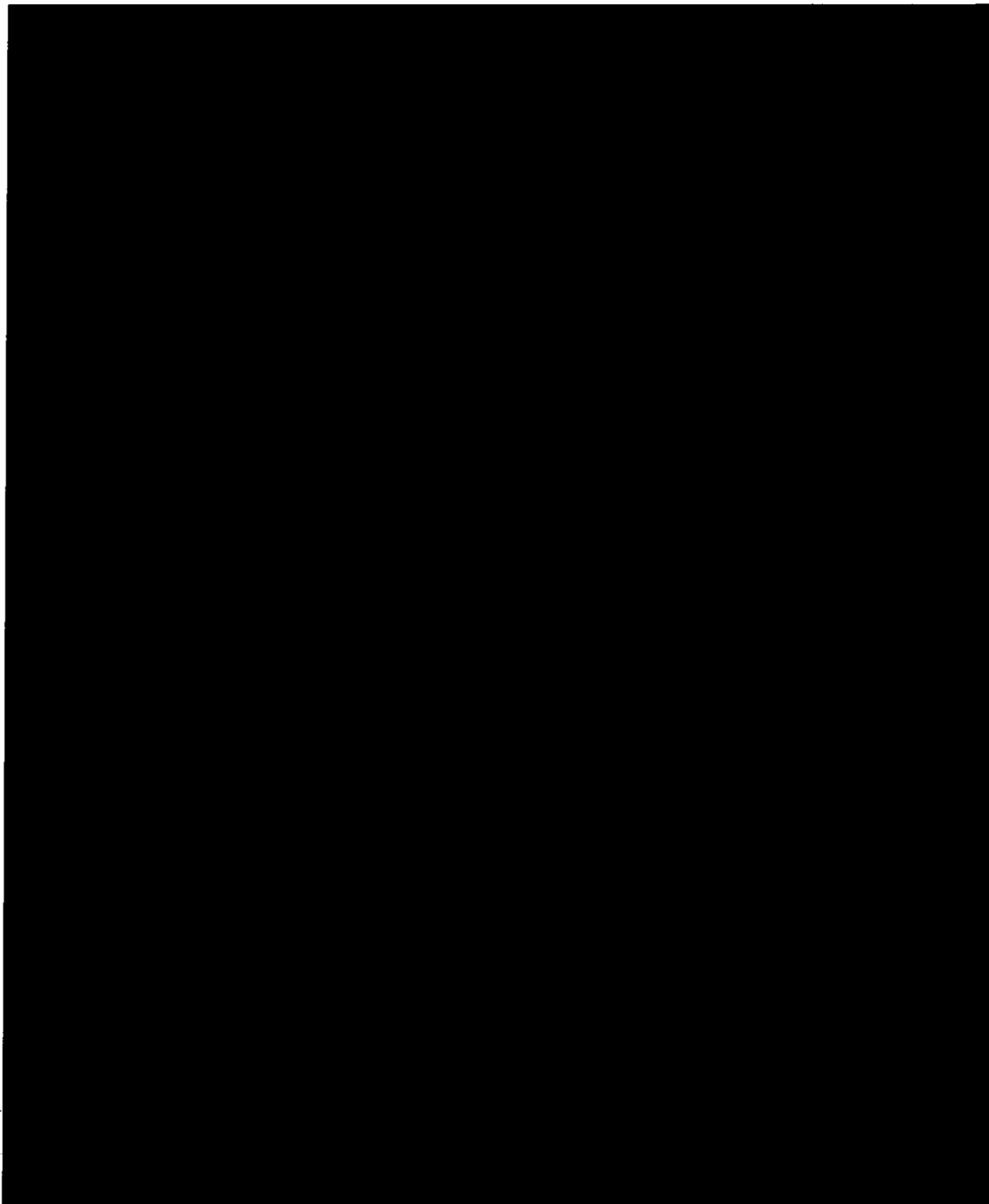


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

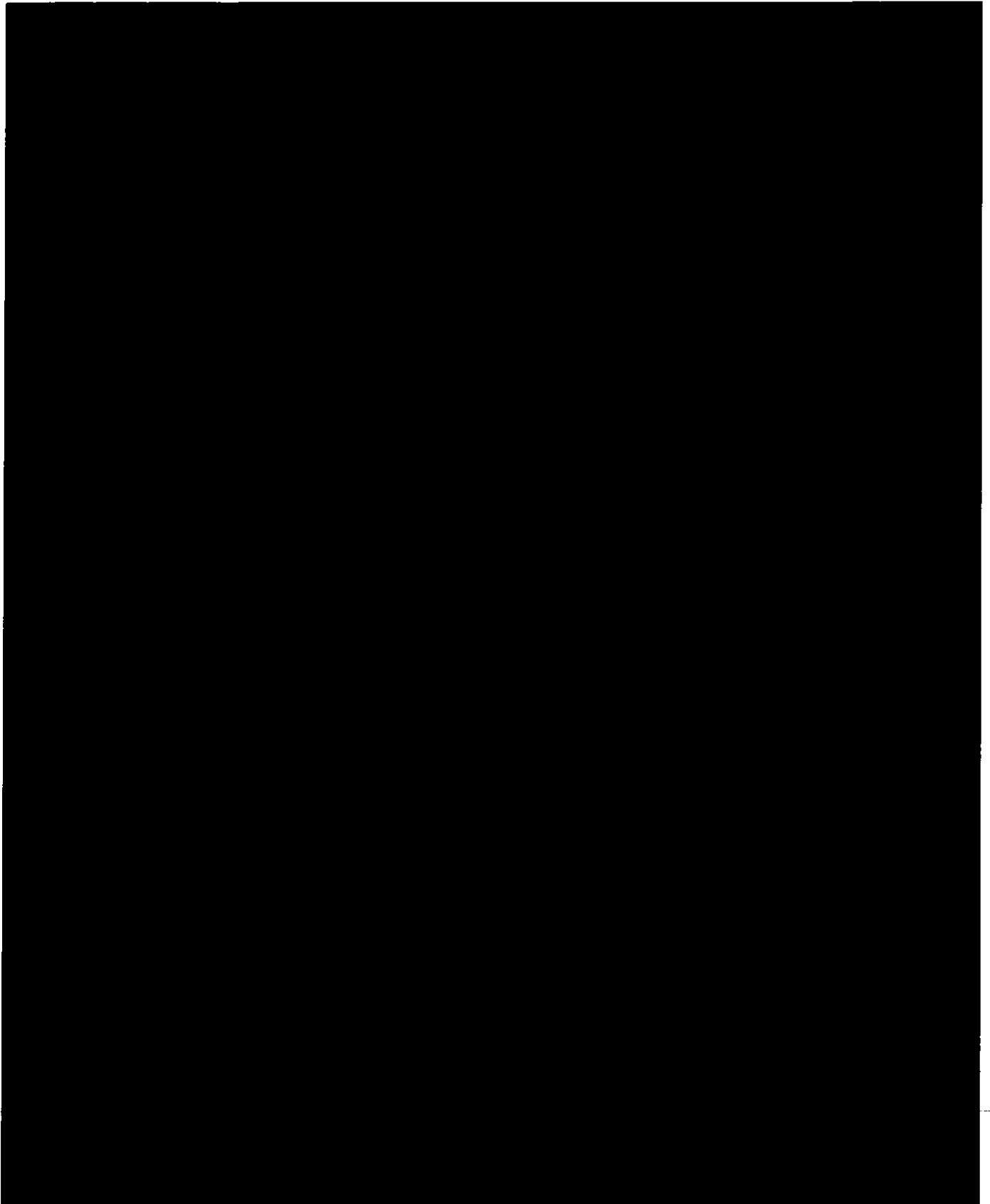


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~



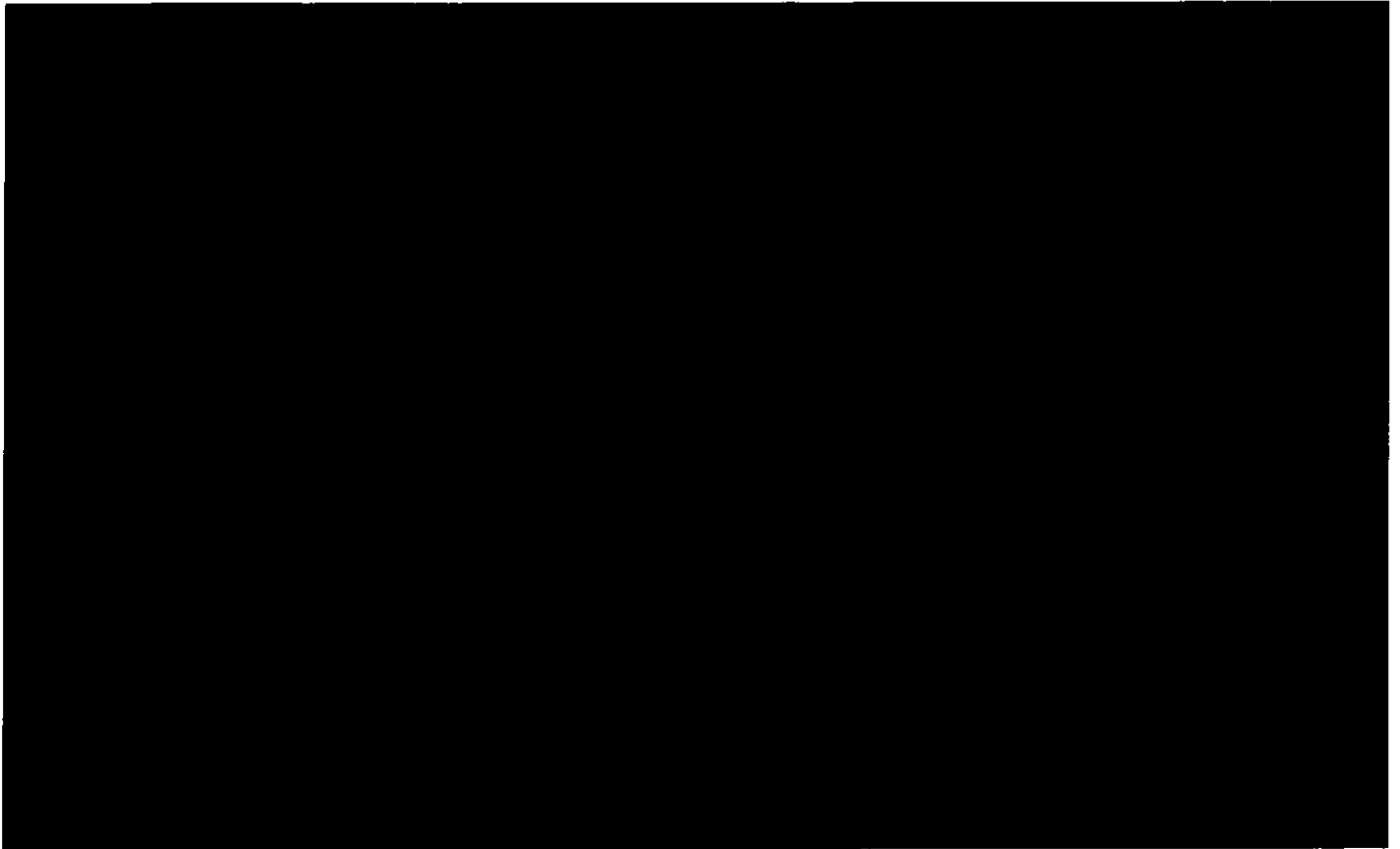
~~TOP SECRET//COMINT//NOFORN//20320108~~



Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~



~~TOP SECRET//COMINT//NOFORN//20320108~~

**EXHIBIT B****MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN  
CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE  
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE  
SURVEILLANCE ACT OF 1978, AS AMENDED**  
U.S. DEPT. OF JUSTICE  
INTELLIGENCE  
SURVEILLANCE  
2007 APR 20 AM 11:20  
CLERK OF COURT**Section 1 - Applicability and Scope (U)**

These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). (U)

If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity. (U)

For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). (U)

**Section 2 - Definitions (U)**

In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

- (a) Acquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party. (U)
- (b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. (U)
- (c) Communications of a United States person include all communications to which a United States person is a party. (U)

~~Derived From: NSA/CSSM 1-52~~~~Dated: 20070108~~~~Declassify On: 20320108~~~~SECRET//COMINT//NOFORN//20320108~~

- (d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)
- (e) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications. ~~(S//SI)~~
- (f) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S//SI)~~
- (g) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)
- (h) Publicly-available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)
- (i) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S//SI)~~
- (j) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)
- (1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person. (U)
  - (2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

~~SECRET//COMINT//NOFORN//20310108~~

- (3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with 8 U.S.C. § 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)
- (4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

### Section 3 - Acquisition and Processing - General (U)

#### (a) Acquisition (U)

The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition. (S//SI)

#### (b) Monitoring, Recording, and Processing (U)

- (1) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications. ~~(S//SI)~~
- (2) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, 6, and 8 of these procedures. ~~(C)~~
- (3) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S)~~

~~SECRET//COMINT//NOFORN//20320108~~

- (4) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5, 6, and 8 of these procedures.

~~(S//SI)~~

- (5) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Any United States person identifiers used as terms to identify and select communications must be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.

~~(S//SI)~~

- (6) Further processing, retention and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below.

~~(S//SI)~~

(c) Destruction of Raw Data ~~(C)~~

Communications and other information, including that reduced to graphic or "hard copy" form such as facsimile, telex, computer data, or equipment emanations, will be reviewed for retention in accordance with the standards set forth in these procedures. Communications and other information, in any form, that do not meet such retention standards and that are known to contain communications of or concerning United States persons will be destroyed upon recognition, and may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications.

~~(S//SI)~~

(d) Change in Target's Location or Status ~~(S//SI)~~

- (1) In the event that NSA determines that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person is in fact a United States person, the acquisition from that person will be terminated without delay.
- (2) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact

~~(S//SI)~~

~~SECRET//COMINT//NOFORN//20320108~~

~~SECRET//COMINT//NOFORN//20310108~~

located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person, will be treated as domestic communications under these procedures. ~~(S//SI)~~

#### Section 4 - Acquisition and Processing - Attorney-Client Communications ~~(C)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed disseminations of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination. ~~(S//SI)~~

#### Section 5 - Domestic Communications (U)

A communication identified as a domestic communication will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that: ~~(S)~~

- (1) the communication is reasonably believed to contain significant foreign intelligence information. Such communication may be provided to the Federal Bureau of Investigation (FBI) (including United States person identities) for possible dissemination by the FBI in accordance with its minimization procedures; ~~(S)~~
- (2) the communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such communications may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes; ~~(S)~~
- (3) the communication is reasonably believed to contain technical data base information, as defined in Section 2(i), or information necessary to understand or assess a communications security vulnerability. Such communication may be provided to the

~~SECRET//COMINT//NOFORN//20320108~~

~~SECRET//COMINT//NOFORN//20310108~~

FBI and/or disseminated to other elements of the United States Government. Such communications may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. ~~(S//SI)~~

- a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S//SI)~~
- b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signal Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or ~~(S//SI)~~

- (4) the communication contains information pertaining to a threat of serious harm to life or property. ~~(S)~~

Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may advise the FBI of that fact. Moreover, technical data regarding domestic communications may be retained and provided to the FBI and CIA for collection avoidance purposes. ~~(S//SI)~~

#### Section 6 - Foreign Communications of or Concerning United States Persons (U)

##### (a) Retention (U)

Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

- (1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.
  - a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

~~SECRET//COMINT//NOFORN//20320108~~

- b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signals Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;
- (2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or
- (3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. ~~(S//SI)~~

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 or 8 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

- (1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;
- (2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;
- (3) the communication or information indicates that the United States person may be:
  - a. an agent of a foreign power;
  - b. a foreign power as defined in Section 101(a) of the Act;
  - c. residing outside the United States and holding an official position in the government or military forces of a foreign power;
  - d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
  - e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;



~~SECRET//COMINT//NOFORN//20310108~~

- (4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;
- (5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications security vulnerability, but only after the agency that originated the information certifies that it is properly classified;
- (6) the communication or information indicates that the United States person may be engaging in international terrorist activities;
- (7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or
- (8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. (U)

(c) Provision of Unminimized Communications to CIA and FBI ~~(S//NF)~~

- (1) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI//NF)~~
- (2) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will process any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI)~~

Section 7 - Other Foreign Communications (U)

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

(U)

~~SECRET//COMINT//NOFORN//20320108~~

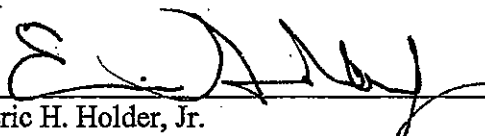
~~SECRET//COMINT//NOFORN//20310108~~Section 8 - Collaboration with Foreign Governments ~~(S//SI)~~

- (a) Procedures for the dissemination of evaluated and minimized information. Pursuant to Section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with subsections 6(b) and 7 of these NSA minimization procedures. ~~(S)~~
- (b) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated: ~~(S)~~
- (1) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA. ~~(S)~~
  - (2) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data. ~~(S)~~
  - (3) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA. ~~(S)~~
  - (4) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA. ~~(S)~~

~~SECRET//COMINT//NOFORN//20320108~~

- (5) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures. ~~(S)~~

4-11-11  
Date

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

~~SECRET//NOFORN//21 JULY 2034~~

## EXHIBIT C

2011 APR 20 AM 11:20  
U.S. FEDERAL  
INTELLIGENCE  
SURVEILLANCE COURT  
FEDERAL BUILDING HALL  
COURT

**PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION FOR  
TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE  
LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN  
INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN  
INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED**

~~(S)~~ These procedures address: (I) the process the Federal Bureau of Investigation (FBI) will use in acquiring foreign intelligence information, [REDACTED] by targeting electronic communications accounts/addresses/identifiers designated by the National Security Agency (NSA) [REDACTED] as being used by non-United States persons reasonably believed to be located outside the United States, (II) the FBI's documentation of that process, and (III) compliance and oversight.

I. (U) DETERMINATION OF WHETHER A PERSON IS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES AND NOT A UNITED STATES PERSON

1. ~~(S)~~ [REDACTED] NSA will follow its targeting procedures, adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(d) of the Act, for determining that the user of the [REDACTED] is a person reasonably believed to be located outside the United States and is not a United States person. NSA will also be responsible for determining that a significant purpose of the acquisition is to obtain foreign intelligence information.
2. ~~(S)~~ NSA will provide the FBI with identifying information of any [REDACTED] together with an explanation of NSA's conclusion that the user of the [REDACTED] is a person reasonably believed to be located outside the United States and its determination regarding the non-United States person status of the user. NSA will also represent that a significant purpose of [REDACTED] is to obtain foreign intelligence information and that the purpose of such acquisition is not to intentionally target a particular, known person reasonably believed to be in the United States.
3. ~~(S)~~ The FBI, in consultation with NSA, will review and evaluate the sufficiency of: (a) NSA's explanation for its reasonable belief that the user of the [REDACTED] is located outside of the United States; and (b) information provided by NSA concerning the [REDACTED] user's non-United States person status.

~~Classified By: PSCG  
Reason: E.O. 12958 Section 1.4((c))  
Declassify On: 21 July 2034  
SECRET//NOFORN//21 JULY 2034~~

~~SECRET//NOFORN//21 JULY 2034~~

4. ~~(S)~~ In the ordinary course of determining whether to

[REDACTED]

- a. ~~(S)~~

[REDACTED]

- b. ~~(S)~~

[REDACTED]

5. ~~(S)~~ Unless the FBI [REDACTED] the user of the [REDACTED]  
[REDACTED] is a United States person or is located inside of the United States, the FBI will

[REDACTED]

6. ~~(S//NF)~~

[REDACTED]

~~SECRET//NOFORN//21 JULY 2034~~

~~SECRET//NOFORN//21 JULY 2034~~

[REDACTED]

All such communications retained by the FBI will be processed in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

7. ~~(S)~~ If NSA analysis of [REDACTED] indicates that a user of a [REDACTED] from which [REDACTED] pursuant to these procedures is actually located within the United States or is a United States person, NSA will promptly [REDACTED]
8. ~~(S)~~ If the FBI [REDACTED] is not appropriate for tasking under section 702 (i.e., because the user of the [REDACTED] is a United States person and/or is located inside of the United States), the FBI will inform NSA, and the FBI will not [REDACTED] of the [REDACTED] until the FBI determines that the [REDACTED] is in fact appropriate for tasking under section 702.
9. ~~(S)~~ In addition, the FBI will take appropriate action, which may include the [REDACTED]

[REDACTED]

~~SECRET//NOFORN//21 JULY 2034~~

~~SECRET//NOFORN//21 JULY 2034~~

## II. (U) DOCUMENTATION

10. ~~(S)~~ The FBI will ensure the retention of information it receives from NSA concerning the non-United States person status of the user of the [REDACTED] and the factual basis for NSA's determination that the user of the [REDACTED] is reasonably believed to be located outside the United States in accordance with the National Archives and Records Administration (NARA) and, as appropriate, the FBI's Records Management Division and/or Security Division standards, policies, and guidelines.

11. ~~(S)~~ [REDACTED]

## III. (U) COMPLIANCE AND OVERSIGHT

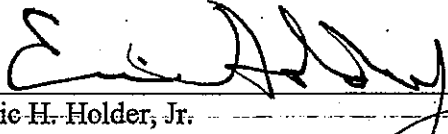
12. ~~(S)~~ The FBI will develop and deliver training regarding the applicable procedures to ensure that all personnel responsible for [REDACTED] under these procedures understand their responsibilities with respect to [REDACTED]. The FBI has established processes for determining which [REDACTED] and for ensuring that [REDACTED] and the related [REDACTED] are accessible only to those who are authorized and have had the proper training.

13. ~~(S)~~ The FBI Inspection Division will conduct oversight of the FBI's exercise of these procedures. This oversight will include periodic reviews by FBI Inspection Division personnel to evaluate the implementation of the procedures and the training given to relevant personnel. Such reviews will occur at least once every quarter.

14. ~~(S)~~ The DOJ and ODNI will conduct oversight of the FBI's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of these procedures. Such reviews will occur at least once every sixty days.

15. ~~(S)~~ The FBI will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by FBI personnel within five business days of learning of the incident.

9-11-11  
Date

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

~~SECRET//NOFORN//21 JULY 2034~~

~~SECRET//NOFORN~~

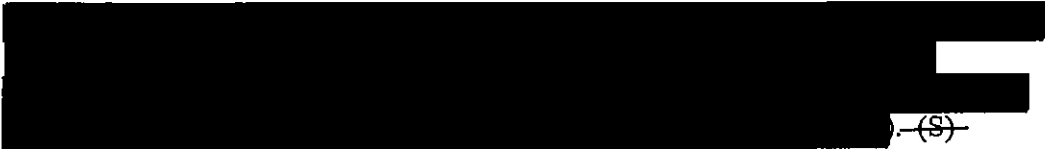


U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

EXHIBIT D

2009 JUL 29 PM 3:14  
CLERK OF COURT  
**MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF  
INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN  
INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN  
INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED**

These Federal Bureau of Investigation (FBI) minimization procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). (U)

With respect to any unminimized communications acquired pursuant to section 702 of the Act, the FBI will apply its standard minimization procedures as described in the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act (adopted October 21, 2008) ("Standard Minimization Procedures"), with the following modifications: ~~(S)~~

- a. References to "information acquired pursuant to FISA" and "FISA-acquired information" will be understood to also include communications acquired pursuant to section 702 of the Act. (U)
- b.  ~~(S)~~
- c. References to "target" will be understood to refer to the user(s) of a targeted selector, account, or  ~~(S)~~
- d. Section II.A ("Acquisition – Electronic Surveillance") will not apply. (U)
- e. Subparagraphs 1 through 5 of Section II.B ("Acquisition – Physical Search, including of Electronic Data") will be replaced in their entirety by the following subparagraphs: ~~(S)~~
  1. The FBI may acquire  pursuant to section 702 of the Act only in accordance with FBI targeting procedures that have been adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to section 702(d) of the Act. ~~(S)~~
  2. Any communication acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States but is in fact located inside the United States at the time

Derived From: Multiple Sources  
Declassify On: July 21, 2034

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

such communication is acquired or is subsequently determined to be a United States person will be removed from FBI systems upon recognition, unless the Director or Deputy Director of the FBI specifically determines in writing that such communication is reasonably believed to contain significant foreign intelligence information, evidence of a crime that has been, is being, or is about to be committed, or information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. Notwithstanding the above, if any such communications indicate that a person targeted under section 702 has entered the United States, nothing in these procedures shall prevent the FBI from retaining and providing to the National Security Agency (NSA) and Central Intelligence Agency (CIA) technical information derived from such communication for collection avoidance purposes. ~~(S)~~

3. As soon as FBI personnel recognize that an acquisition of a communication under section 702 of this Act is inconsistent with any of the limitations set forth in section 702(b),<sup>1</sup> the FBI will purge the communication and destroy all other copies of that communication that are accessible to any end user electronically or in hard copy. Any electronic copies of the communication that are not available to any end user but are available to a systems administrator as an archival back-up will be restricted and destroyed in accordance with normal business practices and will not be made available to any other person except as permitted by the FISC. In the event FBI archival back up data is used to restore an electronic and data storage system, the FBI will ensure that the previously deleted communication will not be accessible to any user and will be deleted from any stored system. ~~(S)~~

- f. Paragraph 4 of Section III.B will be replaced in its entirety with the following:

Required training on the Standard Minimization Procedures and the FBI's policies regarding access to raw FISA-acquired information before granting access to raw FISA-acquired information. ~~(S)~~

---

<sup>1</sup> Subsection 702(b) provides that "[a]n authorization authorized under subsection (a) --

- (1) may not intentionally target any person known at the time of the acquisition to be located in the United States;
- (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be located in the United States;
- (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
- (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
- (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States." (U)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- g. The following will be added as Paragraph 6 to Section III.B:

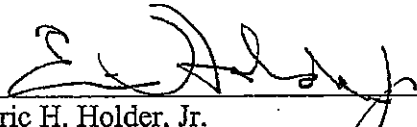
With respect to information acquired pursuant to section 702 of the Act, only those FBI personnel who have received training on the application of these "Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" may be designated as case coordinators. All FBI personnel having access to information acquired pursuant to section 702 of the Act will be informed of and provided access to these minimization procedures. ~~(S)~~

- h. Section III.C.3 ("Categories of Non-Pertinent and Sensitive Information") will not apply. ~~(S)~~
- i. In Section III.E ("Retention of Attorney-Client Communications"), the second sentence of the preamble (i.e., "In certain cases, however, the Government may propose and/or the FISC may order the use of supplemental procedures.") shall not apply. Furthermore, all remaining references to the FISC in this section shall be replaced by DOJ-NSD. ~~(S)~~
- j. The time limits described in Section III.G ("Time Limits for Retention") as applied to communications acquired pursuant to section 702 of the Act will be measured from the expiration date of the certification authorizing the collection. ~~(S)~~
- k. Section IV.E ("Dissemination Under [REDACTED]") will be replaced in its entirety with the following paragraph: ~~(S)~~

With respect to any communications that the FBI acquires from an electronic communication service provider pursuant to Section 702 of the Act, the FBI may convey such communications to the NSA and CIA in unminimized form. The NSA and CIA shall process any [REDACTED] received from the FBI pursuant to these procedures in accordance with the NSA and CIA minimization procedures, respectively, adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S)~~

- l. Section V.C ("Minimization Briefings") will not apply. ~~(S)~~

7-28-09  
Date

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

~~SECRET//NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~SECRET~~

**STANDARD MINIMIZATION PROCEDURES FOR FBI ELECTRONIC  
SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED  
UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U)**

EFFECTIVE: November 1, 2008

~~Classified by: Michael Mukasey, Attorney General  
Reason: 1.4(c)  
Declassify on: October 21, 2033~~

~~SECRET~~

~~SECRET~~TABLE OF CONTENTS

I. GENERAL PROVISIONS (U).....	1
II. ACQUISITION (U).....	4
A. Acquisition – Electronic Surveillance (U) .....	4
B. Acquisition – Physical Search, [REDACTED] (S).....	5
1. Personnel Authorized to Conduct Physical Search (U) .....	5
2. Conducting Physical Search (U) .....	5
a. Areas of search (U) .....	6
b. Manner of search (U) .....	6
i. [REDACTED] (S).....	6
ii. Temporary Removal (S) .....	7
iii. Destructive Testing (U).....	7
c. United States Person [REDACTED] (S).....	7
3. Physical Search Involving Mail or Private Couriers (U) .....	7
4. Record of Information Collected in Physical Search (U).....	8
5. Report of Physical Search (U).....	8
C. Acquisition – Third Parties (U) .....	8
III. RETENTION (U) .....	9
A. Retention – Storage of FISA-acquired Information (U).....	9
B. Retention – Access to FISA-acquired Information (U).....	10
C. Retention – Review and Use of FISA-acquired Information (U).....	12
1. General Provisions (U).....	12
2. Third-Party Information (U).....	13
3. Categories of Non-Pertinent and Sensitive Information (U).....	14

~~SECRET~~

~~SECRET~~

D. Retention - [REDACTED]	
[REDACTED] (S) .....	16
E. Retention of Attorney-Client Communications (U) .....	17
1. Target charged with a crime pursuant to the United States Code (U) .....	17
2. Target charged with a non-Federal crime in the United States and persons other than a target charged with a crime in the United States (U) .....	19
3. Privileged communications involving targets and other persons not charged with a crime in the United States (U) .....	21
F. Additional Procedures for Retention, Use and Disclosure of FISA Information (U) .....	22
G. Time Limits for Retention (U) .....	25
1. [REDACTED]	
2. [REDACTED]	
3. [REDACTED]	
4. [REDACTED]	

#### IV. DISSEMINATION (U) .....

A. Dissemination of Foreign Intelligence Information to Federal, State, Local and Tribal Officials and Agencies (U) .....	27
1. Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(1) (U) .....	27
2. Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(2) (U) .....	28
B. Dissemination of Evidence of a Crime to Federal, State, Local and Tribal Officials (U) .....	28

~~SECRET~~

~~SECRET~~

C. Dissemination of Foreign Intelligence Information Concerning United States Persons to Foreign Governments (U).....	29
D. [REDACTED].....	30
E. [REDACTED].....	32
F. [REDACTED].....	32
G. [REDACTED].....	33
V. COMPLIANCE (U).....	33
A. Oversight (U).....	33
B. Training (U).....	35
C. Minimization Briefings (U).....	35
VI. Interpretation (U).....	35
VII. Review of Procedures (U) .....	36

~~SECRET~~

~~SECRET~~

## I. GENERAL PROVISIONS (U)

A. In accordance with 50 U.S.C. §§ 1801(h) and 1821(4), these procedures govern the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting United States persons that the Federal Bureau of Investigation (FBI) obtains pursuant to orders issued by the Foreign Intelligence Surveillance Court (FISC) or emergency authorizations by the Attorney General under the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), 50 U.S.C. §§ 1801-1811 and 1821-1829. For the purpose of these procedures, the term "applicable FISA authority" refers to both FISC-ordered and Attorney General authorized electronic surveillance or physical search conducted in a particular case pursuant to FISA. The Attorney General has adopted these procedures after concluding that they meet the requirements of 50 U.S.C. §§ 1801(h) and 1821(4) because they are specific procedures that are reasonably designed in light of the purpose and technique of the particular surveillance or physical search to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information and otherwise comport with the statutory definition of minimization procedures. In accordance with 50 U.S.C. § 403-1(f)(6), the Director of National Intelligence (DNI) has provided assistance to the Attorney General with respect to the dissemination procedures set forth herein so that FISA-acquired information may be used efficiently and effectively for foreign intelligence purposes. (U)

~~SECRET~~

~~SECRET~~

B. Pursuant to 50 U.S.C. §§ 1806(a) and 1825(a), no information acquired pursuant to FISA may be used or disclosed by Federal officers or employees except for lawful purposes.

Information acquired from electronic surveillance or physical search conducted under FISA concerning United States persons may be used and disclosed by Federal officers and employees without the consent of the United States persons only in accordance with these minimization procedures and any modified or supplemental minimization procedures that may apply. These procedures do not apply to publicly available information concerning United States persons, nor do they apply to information that is acquired, retained, or disseminated with a United States person's consent. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] S

C. These procedures adopt the definitions set forth in 50 U.S.C. § 1801, including those for the terms "foreign intelligence information" and "United States person." [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~SECRET~~



~~SECRET~~

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] (S)

D. If FBI personnel, which, for the purposes of these procedures, includes all contractors and others authorized to work under the direction and control of the FBI on FISA related matters, encounter a situation that they believe requires them to act inconsistently with these procedures in order to protect the national security of the United States, enforce the criminal law, or protect life or property from serious harm, those personnel immediately should contact FBI

Headquarters and the Office of Intelligence of the National Security Division of the Department of Justice (NSD) to request that these procedures be modified. The United States may obtain modifications to these procedures with the approval of the Attorney General and a determination by the FISC that the modified procedures meet the definition of minimization procedures under sections 1801(h) and/or 1821(4) of FISA. (U)

E. If, in order to protect against an immediate threat to human life, the FBI determines that it must take action in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the FISC, the FBI shall report that activity promptly to the NSD, which shall notify the FISC promptly of such activity. (U)

F. Nothing in these procedures shall restrict the FBI's performance of lawful oversight functions of its personnel. (U)

~~SECRET~~

~~SECRET~~

## II. ACQUISITION (U)

### A. Acquisition – Electronic Surveillance. (U)

1. Prior to initiating electronic surveillance, the FBI shall verify that the facility or place at which it will direct surveillance is the facility or place specified in the applicable FISA authority. The FBI is under a continuing obligation to verify that the authorized target of the surveillance uses or is about to use the facility or place at which the surveillance is directed during the authorized period of surveillance. The FBI shall terminate electronic surveillance of a facility or place as soon as it determines that the authorized target of the electronic surveillance no longer uses, nor is about to use, the facility or place, and shall promptly notify the NSD of such termination. (U)

2. When conducting electronic surveillance of a facility or place pursuant to the applicable FISA authority, the FBI may acquire, using the means and to the extent approved by the court or authorized by the Attorney General for that facility or place: (a) all information or communications transmitted to or from the facility or place; (b) all communications that occur at such facility or place; (c) all visual, aural, and other non-verbal information that the approved surveillance device(s) can acquire at such facility or place; and (d) all information, communications, or other data processed at such facility or place by computers or other equipment present at the facility or place. To the extent consistent with the electronic surveillance approved by the Court or authorized by the Attorney General, the FBI may, at its discretion, automatically record all information, communications and data that it acquires, and also may conduct live monitoring of such acquisition. ~~(S)~~

~~SECRET~~

~~SECRET~~

3. Notwithstanding Section II.A.2, the FBI shall, to the extent reasonably feasible:

(a) use means of surveillance that are designed to limit the acquisition of nonpublicly available information or communications of or concerning unconsenting United States persons that are not foreign intelligence information relating to a target of the surveillance; and (b) place surveillance devices in locations within a facility or place at which surveillance is directed only where they are likely to acquire foreign intelligence information relating to a target of the surveillance. ~~(S)~~

**B. Acquisition – Physical Search, [REDACTED] ~~(S)~~**

**1. Personnel Authorized to Conduct Physical Search. (U)**

Physical search shall be conducted only by: (i) appropriately authorized and trained personnel of the FBI, not including contractors; (ii) [REDACTED]

[REDACTED] (iii) [REDACTED]

[REDACTED]

[REDACTED]. Pursuant to 50 U.S.C. § 1824(e)(2)(B)-(D), other persons, [REDACTED], may assist in the physical search as specified in the applicable FISA authority. ~~(S)~~

**2. Conducting Physical Search. (U)**

Prior to initiating physical search, the FBI shall verify that the premises or property at which it will conduct physical search is the premises or property specified in the applicable FISA authority. The FBI shall conduct physical search with the minimum intrusion necessary to acquire the foreign intelligence information sought. Personnel conducting physical search shall exercise reasonable judgment in determining whether the information, material, or property

~~SECRET~~

~~SECRET~~

revealed through the search reasonably appears to be foreign intelligence information relating to a target of the search or evidence of a crime. The FBI shall conduct the search in accordance with the applicable FISA authority. (U)

a. Areas of search. For physical search of premises or property, after conducting any necessary protective sweep, the FBI shall, where reasonably feasible, limit search areas to locations within premises or property where the FBI reasonably expects that: (i) foreign intelligence information may be stored or concealed by the target; or (ii) foreign intelligence information related to the target or the activities of the target may be found. (U)

b. Manner of Search. The FBI may conduct physical search using the methods most suitable for acquiring the foreign intelligence information sought in light of the particular circumstances of the search. When conducting a physical search of electronic data, the FBI may acquire all information, communications, or data relating to the target in accordance with the applicable FISA authority. Methods used to conduct physical search may include: inspection; examination; reproduction; temporary removal; marking for identification; testing; alteration; substitution; or seizure of information, material, or property. (U)

i.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ~~(S)~~

~~SECRET~~

~~SECRET~~

- ii. Temporary Removal. The FBI may temporarily remove information, material, or property for technical, scientific, or other reasonably necessary examination, and for any other purpose approved by the Court. ~~(S)~~
- iii. Destructive Testing. The FBI may conduct destructive testing of material discovered in a physical search only when such testing is provided for in the applicable FISA authority or in case of emergency when reasonably necessary to protect against immediate threat to public safety. (U)

c. United States Person Information, Material, or Property. The FBI may intentionally alter, substitute, or seize information, material, or property belonging to a United States person only when reasonably necessary to prevent serious injury, loss of life, crime, damage to property, or damage to the national security of the United States. The preceding sentence does not preclude the alteration or substitution of material or property that is necessary to effect a physical search of electronic data in accordance with the applicable FISA authority.

~~(S)~~

3. Physical Search Involving Mail or Private Couriers. (U)

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ~~(S)~~

~~SECRET~~

~~SECRET~~

b. [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] ~~(S)~~

4. Record of Information Collected in Physical Search. (U)

The FBI shall keep records identifying all information, material, or property acquired during a physical search. (U)

5. Report of Physical Search. (U)

Within seven business days following the execution of a physical search, or receiving notice that a search has been executed, and for which the FISC ordered that a search return be filed, the FBI shall notify the NSD of the date the search took place. The preceding requirement shall not apply to physical searches of electronic data. ~~(S)~~

C. Acquisition – Third Parties. (U)

“Third-party information” is: (a) nonpublicly available information of or concerning an unconsenting United States person who is not the authorized target of the particular FISA collection, or (b) the material or property of a United States person who is not the authorized target of the particular FISA collection. Third-party information may include the communications or property of family members, coworkers or others, who are not the targets of the collection, but who share facilities, premises or property with the target. Third-party information does not include any information contained in a communication to which the target

~~SECRET~~

**~~SECRET~~**

is a party. The FBI shall limit, to the extent reasonably feasible, its acquisition of third-party information during the course of electronic surveillance or physical search. The foregoing does not preclude the acquisition of all information, communications, or data relating to the target in accordance with the applicable FISA authority where necessary to effect electronic surveillance or physical search of electronic data. ~~(S)~~

**III. RETENTION (U)****A. Retention — Storage of FISA-acquired Information. (U)**

The FBI must retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with these and other applicable FBI procedures. These retention procedures apply to FISA-acquired information retained in any form. FBI electronic and data storage systems may permit multiple authorized users to access the information simultaneously or sequentially and to share FISA-acquired information between systems. "FISA-acquired information" means all information, communications, material, or property that the FBI acquires from electronic surveillance or physical search conducted pursuant to FISA. (U)

"Raw FISA-acquired information" is FISA-acquired information that (a) is in the same or substantially same format as when the FBI acquired it, or (b) has been processed only as necessary to render it into a form in which it can be evaluated to determine whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. Illustrative examples of raw FISA-acquired information include audio recordings of intercepted communications

**~~SECRET~~**

~~SECRET~~

(including copies thereof); soft or hard copies of e-mails and other Internet communications or data; digital images, negatives, or prints of photographs of documents obtained during a physical search; electronic storage media (including computer hard drives and removable storage media); verbatim translations of documents or communications; and intercepted communications that have been processed into the form of "tech cuts" but have not been evaluated to determine whether the tech cuts reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. ~~(S)~~

**B. Retention – Access to FISA-acquired Information. (U)**

The FBI may grant access to FISA-acquired information to all authorized personnel in accordance with policies established by the Director, FBI, in consultation with the Attorney General or a designee. The FBI's policies regarding access will vary according to whether a particular storage system contains raw FISA-acquired information, will be consistent with the FBI's foreign intelligence information-gathering and information-sharing responsibilities, and shall include provisions:

1. Permitting access to FISA-acquired information only by individuals who require access in order to perform their job duties or assist in a lawful and authorized governmental function;
2. Requiring the FBI to maintain accurate records of all persons to whom it has granted access;

~~SECRET~~



~~SECRET~~

3. Requiring the FBI to maintain accurate records of all persons who have accessed raw FISA-acquired information, and to audit its access records regularly to ensure that raw FISA-acquired information is only accessed by authorized individuals [REDACTED]

4. Requiring training on these minimization procedures and the FBI's policies regarding access to raw FISA-acquired information before granting access to raw FISA-acquired information; and

5. Requiring the primary case agent(s) and his/her/their designees (hereinafter "case coordinator(s)") to control the marking of information in a particular case in accordance with FBI policy. A marking, for example, would include an indication that the information is or is not foreign intelligence. ~~(S)~~


The FBI shall provide such policies to the Court when these procedures go into effect. Thereafter, the FBI shall provide any new policies or materially modified policies to the Court [REDACTED]

[REDACTED] ~~(S)~~

The FBI may make raw FISA-acquired information available to authorized personnel on a continuing basis for review, translation, analysis, and use in accordance with these procedures.

Authorized personnel may [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]



~~SECRET~~

~~SECRET~~ (S)

**C. Retention – Review and Use of FISA-acquired Information. (U)**

**1. General Provisions. (U)**

FBI personnel with authorized access to raw FISA-acquired information may review, translate, analyze, and use all such information only in accordance with these procedures and FISA and only for the purpose of determining whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. Such personnel shall exercise reasonable judgment in making such determinations. (S)

FBI personnel with authorized access may copy, transcribe, summarize, review, or analyze raw FISA-acquired information only as necessary to evaluate whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. Once FBI personnel have assessed that raw FISA-acquired information meets one of these criteria, the FBI may retain that information for further investigation and analysis and may disseminate it in accordance with these procedures. Pursuant to 50 U.S.C. §§ 1801(h)(3) and 1821(4)(C), however, information that is assessed to be evidence of a crime but not to be foreign intelligence or necessary to understand foreign intelligence may only be retained and disseminated for law enforcement purposes. The FBI shall identify FISA-acquired information in its storage systems,   
 that has been reviewed and meets these standards.

~~SECRET~~

~~SECRET~~

If the FBI proposes to use any storage system that is incapable of meeting these requirements, the FBI shall follow the procedures set forth in Section I.D. ~~(S)~~

Before using FISA-acquired information for further investigation, analysis, or dissemination, the FBI shall strike, or substitute a characterization for, information of or concerning a United States person, including that person's identity, if it does not reasonably appear to be foreign intelligence information, to be necessary to understand or assess the importance of foreign intelligence information, or to be evidence of a crime. (U)

The FBI may disseminate copies, transcriptions, summaries, and other documents containing FISA-acquired information only in accordance with the dissemination procedures set forth in Part IV below. (U)

The FBI shall retain FISA-acquired information that is not foreign intelligence information that has been reviewed and reasonably appears to be exculpatory or impeachment material for a criminal proceeding, or reasonably appears to be discoverable in a criminal proceeding, and shall treat that information as if it were evidence of a crime. ~~(S)~~

2. Third-Party Information. (U)

The FBI may retain and use third-party information for investigative and analytical purposes in accordance with these procedures if such information reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime (which is being retained or used for law enforcement purposes), and:

- (a) is a communication made or received on behalf of the target(s);

~~SECRET~~

~~SECRET~~

- (b) concerns activities in which the target(s) is or may be involved; or
- (c) concerns a serious threat of injury, loss of life, damage to property, or damage to the national security of the United States. ~~(S)~~

Third-party information that does not fall into these categories may be retained in accordance with Section III.G of these procedures but may not be used for investigation or analysis and may not be included in investigative or analytical documents such as Electronic Communications or reports. If, however, FBI personnel acquire information that does not fall into one of these categories but that they believe should be used, the FBI shall proceed in accordance with Sections I.D and I.E. ~~(S)~~

3. Categories of Non-Pertinent and Sensitive Information. (U)

FBI personnel shall continually analyze communications of or information concerning United States persons acquired pursuant to FISA for the purpose of establishing categories of information that are not foreign intelligence information, are not necessary to understand foreign intelligence information or assess its importance, or are not evidence of a crime. These categories should be established after a reasonable period of monitoring the communications of the target and shall be reported to the Court in a later renewal application relating to that target. When developing these categories, particular attention should be given to the following types of sensitive information:

(a) [REDACTED]

(b) [REDACTED]

[REDACTED]

~~SECRET~~

~~SECRET~~

(c) [REDACTED]

[REDACTED]

(d) [REDACTED]

(e) [REDACTED]

(f) [REDACTED]

(g) [REDACTED]

[REDACTED] ~~(S)~~

Before using information from an established category of sensitive information for investigation or analysis, including using the information in investigative or analytical documents such as Electronic Communications (ECs) or reports, FBI personnel shall determine that the information that falls into such categories reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ~~(S)~~

SECRET

~~SECRET~~

D. Retention — [REDACTED] (S)

Authorized users may query FBI electronic and data storage systems that contain raw FISA-acquired information to find, extract, review, translate, and assess whether such information reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. Such queries may involve the use of keywords, identifiers, formulas, attributes, or other sophisticated data exploitation techniques. To the extent reasonably feasible, authorized users must design such queries to find and extract foreign intelligence information or evidence of a crime and to minimize the extraction of third-party information. Authorized users may process the results of an appropriate query in accordance with Section III.C above. The FBI shall maintain records of all searches, including search terms, used to query such systems. (S)

Authorized users may query FBI electronic and data storage systems to find, extract, and analyze "metadata" pertaining to communications. The FBI may also use such metadata to analyze communications and may upload or transfer some or all such metadata to other FBI electronic and data storage systems for authorized foreign intelligence or law enforcement purposes. [REDACTED]

[REDACTED]

[REDACTED] (S)

~~SECRET~~

~~SECRET~~**E. Retention of Attorney-Client Communications. (U)**

This section governs the retention of attorney-client communications. In certain cases, however, the Government may propose and/or the FISC may order the use of supplemental procedures. FBI personnel shall consult as appropriate with FBI Division Counsel, the FBI Office of General Counsel, or the NSD to determine whether a communication is privileged. (U)

**I. Target charged with a crime pursuant to the United States Code. (U)**

As soon as the FBI knows that a target is charged with a crime pursuant to the United States Code, the FBI shall implement procedures that ensure that the target's attorney-client privilege is protected. These procedures shall include the following, unless otherwise authorized by the FISC:

a. Establishment of a review team of one or more monitors and/or reviewers, who have no role in the prosecution of the charged criminal matter, to initially access and review information or communications acquired from a surveillance or search of a target who is charged with a crime pursuant to the United States Code;

b. A procedure to ensure that as soon as the review team determines that the FBI has acquired a privileged communication concerning the charged criminal matter between the target and the attorney representing the target in that matter, the FBI will appropriately mark the communication privileged in a manner that is apparent to anyone who accesses the information, including in any FBI electronic and data storage system. An attorney representing the target in the criminal matter includes anyone working on behalf of that attorney, such as another attorney, an expert witness, a paralegal, or an administrative assistant; and

~~SECRET~~

~~SECRET~~

c. A procedure to ensure that within 10 business days of determining that a privileged communication under this section has been acquired [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]. Any electronic

versions of the privileged communications that are not available to any end user but are available to a systems administrator as an archival back-up will be restricted and destroyed in accordance with normal business practices and will not be made available to any other person except as permitted by the FISC. In the event FBI archival back up data is used to restore an electronic and data storage system, the FBI will ensure that the previously deleted privileged communications will not be accessible to any user and will be deleted from any restored system.

d. FISA-acquired information, other than privileged information that has been sealed according to Sections III.E.1.a-c, above, may subsequently be made available to the investigative team, including prosecutors, as appropriate.

e. As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired pursuant to a particular FISA search or surveillance, the FBI shall ensure that whenever any user reviews information or communications acquired from that search or surveillance, which are in an FBI electronic and data storage system containing raw FISA-acquired information, he receives electronic notification that attorney-client communications have been acquired during the search or

~~SECRET~~



~~SECRET~~

surveillance. The purpose of the notification is to alert others who may review this information that they may encounter privileged communications, (S).

2. Target charged with a non-Federal crime in the United States and persons other than a target charged with a crime in the United States. (U)

FBI monitors and other personnel with access to FISA-acquired information shall be alert for communications that may be (i) between a target who is charged with a non-Federal crime in the United States and the attorney representing the individual in the criminal matter, or (ii) between a person other than a target charged with a crime in the United States and the attorney representing the individual in the criminal matter. As soon as FBI personnel know that a target is charged with a non-Federal crime in the United States or someone other than the target who appears to regularly use the targeted facility, place, premises or property is charged with a crime in the United States, they will notify the Chief Division Counsel, FBI Office of General Counsel, and the NSD to determine whether supplemental procedures or a separate monitoring team are required. In the absence of such supplemental procedures or a separate monitoring team, as soon as FBI personnel recognize that they have acquired a communication between (i) a target who is charged with a non-Federal crime in the United States and the attorney representing the individual in the criminal matter, or (ii) a person other than a target charged with a crime in the United States and the attorney representing the individual in the criminal matter, the FBI shall implement procedures that include the following:

- a. A procedure to ensure that the FBI immediately ceases monitoring or reviewing a privileged communication concerning the charged criminal matter;

~~SECRET~~

~~SECRET~~

b. [REDACTED]  
[REDACTED]  
[REDACTED]

c. A procedure to ensure that within 10 business days of determining that a privileged communication under this section has been acquired, [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]. Any electronic versions of the privileged communications that are not available to any end user but are available to a systems administrator as an archival back-up will be restricted and destroyed in accordance with normal business practices and will not be made available to any other person except as permitted by the FISC. In the event FBI archival back up data is used to restore an electronic and data storage system, the FBI will ensure that the previously deleted privileged communications will not be accessible to any user and will be deleted from any restored system; and

d. As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired pursuant to a particular FISA search or surveillance, the FBI shall ensure that whenever any user reviews information or communications acquired from that search or surveillance, which are in an FBI electronic and data storage system containing raw FISA-acquired information, he receives electronic

~~SECRET~~

~~SECRET~~

notification that attorney-client communications have been acquired during the search or surveillance. The purpose of the notification is to alert others who may review this information that they may encounter privileged communications. ~~(S)~~

3. Privileged communications involving targets and other persons not charged with a crime in the United States. (U)

The FBI may review and use FISA-acquired communications of a target or other person not charged with a crime in the United States that are attorney-client privileged in conducting a National Security investigation. Authorized FBI personnel who review FISA-acquired information that is privileged (i) must mark the communication (in hard copy and electronically) as privileged in a manner that is apparent to anyone who accesses the information; and (ii) may disseminate the item within the United States Intelligence Community if it otherwise meets the standards for dissemination. Before disseminating such item that otherwise meets the standards for dissemination outside the United States Intelligence Community, the FBI must obtain the approval of the Attorney General or the Attorney General's designee. ~~(S)~~

If the FBI determines that a privileged FISA-acquired communication of a person not charged with a crime in the United States is not foreign intelligence information but is evidence of a crime, the FBI must obtain approval to disseminate the information for law enforcement purposes from the Attorney General or the Assistant Attorney General for National Security. The FBI may disseminate the information immediately if it determines there is an immediate threat to life or of serious property damage. If the FBI makes such a dissemination, it shall immediately inform the NSD. ~~(S)~~

~~SECRET~~

~~SECRET~~

**F. Additional Procedures for Retention, Use and Disclosure of FISA Information. (U)**

1. Pursuant to 50 U.S.C. §§ 1806(b) and 1825(c), no information acquired pursuant to an order authorizing electronic surveillance or physical search under FISA shall be disclosed for law enforcement purposes unless [REDACTED]

[REDACTED] FISA-acquired information, including raw FISA-acquired information, may be disclosed for law enforcement purposes in criminal proceedings. (S)

2. The FBI shall ensure that identities of any persons, including United States persons, that reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime, [REDACTED] (S)

3. Prosecutors. (U)

a. The FBI may disclose FISA-acquired information, including raw FISA-acquired information, and information derived therefrom, to federal prosecutors and others working at their direction, for all lawful foreign intelligence and law enforcement purposes, [REDACTED]

[REDACTED] When federal prosecutors and

~~SECRET~~

~~SECRET~~

others working at their direction are provided access to raw FISA-acquired information, they shall be trained on and comply with these and all other applicable minimization procedures. (S)

b. In accordance with applicable Attorney General-approved policies and procedures, federal prosecutors may also disclose FISA-acquired information, when necessary for the prosecutors to carry out their responsibilities, including to witnesses, targets or subjects of an investigation, or their respective counsel, when the FISA-acquired information could be foreign intelligence information or is evidence of a crime. This provision does not restrict a federal prosecutor's ability, in a criminal proceeding, to disclose FISA-acquired information that contains exculpatory or impeachment information or is otherwise discoverable under the Constitution or applicable federal law. (U)

c. The FBI may not provide federal prosecutors and others working at their direction [REDACTED] containing raw FISA-acquired information unless such access is: (a) for foreign intelligence or law enforcement purposes; (b) consistent with their responsibilities as federal prosecutors; and (c) pursuant to procedures established by the Attorney General and provided to the FISC. The procedures established by the Attorney General and provided to the FISC shall include the following:

- i. Access [REDACTED]  
[REDACTED] must be limited to that which is consistent with their responsibilities as federal prosecutors and necessary to carry out their responsibilities efficiently during a specific investigation or prosecution;

~~SECRET~~

~~SECRET~~

- ii. Access must be requested from and approved by an executive at FBI Headquarters in a position no lower than Assistant Director (AD) and in coordination with the Deputy General Counsel of the FBI National Security Law Branch or a Senior Executive Service attorney in the National Security Law Branch, and will be considered on a case-by-case basis;
- iii. A request for access must specify [REDACTED], Foreign Intelligence Surveillance Court (FISC) docket numbers, and targeted facilities the prosecutor needs access, why such access is necessary, and the duration of such access;
- iv. All individuals receiving authorization to have direct access must receive [REDACTED] and training on the standard minimization procedures and any relevant supplemental minimization procedures applicable to the information to which they have access;
- v. Access shall be terminated no later than the conclusion of the relevant investigation or prosecution; and
- vi. Federal prosecutors may immediately be given access to FBI [REDACTED] raw FISA-acquired information if FBI personnel determine that an immediate

~~SECRET~~

~~SECRET~~

threat to life or of serious damage to property necessitates immediate access, and if such immediate access is given to federal prosecutors, notification shall be made to FBI Headquarters, FBI's Office of General Counsel, and NSD. ~~(S)~~

**G. Time Limits for Retention. (U)**

In general, the FBI may retain FISA-acquired information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. ~~(S)~~

1. The FBI is authorized to retain data in electronic and data [REDACTED]

[REDACTED], in accordance with the following:

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ~~(S)~~

b. [REDACTED]

[REDACTED] ~~(S)~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~SECRET~~

~~SECRET~~

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] (S)  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] (S)

2. [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] (S)

3. Audio and video recordings not accessible through an electronic and data storage system, and items and/or records obtained through physical search of premises or property, including images or copies of computer hard drives and removable media acquired during the execution of a physical search order, whether reviewed or not, but not identified as information that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or evidence of a crime, shall be destroyed within specific time periods

~~SECRET~~



~~SECRET~~

as set forth in FBI policy, which shall provide for periodic destruction of certain categories of FISA-acquired information. This provision does not apply to FISA-acquired information within the scope of Section IILG.1 or IILG.2. ~~(S)~~

4. FISA-acquired information retained by the FBI in any other form. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] ~~(S)~~

#### IV. DISSEMINATION (U)

##### A. Dissemination of Foreign Intelligence Information to Federal, State, Local and Tribal Officials and Agencies. (U)

The FBI may disseminate FISA-acquired information that reasonably appears to be foreign intelligence information in accordance with Sections IV.A.1 and IV.A.2 to federal, state, local and tribal officials and agencies with responsibilities directly related to the information proposed to be disseminated. Information that reasonably appears to be foreign intelligence information not directly related to responsibilities of such agencies may be disseminated incidental to the dissemination of information directly related to responsibilities of such agencies. Such information may be disseminated only consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. (U)

1. Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(1). (U)

The FBI may disseminate to [REDACTED] FISA-acquired information concerning United States persons that reasonably appears to be necessary

~~SECRET~~

~~SECRET~~

to the ability of the United States to protect against: (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. ~~(S)~~

2. Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(2). (U)

The FBI may disseminate to [REDACTED] FISA-acquired information concerning United States persons that reasonably appears to be necessary: (i) to the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States. Such information shall not be disseminated, however, in a manner that identifies a United States person, unless such person's identity is necessary to understand foreign intelligence information or to assess its importance. ~~(S)~~

**B. Dissemination of Evidence of a Crime to Federal, State, Local and Tribal Officials.** (U)

The FBI may disseminate, for a law enforcement purpose, FISA-acquired information concerning a United States person that reasonably appears to be evidence of a crime but not foreign intelligence information to [REDACTED]

[REDACTED] The FBI shall disseminate such FISA-acquired information in a manner consistent with the requirements of Section III.F. ~~(S)~~

~~SECRET~~

~~SECRET~~

**C. Dissemination of Foreign Intelligence Information Concerning United States Persons to Foreign Governments. (U)**

The FBI may disseminate FISA-acquired information concerning United States persons, which is foreign intelligence information, to foreign governments as follows:

1. Disseminations of FISA-acquired information concerning United States persons to the governments of the United Kingdom, Canada, Australia or New Zealand may be made upon the approval of the Director of the FBI, or a designee. ~~(S)~~
2. Disseminations of FISA-acquired information concerning United States persons to other foreign governments shall be made consistently with Department of Justice guidance and may be made upon the approval of the Director of the FBI, or a designee who shall hold a position no lower than Section Chief in the FBI, and shall be in coordination with the FBI Office of General Counsel, upon consideration of the following factors: the national security benefit the United States may reasonably expect to obtain from making the dissemination; the anticipated uses to which the foreign government will put the information; and any potential for economic injury, physical harm, or other restriction of movement to be reasonably expected from providing the information to the foreign government. If the proposed recipient(s) of the dissemination have a recent record of human rights abuses, that history should be considered in assessing the potential for economic injury, physical harm, or other restriction of movement, and whether the dissemination should be made. ~~(S)~~

Where there is a reasonable basis to anticipate that the dissemination will result in economic injury, physical harm, or other restriction of movement, no dissemination shall be

~~SECRET~~

~~SECRET~~

made without the approval of the Attorney General. If the Attorney General approves the dissemination, the FBI shall undertake reasonable steps to ensure that the disseminated information will be used in a manner consistent with United States laws, including Executive Order 12333 (as amended) and applicable federal criminal statutes. ~~(S)~~

3. The Attorney General, in consultation with the DNI or a designee, may authorize

[REDACTED]  
[REDACTED]. Prior to granting such authorization, those officials shall consider, among other things: (1) whether such use is consistent with the national security interests of the United States, and (2) the effect of such use on any identifiable United States person. ~~(S)~~

4. The FBI will make a written record of each dissemination approved pursuant to this section, and information regarding such disseminations and approvals shall be [REDACTED]

[REDACTED] ~~(S)~~

D. [REDACTED]

~~(S)~~

The FBI may [REDACTED]

[REDACTED]  
[REDACTED] Consistent with the other provisions of these procedures, the FBI is authorized to disseminate FISA-acquired information, including, tape recordings, transcripts, or electronic storage media (including computer hard drives and removable storage media), [REDACTED]

~~SECRET~~

~~SECRET~~

[REDACTED] The following restrictions apply with respect to any materials so disseminated:

1. Dissemination to [REDACTED]

[REDACTED] of such information or communications. [REDACTED]  
[REDACTED]  
[REDACTED] ~~(S)~~

2. Dissemination will be only to [REDACTED]

[REDACTED] of such information or communications. [REDACTED]  
[REDACTED]  
[REDACTED] ~~(S)~~

3. [REDACTED] shall make no permanent [REDACTED] record of information or communications of or concerning any person referred to in FISA-acquired information or recorded on FISA-acquired tape recordings, transcripts, electronic storage media (including computer hard drives and removable storage media), or other [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] Records maintained [REDACTED] for this purpose may not be disseminated [REDACTED] [REDACTED]  
[REDACTED] ~~(S)~~

4. Upon the conclusion [REDACTED] to the FBI, the FISA-acquired information, including all tape recordings, transcripts, electronic storage media (including

~~SECRET~~

~~SECRET~~

computer hard drives and removable storage media), or other items, or information disseminated

[REDACTED]

[REDACTED] (S)

5. Any information that [REDACTED] provide to the FBI as a result of [REDACTED] may be disseminated by the FBI in accordance with the applicable minimization procedures. (S)

E. [REDACTED] (S)

The FBI may disseminate [REDACTED] raw FISA-acquired information that relates to international terrorism acquired from electronic surveillance or physical search conducted by the FBI as provided in [REDACTED]

[REDACTED] (S)

F. [REDACTED] (S)

In addition to dissemination authorized under other provisions herein, foreign intelligence information, as defined in Section 1801(e), may be disseminated to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (U)

~~SECRET~~

~~SECRET~~G. [REDACTED] ~~(S)~~

Notwithstanding any other provision of these procedures, the FBI may [REDACTED] access to its [REDACTED] database, provided that such access is limited to classifications of cases that are likely to contain information [REDACTED] is contingent upon [REDACTED] [REDACTED] which are on file with the FISC. If the FBI authorizes [REDACTED] to disseminate any information [REDACTED] receives pursuant to this section, such authorization shall be made consistent with these procedures and applicable Department of Justice guidance, including but not limited to restrictions governing dissemination to foreign governments. ~~(S)~~

## V. COMPLIANCE (U)

### A. Oversight. (U)

To ensure compliance with these procedures, the Attorney General, through the Assistant Attorney General for National Security or other designee, shall implement policies and procedures that ensure the good faith compliance with all of the requirements set forth herein, and shall conduct periodic minimization reviews, including reviews at FBI Headquarters, field offices, and U.S. Attorney's Offices that receive raw FISA-acquired [REDACTED]

[REDACTED] The Attorney General and the NSD or other designee of the

~~SECRET~~

~~SECRET~~

Attorney General shall have access to all FISA-acquired information to facilitate minimization reviews and for all other lawful purposes. ~~(S)~~

To assess compliance with these procedures, minimization reviews shall consist of reviews of documents, communications, audit trails, or other information. They shall include, as appropriate, but are not limited to:

1. Reviews of electronic communications or other documents containing FISA-acquired information that have been retained for further investigation and analysis or disseminated in accordance with these procedures. ~~(S)~~
2. Reviews of FISA-acquired information (from electronic surveillance and physical search) in FBI electronic and data storage systems that contain raw FISA-acquired information to assess compliance with these procedures, including whether raw FISA-acquired communications or property have been properly marked as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. FISA-acquired communications and property in FBI electronic and data storage systems that contain raw FISA-acquired information may also be reviewed to determine whether they were properly marked pursuant to the attorney-client communications provisions of these procedures. ~~(S)~~
3. Audits of [REDACTED] raw FISA-acquired information to assess the FBI's compliance with the retention procedures for FISA-acquired information as detailed in Section III of these procedures. The audits may also include reviewing a sampling [REDACTED]

~~SECRET~~



~~SECRET~~

██████ and accesses in FBI electronic and data storage systems containing raw FISA-acquired information. These audits may assist in determining the FISA-acquired information that was accessed in these FBI electronic and data storage systems and the individuals who accessed the information. In turn, the minimization reviews may include verifying that the individuals who accessed the FISA-acquired information in these FBI systems were individuals who had properly been given access under FBI guidelines. ~~(S)~~

**B. Training. (U)**

The Attorney General, or a designee, shall ensure that adequate training on these procedures be provided to appropriate personnel. (U)

**C. Minimization Briefings. (U)**

Following the authorization of collection activity, an NSD attorney shall conduct a minimization briefing with appropriate FBI personnel responsible for the FISA surveillance or search. (U)

**VI. Interpretation (U)**


The FBI shall refer all significant questions relating to the interpretation of these procedures to the NSD. (U)

~~SECRET~~

~~SECRET~~

**VII. Review of Procedures (U)**

The Attorney General, or a designee, in consultation with the FBI Office of General Counsel, shall review these procedures and determine whether they remain appropriate in light of the technology and practices used by the FBI no later than five years from the date of the Attorney General's approval of these procedures filed with the Court, and every five years thereafter. A written report of such review shall be provided to the Court within six months of the completion of the review. (U)



Michael B. Mukasey  
Attorney General of the United States

10/22/08  
Date

~~SECRET~~

EXHIBIT E

MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED ~~(S//NF)~~

With respect to unminimized communications the Central Intelligence Agency (CIA) receives from the National Security Agency (NSA) or the Federal Bureau of Investigation (FBI) that are acquired pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), the CIA will follow the following minimization procedures:

~~(S//NF)~~

1. Definitions:

- a. As used herein, the terms "Attorney General," "foreign power," "agent of a foreign power," "United States person," "person," "foreign intelligence information," "international terrorism," and "sabotage" have the meanings specified in sections 101 and 701 of the Act.
- b. The term "United States person identity" means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name or manufacturer's name, or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not a United States person identity. ~~(S//NF)~~

2. Unminimized communications acquired in accordance with section 702 of the Act and received by CIA will be maintained in access-controlled repositories that are accessible only to those who have had the required training and are physically or logically separated from repositories with general access. Unminimized communications that may contain United States person information that does not otherwise qualify for retention under paragraphs 3, 6, or 8 of these procedures may be retained in such access-controlled repositories for no longer than five years from the expiration date of the certification authorizing the collection unless the Director of the National Clandestine Service (NCS), or one of his or her superiors, determines that an extension is necessary because the communications are reasonably believed to contain significant foreign intelligence information, or evidence of a crime that has been, is being, or is about to be committed. An extension under this paragraph may apply to a specific category of communications, and must be documented in writing, renewed on an annual basis, and promptly reported to the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI). ~~(S//NF)~~

3. Information concerning a United States person may be retained by CIA indefinitely and outside of access-controlled repositories if (a) the information concerning the United States

~~SECRET//NOFORN~~

Classified by: The Attorney General  
Reason: 1.4(c)  
Declassify on: 11 April 2036

person is publicly available; (b) the United States person has consented to retention of the information concerning him or her; or (c) the United States person identity is deleted or otherwise sanitized to prevent the search, retrieval, or review of the identifying information (a generic term may be substituted which does not identify the United States person in the context of the data). If the information cannot be sanitized in such a fashion because the identity is necessary, or it is reasonably believed that it may become necessary, to understand or assess the information, CIA may retain that information and the United States person identity indefinitely and outside of access-controlled repositories if: ~~(S//NF)~~

- a. The information is foreign intelligence information. Such information includes, but is not limited to, information falling within one or more of the following categories:
  - (1) the information indicates that the United States person has acted or may be acting as an agent of a foreign power, including information indicating that a United States person was in contact with a foreign power under facts and circumstances indicating that he intends to collaborate with a foreign power or become an agent of a foreign power;
  - (2) the information indicates that a United States person may be a target of intelligence activities of a foreign power;
  - (3) the information indicates that a United States person has engaged or may be engaging in the unauthorized disclosure of properly classified national security information; or
- b. The information concerns corporations or other commercial organizations the deletion of which would hamper the correlation of foreign intelligence information on the same subject;
- c. The information is enciphered or contains secret meaning;
- d. The information is needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of groups engaged in international terrorism;
- e. The information concerns a United States person who is or reasonably appears to be, on the basis of that or other information, an agent of a foreign power;
- f. The information indicates that a United States person is engaged or may be engaged in international terrorism or activities in preparation therefor;
- g. The information is needed and retained solely to identify individuals in contact with a foreign power or an agent of a foreign power (including for purposes of this subparagraph (g) any person, regardless of location, who engages in international terrorism or activities in preparation therefor; who aids, abets, or conspires with persons to engage in such activities; or who acts as a member of a group engaged in such activities);

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- h. [REDACTED]
- i. The information concerns a person or activity that poses a threat of sabotage, international terrorism, actual or potential attack or other grave hostile act, to any facility or personnel of any agency within the U.S. Intelligence Community, or any department containing such an agency;
- j. The information indicates that a United States person may be a target of intelligence activities of a foreign power; or
- k. The information concerns a U.S. Government official acting in an official capacity.  
~~(S//NF)~~
4. CIA personnel may query CIA electronic and data storage systems containing unminimized communications acquired in accordance with Section 702 of the Act. [REDACTED]  
[REDACTED] Such queries must be reasonably designed to find and extract foreign intelligence information. CIA will maintain records of all such queries, including but not limited to United States person names and identities, and NSD and ODNI will review CIA's activities that are conducted pursuant to this paragraph. ~~(S//NF)~~
5. Any information retained pursuant to paragraph 3 above may be disseminated to otherwise authorized recipients outside of CIA if the identity of the United States person and all personally identifiable information regarding the United States person are deleted or otherwise sanitized to prevent the search, retrieval or review of the identifying information. A generic term may be substituted which does not identify the United States person in the context of the data. However, if the information cannot be sanitized in such a manner because such person's identity is necessary to understand foreign intelligence information or assess its importance, that identity may be disseminated outside of CIA without such person's consent. Additionally, if the information cannot be sanitized in such a manner because it is reasonably believed that such person's identity may become necessary to understand or assess the importance of foreign intelligence information as defined by 50 U.S.C. § 1801 (e)(1), that identity may be disseminated outside of CIA without such person's consent.  
~~(S//NF)~~
6. Nothing in these procedures shall prohibit:
- a. The retention or disclosure of information necessary for the purpose of determining whether the requirements of these procedures are satisfied, provided that the recipient under this paragraph does not retain or disclose the identity of a United States person where it is determined that the requirements of these procedures do not permit dissemination;

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- b. The retention of communications necessary for the maintenance of technical data bases, so long as only collection or technical personnel have access to such data bases;
- c. The retention or dissemination of information concerning corporations or other commercial organizations which is limited to their identities as manufacturers of equipment and related nomenclature or their locations;
- d. The retention or dissemination of information required by law to be retained or disseminated; or
- e. The retention or processing of communications in emergency data backup systems, provided that only administrative, collection, or technical personnel have access to such systems. In the event that information from such systems must be used to restore lost, destroyed, or inaccessible data, CIA shall apply these procedures to the transferred data.  
(S//NF)

7. CIA will also follow the following procedures:

a.



- b. Dissemination to Foreign Governments: CIA may disseminate nonpublicly available identity or personally identifiable information concerning United States persons to foreign governments provided that such information is foreign intelligence information and either (i) the Attorney General approves the dissemination; or (ii) CIA disseminates the information under procedures that have been approved by the Attorney General. In addition, CIA may disseminate such foreign intelligence information acquired pursuant to Section 702 of the Act to the extent authorized by the Director of the CIA, and in

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

accordance with Director of National Intelligence Intelligence Community directives. CIA may make such disseminations without specific Attorney General approval subject to the following procedures:

[REDACTED]

- (3) Procedures for technical or linguistic assistance. It is anticipated that CIA may obtain from NSA and FBI unminimized information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments (collectively "assisting foreign governments") to assist CIA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, CIA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired by NSA or FBI pursuant to Section 702 of the Act to assisting foreign governments for further processing and analysis, provided that the following restrictions apply with respect to any materials so disseminated:
- (a) Dissemination to assisting foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical assistance to CIA.
  - (b) Dissemination will be only to those personnel within assisting foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no further dissemination within assisting foreign governments of this raw data.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- (c) Assisting foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by CIA to assisting foreign government, provided that assisting foreign government may maintain such temporary records as are necessary to enable them to assist CIA with the translation or analysis of such information. Records maintained by assisting foreign governments for this purpose may not be disseminated within the assisting foreign government, except to personnel involved in providing technical assistance to CIA.
  - (d) Upon the conclusion of such technical assistance to CIA, computer disks, tape recordings, transcripts, or other items or information disseminated to assisting foreign government will either be returned to CIA or be destroyed with an accounting of such destruction made to CIA.
  - (e) Any information that assisting foreign governments provide to CIA as a result of such technical assistance may be disseminated by CIA in accordance with these minimization procedures.
- (4) CIA will make a written record of each dissemination approved pursuant to these procedures, and information regarding such disseminations and approvals will be made available for review by the Department of Justice. ~~(S//NF)~~
- c. Compliance With Crimes Reporting Obligations. Notwithstanding other provisions of these minimization procedures, information that is not foreign intelligence information, but reasonably appears to be evidence of a crime that has been, is being, or is about to be committed, may be retained and disseminated (including United States person identities) to the FBI and other appropriate federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. ~~(S//NF)~~
8. Any communication received by CIA that is acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States but is in fact located inside the United States at the time such communication is acquired or was in fact a United States person at the time of targeting will be destroyed unless the Director of the CIA specifically determines in writing that such communication is reasonably believed to contain significant foreign intelligence information or evidence of a crime that has been, is being, or is about to be committed. ~~(S//NF)~~

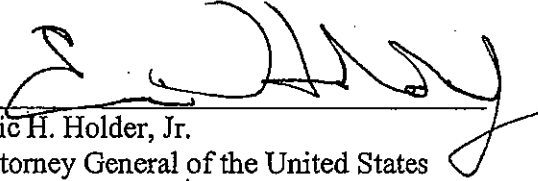
~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

9. If CIA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life and that it is not feasible to obtain a timely modification of these procedures, CIA may take such action immediately. CIA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity. ~~(S//NF)~~

9-17-11  
Date

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

~~SECRET//NOFORN~~

Approved for public release.

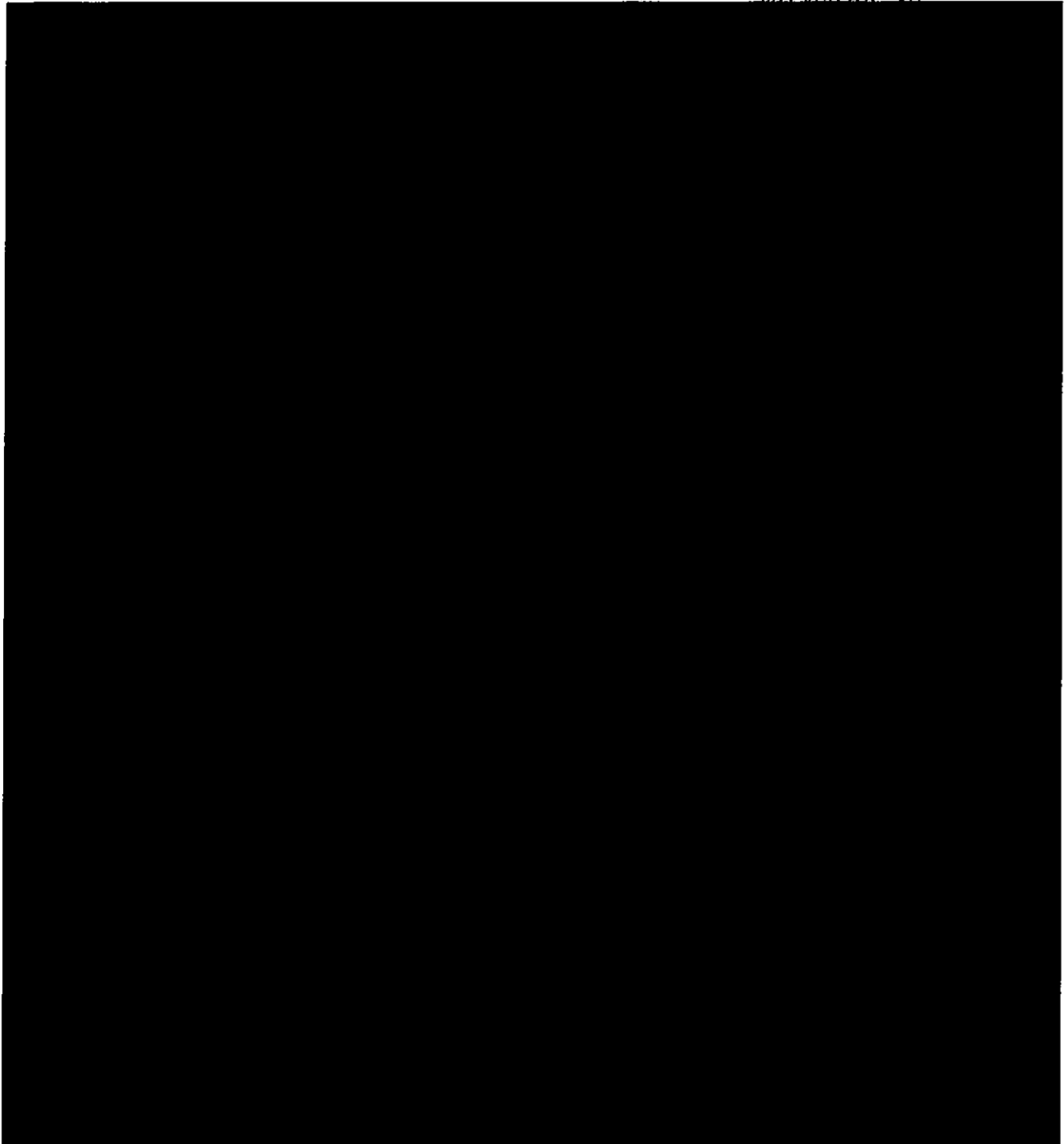
All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE DIVISION

**EXHIBIT F**

2011 APR 28



~~TOP SECRET//NOFORN~~

Derived From: NSA/CSSM 1-52

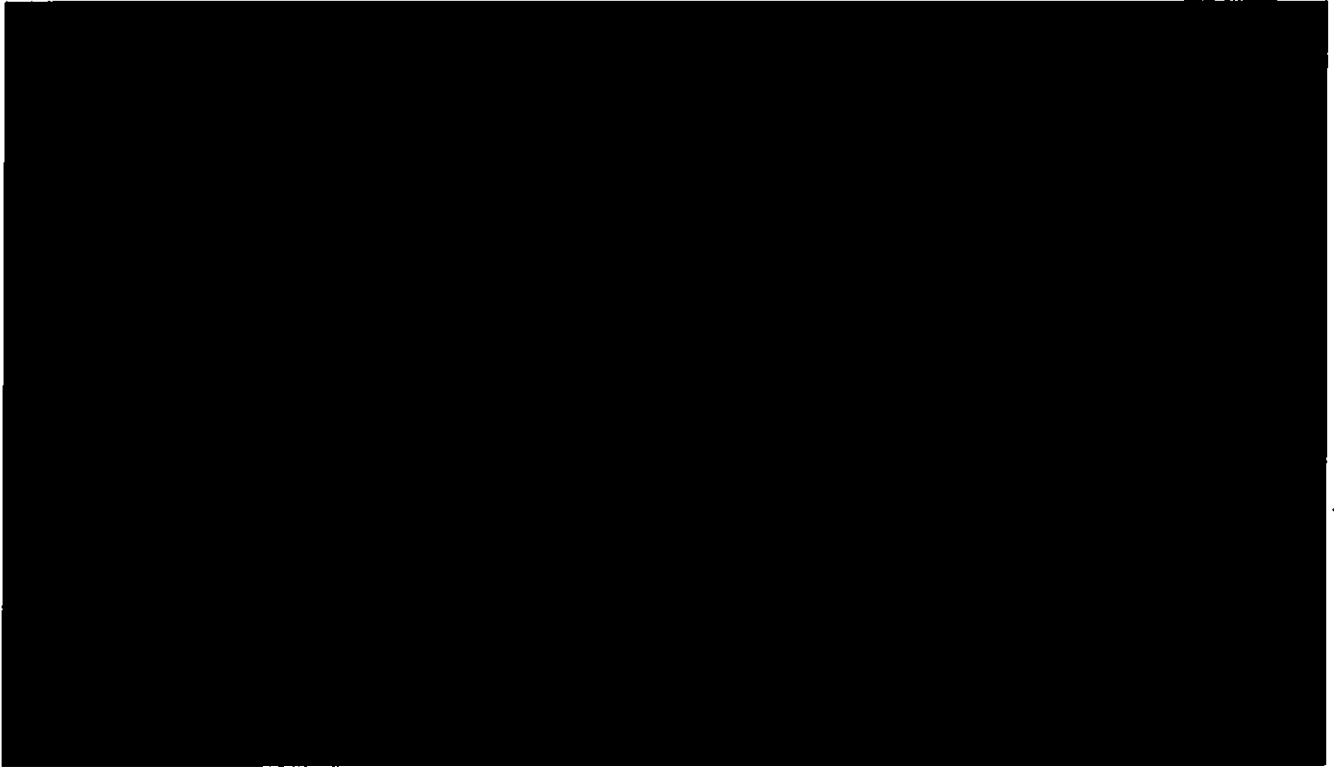
Dated: 20070108

Declassify On: 20340601

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//NOFORN~~



~~TOP SECRET//NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

U.S. FEDERAL  
FOREIGN INTELLIGENCE  
SURVEILLANCE COURT

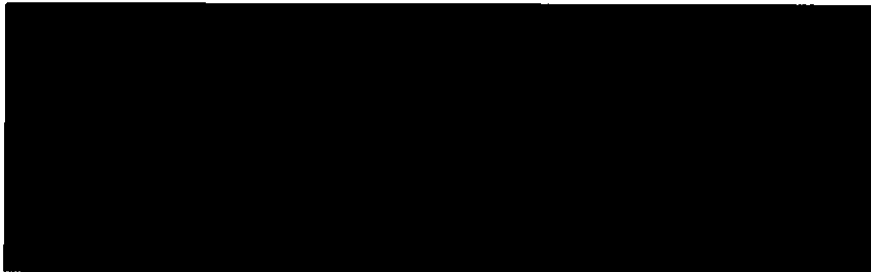
UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

2011 MAY -5 PM 5:18

LEAHN FLYNN HALL  
CLERK OF COURT



UNDER SEAL

MOTION FOR ORDERS EXTENDING TIME LIMITS PURSUANT  
TO 50 U.S.C. § 1881a(j)(2) (S)

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully moves the Court to issue orders pursuant to 50 U.S.C. § 1881a(j)(2) of the Foreign Intelligence Surveillance Act of 1978, as amended (the Act), extending to July 22, 2011, the time limits for the Court to complete its review of and issue orders concerning DNI/AG 702(g) Certifications [REDACTED] and the amendments to their respective predecessor certifications. As discussed below, the government respectfully submits that there is good cause for the extensions of the time limits, and that such extensions would be consistent with national security. (S//OC,NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by:

~~Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ~~

Reason:

~~1.4(c)~~

Declassify on:

~~5 May 2037~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

# ~~I. Procedural Background (S)~~

## A. The 2011 Reauthorization Certifications and Related Amendments ~~(S)~~

On April 20, 2011, the government submitted to the Court DNI/AG 702(g)

[REDACTED]

Included with DNI/AG 702(g)

Certification [REDACTED] were the targeting and minimization procedures to be used by the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Central Intelligence Agency (CIA) under that certification. DNI/AG 702(g) Certification [REDACTED] reauthorizes DNI/AG 702(g) Certification [REDACTED]

[REDACTED]

[REDACTED] ~~(S//OC/NF)~~

DNI/AG 702(g) Certification [REDACTED] also included amendments to its predecessor certifications, DNI/AG 702(g) Certifications [REDACTED]. Specifically, these amendments authorize the use of the minimization procedures attached as Exhibits B and E to DNI/AG 702(g) Certification [REDACTED] in connection with foreign intelligence

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

information acquired in accordance with DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] These amendments also have an effective date of May 23, 2011. (~~S//OC,NF~~)



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~**B. Two Matters Recently Reported to the Court ~~(S)~~****1. Overcollection of [REDACTED] ~~(TS//SI//NF)~~**

On April 19, 2011, the government filed with the Court pursuant to Rule 13(b) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, a preliminary notice of two compliance incidents, both of which concern NSA's collection of [REDACTED] that, in addition to targeted communications, contain communications that are not to, from, or about selectors tasked for acquisition in accordance with section 702 of the Act.<sup>1</sup> One of these incidents concerns NSA's overcollection of [REDACTED] because of [REDACTED]

[REDACTED] The government respectfully incorporates herein by reference this notice dated April 19, 2011. ~~(TS//SI//OC,NF)~~

**2. Clarification Concerning Upstream Collection ~~(TS//SI//NF)~~**

On May 2, 2011, the government filed, pursuant to Rule 13(a) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, a preliminary notice clarifying certain facts concerning NSA's upstream collection of electronic communications.<sup>3</sup> Specifically, this notice provided the Court with additional details

<sup>1</sup> A copy of this notice is attached herewith at Tab A. ~~(S//OC,NF)~~

<sup>2</sup> The other incident reported in this notice concerned NSA's overcollection of [REDACTED] from [REDACTED]. On March 15, 2011, NSA terminated collection [REDACTED] which these [REDACTED] were being collected. ~~(TS//SI//OC,NF)~~

<sup>3</sup> A copy of this notice is attached herewith at Tab B. ~~(S//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

concerning one specified category of Internet communications NSA acquires through its upstream collection -- "electronic communications [REDACTED]

[REDACTED]" As stated in the notice, NSA, NSD, and ODNI are still reviewing this matter and assessing its import, including what effect, if any, this type of Internet communications collection has on the efficacy of the means by which NSA prevents the intentional acquisition of Internet communications where the sender and all intended recipients are known at the time of acquisition to be located in the United States. The government respectfully incorporates herein by reference this notice dated May 2, 2011. ~~(TS//SI//OC,NF)~~

**II. The Issuance of Orders Under 50 U.S.C. § 1881a(j)(2) is Appropriate in These Cases ~~(S)~~**

Upon the government's submission of DNI/AG 702(g) Certification [REDACTED] on April 20, 2011, [REDACTED]

[REDACTED] the thirty-day time periods in which the Court is required to review the certifications began to run. See 50 U.S.C. § 1881a(i)(1)(B). The thirty-day time periods for the Court to review the amendments to the predecessor certifications also began to run on those same dates. See id. § 1881a(i)(C). Accordingly, the time limit for the Court to complete its review of DNI/AG 702(g) Certification [REDACTED] and the amendments to its predecessor certifications is May 20, 2011. Likewise, the time limit for the Court to complete its review of DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] is May 22, 2011. ~~(S//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The Court may, however, "extend[] that time as necessary for good cause in a manner consistent with national security." 50 U.S.C. § 1881a(j)(2). For the following reasons, the government respectfully submits that there is good cause for extensions of the time limits, and that such extensions would be consistent with national security.

~~(S//OC,NF)~~

**A. There is Good Cause for the Court to Extend the Time Limits for Its Review**  
~~(S)~~

The government believes that there is good cause for the Court to extend the deadlines for the Court to complete its review of DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] and the amendments to their respective predecessor certifications.

Specifically, as explained below, the government intends to supplement the record concerning the matters discussed above in a manner that will aid the Court in its review and in making the determinations necessary to issue orders under 50 U.S.C. § 1881a(i)(3). However, the government will not be in a position to supplement the record until after the statutory time limits for such review have expired. ~~(S//OC,NF)~~

First, NSA is in the process of [REDACTED] designed to eliminate the above-discussed overcollection of [REDACTED] communications [REDACTED]

[REDACTED] However, these measures are not expected to be fully operational until on or about June 17, 2011 -- which is after the time limits established by 50 U.S.C.

§ 1881a(i)(1)(B) and (C). Because the government believes that these corrective measures should be considered by the Court as part of its review of the certifications

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

and related amendments, the government respectfully submits that there is good cause for extending the time limits for such review. ~~(S//OC,NF)~~

Second, NSA, NSD, and ODNI are continuing to investigate and assess the manner in which NSA acquires through its upstream collection "electronic communications [REDACTED]

[REDACTED] including what affect, if any, this type of Internet communications collection has on the efficacy of the means by which NSA prevents the intentional acquisition of Internet communications where the sender and all intended recipients are known at the time of acquisition to be located in the United States. The government intends to provide additional information and analysis to the Court upon completion of this review and assessment. However, given the complexity of this issue, the government does not believe its review and assessment will be complete until after the above-discussed time limits established by 50 U.S.C. § 1881a(i)(1)(B) and (C). The government respectfully submits, therefore, there is good cause for extending those time limits because the government believes the additional information and analysis it intends to provide to the Court will assist the Court in making the required statutory findings concerning the certifications and related amendments. ~~(S//OC,NF)~~

**B. Extending the Time Limit for the Court's Review is Consistent with National Security. ~~(S)~~**

As this Court has recognized, "[t]he government's national security interest in conducting these acquisitions [under section 702] 'is of the highest order of magnitude.'"

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

In re DNI/AG Certification [REDACTED] Mem. Op. at 37 (USFISC Sept. 4,

2008) (quoting In re Directives Pursuant to Section 105B of the Foreign Intelligence

Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008)). For example, the foreign

intelligence information the government acquires under DNI/AG 702(g) Certification

[REDACTED]

[REDACTED] DNI/AG 702(g) Certification [REDACTED]

[REDACTED] Affidavit of Lt. General Keith B. Alexander, Director, NSA, ¶ 6. ~~(S//OC,NF)~~

Were the Court to issue orders under 50 U.S.C. § 1881a(j)(2) extending the time limits for its review of the certifications and related amendments so that the Court could consider these additional materials, the authorizations in the certifications being reauthorized, DNI/AG 702(g) Certification [REDACTED] would, by operation of 50 U.S.C. § 1881a(i)(5)(B), continue despite their expiration dates.<sup>4</sup> The government respectfully submits that this result would be consistent with national security, because it would allow the government's acquisition of vitally important foreign intelligence information under DNI/AG 702(g) Certifications [REDACTED]

<sup>4</sup> The government's filing of DNI/AG 702(g) [REDACTED]

[REDACTED] comported with 50 U.S.C. § 1881a(i)(5)(A), which requires that if the government seeks to reauthorize an authorization issued under 50 U.S.C. § 1881a(a), the government must, to the extent practicable, submit to the Court a new certification executed under 50 U.S.C. § 1881a(g), with supporting documents, at least thirty days before the expiration of the certification being reauthorized. If a new certification is filed in accordance with 50 U.S.C. § 1881a(i)(5)(A), 50 U.S.C. § 1881a(i)(5)(B) provides that the existing certification being reauthorized shall remain in effect, notwithstanding its expiration date, until the Court issues an order under 50 U.S.C. § 1881a(i)(3) with respect to the new certification. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] to continue pending the completion of the Court's review of the reauthorization certifications, DNI/AG 702(g) Certification [REDACTED] respectively. ~~(S//OC,NF)~~

The government further submits that it would be consistent with national security for the Court to extend its consideration of the above-discussed amendments, which authorize the use of the NSA and CIA minimization procedures submitted with DNI/AG 702(g) Certifications [REDACTED] in connection with foreign intelligence information acquired in accordance with the predecessors of those certifications. The NSA and CIA minimization procedures currently approved for use under those predecessor certifications, however, differ in some respects from the NSA and CIA minimization procedures submitted with DNI/AG 702(g) Certifications

[REDACTED] The government believes that authorizing the NSA and CIA to use a single set of minimization procedures (i.e., each agency's respective minimization procedures submitted with DNI/AG 702(g) Certifications [REDACTED]


[REDACTED] for the entirety of each agency's holdings of foreign intelligence information acquired under section 702 will result in a more uniform application of minimization standards to that information. Authorizing each agency to use a single set of minimization procedures for that information also will significantly simplify oversight of each agency's adherence to those standards. ~~(S//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~**III. Conclusion ~~(S)~~**

For the foregoing reasons, the government respectfully submits that there is good cause for the Court to issue orders under 50 U.S.C. § 1881a(j)(2) extending to July 22, 2011, the time limit for the Court to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certifications [REDACTED] and the amendments to their respective predecessor certifications, and that such an extension would be consistent with national security. For DNI/AG 702(g) Certification [REDACTED] the government also requests that the Court issue the proposed Notice of Extension, attached herewith. ~~(S//OC,NT)~~

Respectfully submitted,

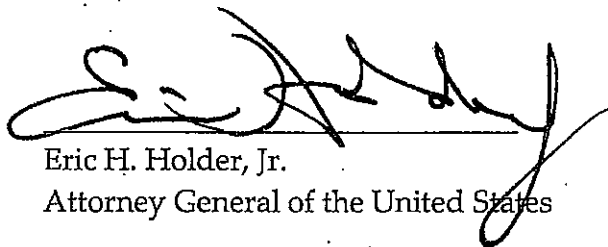
National Security Division  
United States Department of Justice~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

APPROVAL

I find that this motion regarding DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] and the amendments to their respective predecessor certifications satisfies the criteria and requirements set forth in the Foreign Intelligence Surveillance Act of 1978, as amended, and hereby approve its filing with the United States Foreign Intelligence Surveillance Court. (S)



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

---

James M. Cole  
Deputy Attorney General of the United States

~~SECRET~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED] et. al.

Docket No.

ORDER

This matter is before this Court on the motion of the United States for an order under 50 U.S.C. § 1881a(j)(2) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), extending to July 22, 2011, the time limits established by 50 U.S.C. § 1881a(i)(1)(B) and (C) for this Court to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certification [REDACTED]

[REDACTED] In entertaining the government's motion, this Court has considered the following:

1. DNI/AG 702(g) Certification [REDACTED] reauthorizes DNI/AG 702(g) Certification [REDACTED] which expires on August 19, 2011.
2. Included within DNI/AG 702(g) Certification [REDACTED] are amendments to DNI/AG 702(g) Certifications [REDACTED]. These amendments authorize the use of the minimization procedures attached as Exhibits B and E to

~~SECRET~~

Derived From:

~~Submission to the USFISC  
in Docket Number captioned above~~



DNI/AG 702(g) Certification [REDACTED] in connection with foreign intelligence information acquired in accordance with DNI/AG 702(g) Certifications [REDACTED]

3. The government submitted DNI/AG 702(g) Certification [REDACTED] and the amendments to DNI/AG 702(g) Certifications [REDACTED] to the Court on April 22, 2011.

4. By operation of 50 U.S.C. § 1881a(i)(1)(B) and (C), this Court is required to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certification [REDACTED] and the amendments to DNI/AG 702(g) Certifications [REDACTED] by May 22, 2011.

5. Based on the record presently before this Court concerning these matters, this Court will not be able to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certification [REDACTED] and the amendments to DNI/AG 702(g) Certifications [REDACTED] before May 22, 2011.

6. The government has asserted that it will be able to supplement the record concerning these matters in a manner that will aid the Court in reviewing DNI/AG 702(g) Certification [REDACTED] and the amendments to DNI/AG 702(g) Certifications [REDACTED] [REDACTED] and in making the determinations necessary to issue orders under 50 U.S.C. § 1881a(i)(3). However, the government has represented that it will not be able to supplement the record until after May 22, 2011.

~~SECRET~~

7. 50 U.S.C. § 1881a(j)(2) permits this Court, by order for reasons stated, to extend, as necessary for good cause in a manner consistent with national security, the time limit for this Court to issue orders under 50 U.S.C. § 1881a(i)(3) concerning DNI/AG 702(g) Certification [REDACTED] and the amendments to DNI/AG 702(g) Certifications [REDACTED]

8. By operation of 50 U.S.C. § 1881a(i)(5)(B), the authorization in the certification to be reauthorized, DNI/AG 702(g) Certification [REDACTED] continues beyond its stated expiration date until this Court issues an order under 50 U.S.C. § 1881a(i)(3) concerning DNI/AG 702(g) Certification [REDACTED]

Having given full consideration to these matters and the representations in the government's motion, this Court finds that there is good cause to extend the time limit for its review of DNI/AG 702(g) Certification [REDACTED] and the amendments to DNI/AG 702(g) Certifications [REDACTED] beyond May 22, 2011, and that such extension is consistent with national security.

WHEREFORE, IT IS HEREBY ORDERED that the government's motion is GRANTED; and

~~SECRET~~

IT IS FURTHER ORDERED, pursuant to 50 U.S.C. § 1881a(j)(2), that the time limit for this Court to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certification [REDACTED] and the amendments to DNI/AG 702(g) Certifications [REDACTED] is EXTENDED to July 22, 2011.

Signed \_\_\_\_\_ Eastern Time  
Date Time

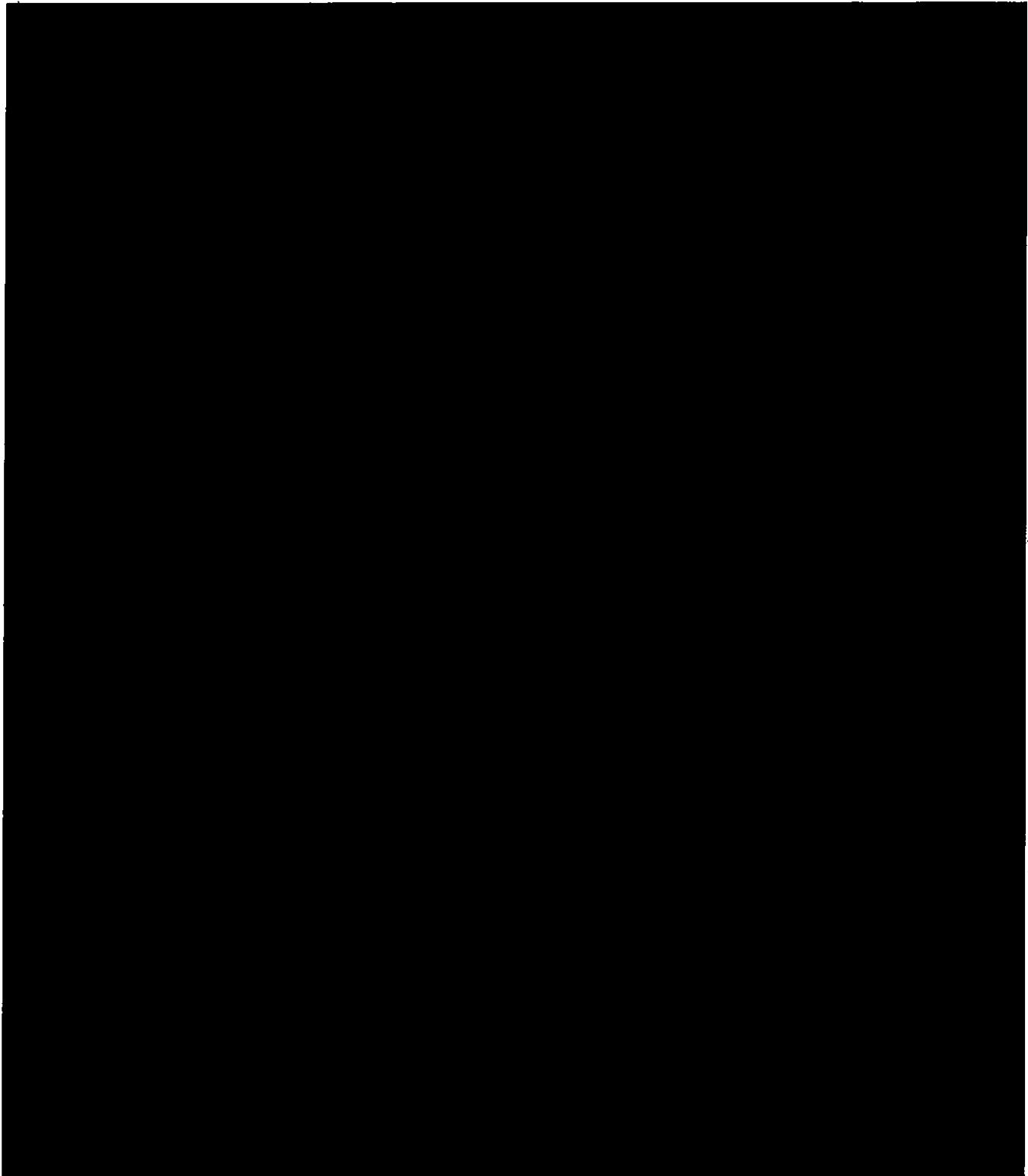
\_\_\_\_\_  
Judge, United States Foreign  
Intelligence Surveillance Court

~~SECRET~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~SECRET~~



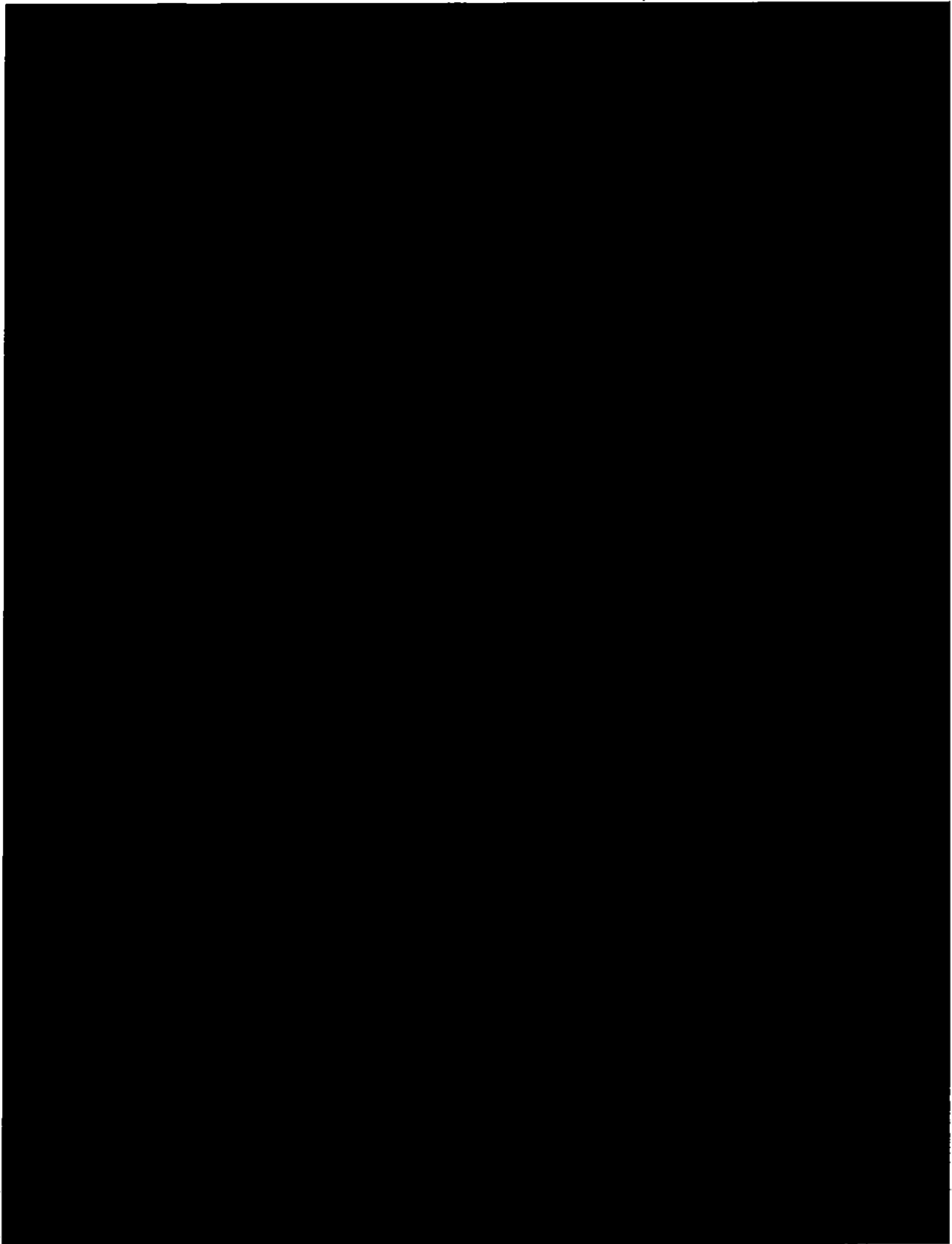
~~SECRET~~

Derived From:

~~Submission to the USFISC  
in Docket Number captioned above~~

Approved for public release.

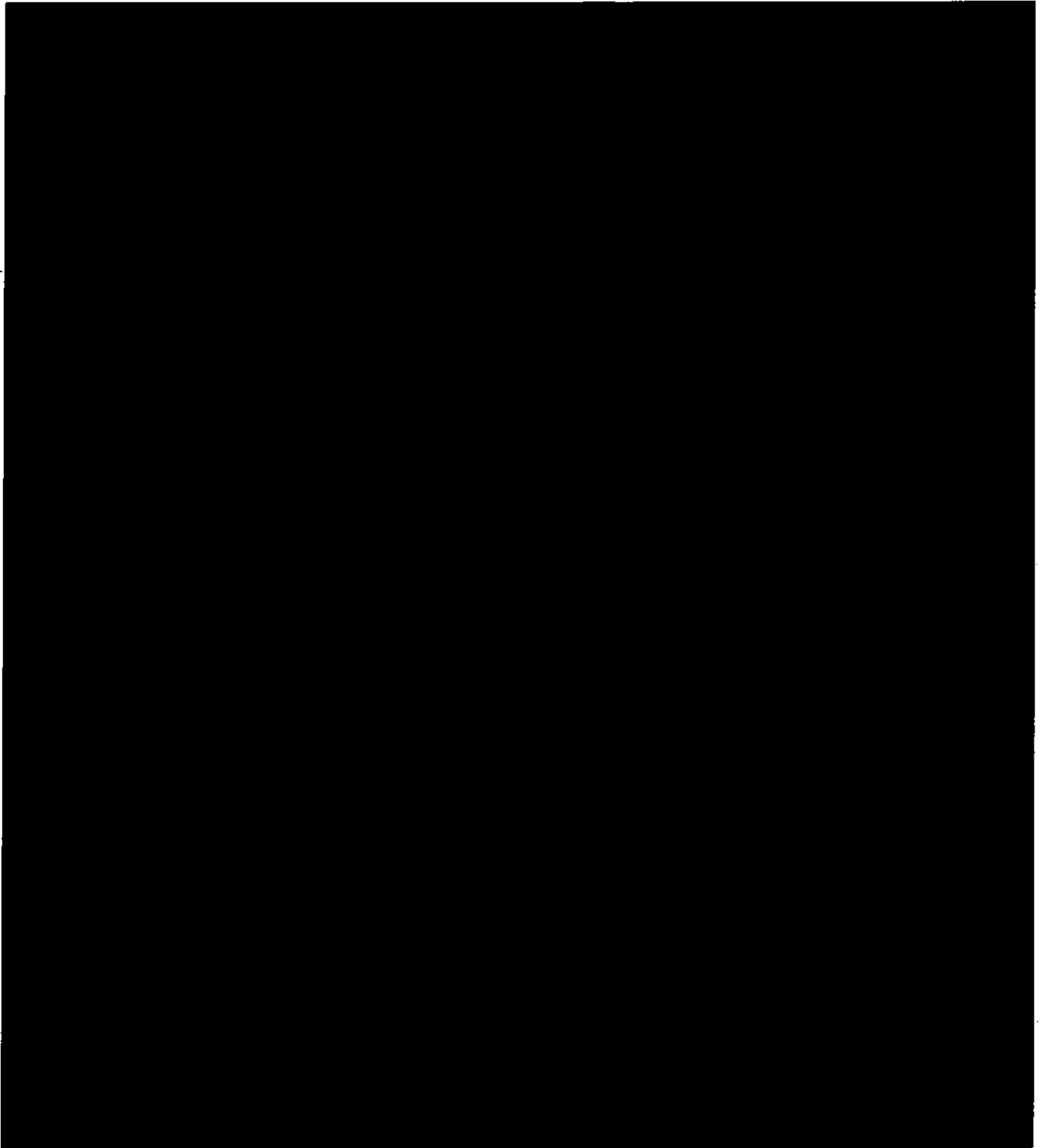
All withheld information exempt under b(1) and b(3) except as otherwise noted.



~~SECRET~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.



~~SECRET~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

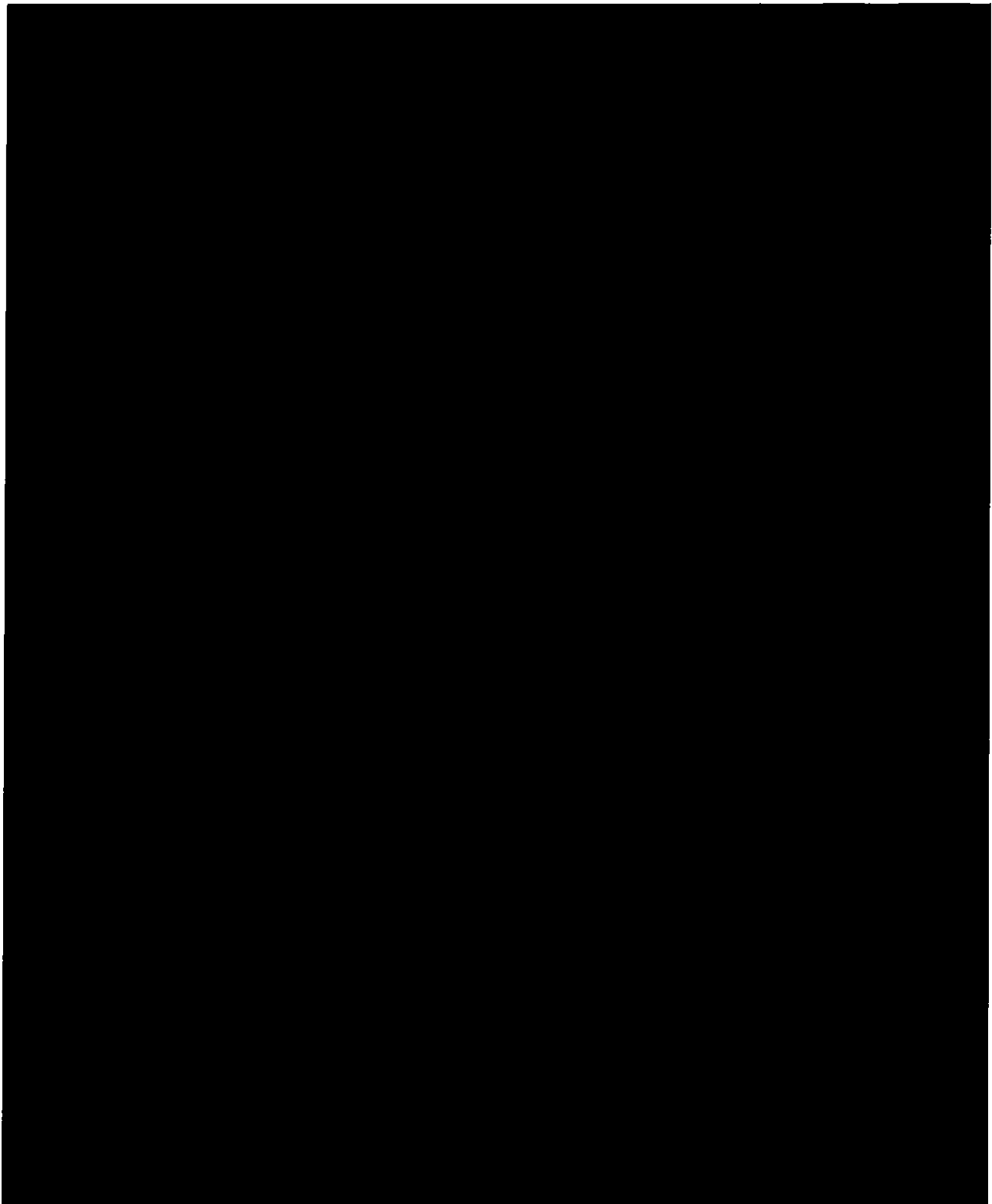


~~SECRET~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~SECRET~~



~~SECRET~~

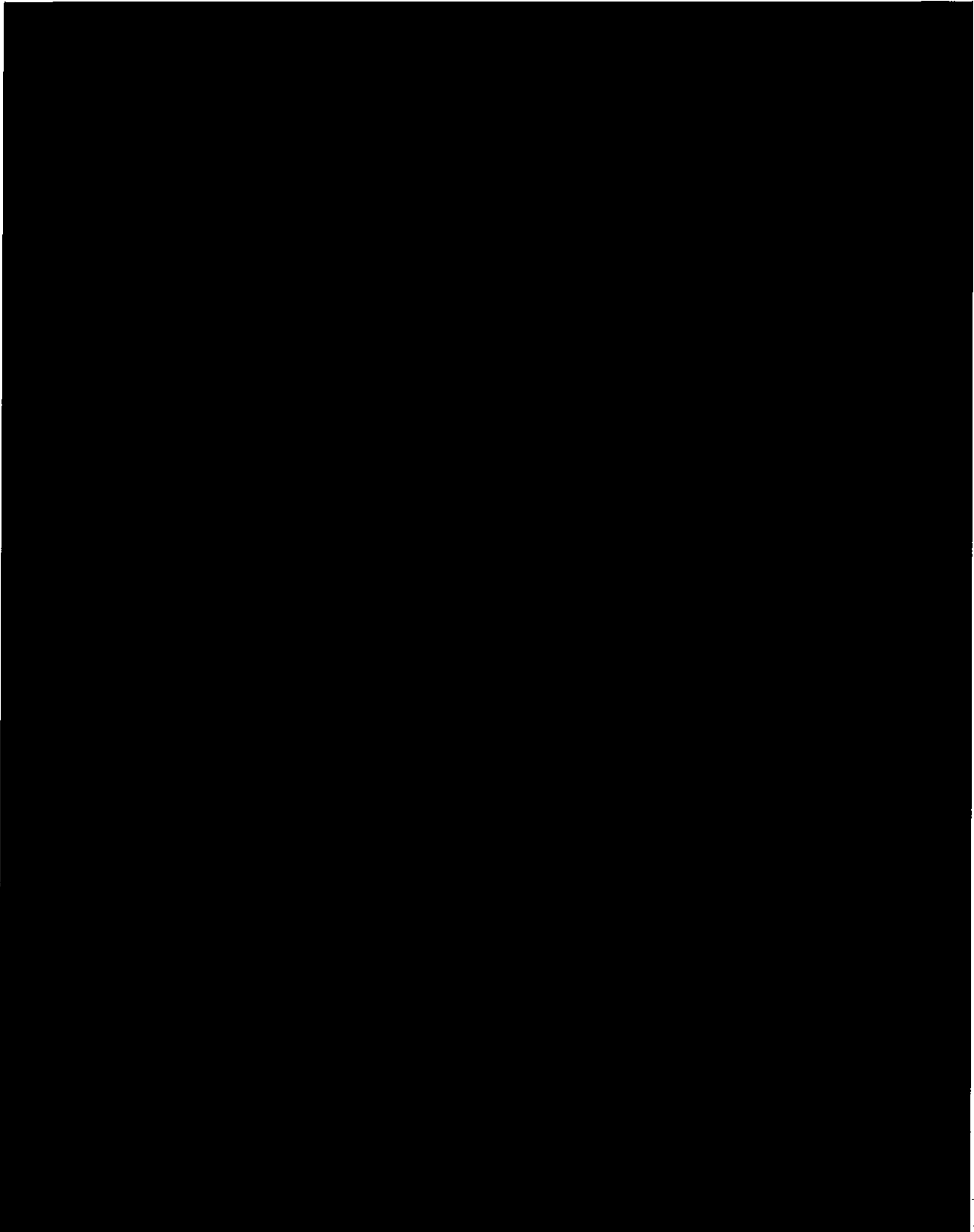
Derived From:

~~Submission to the USFISC  
in Docket Number captioned above~~



Approved for public release.

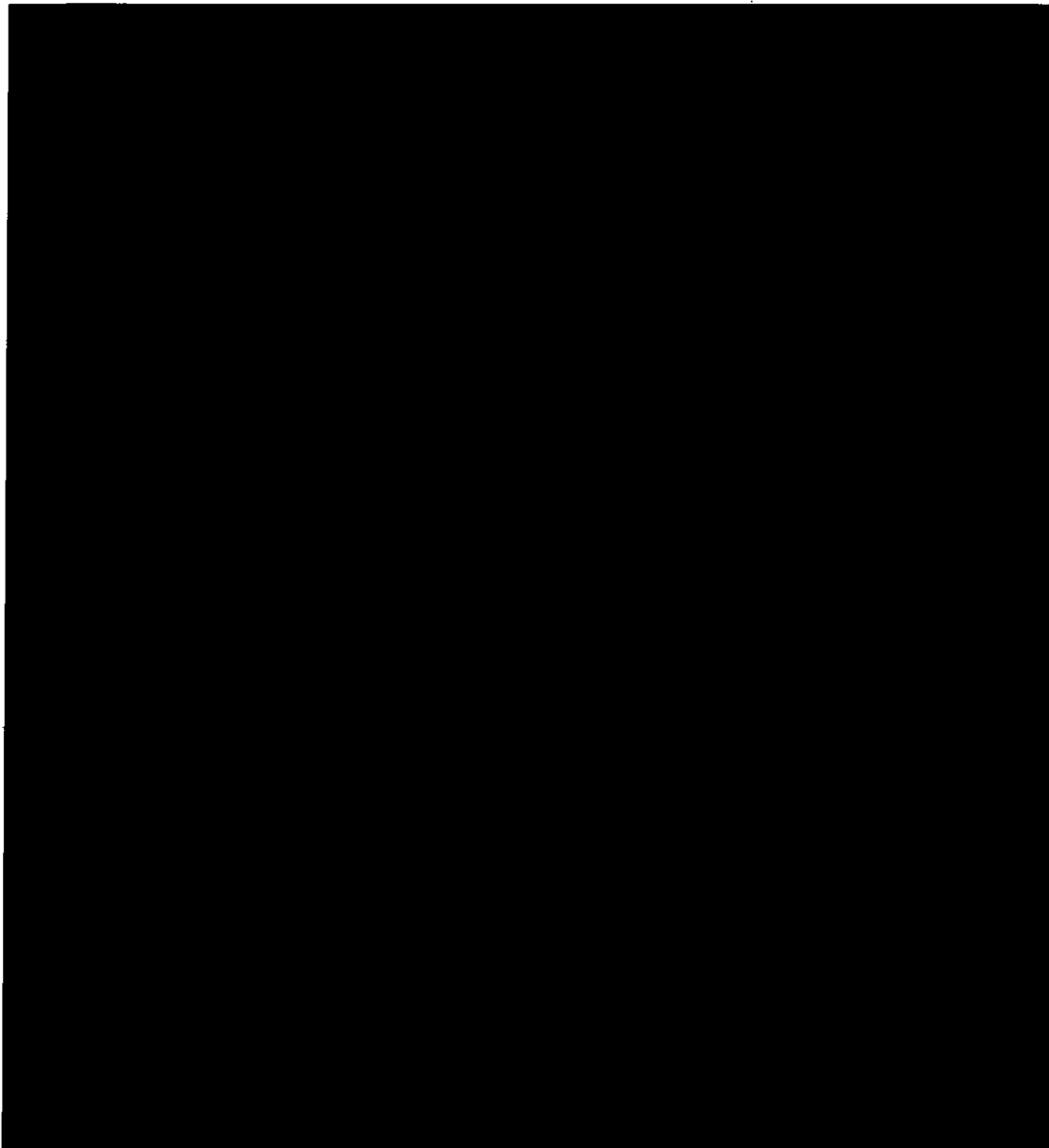
All withheld information exempt under b(1) and b(3) except as otherwise noted.



~~SECRET~~

Approved for public release.

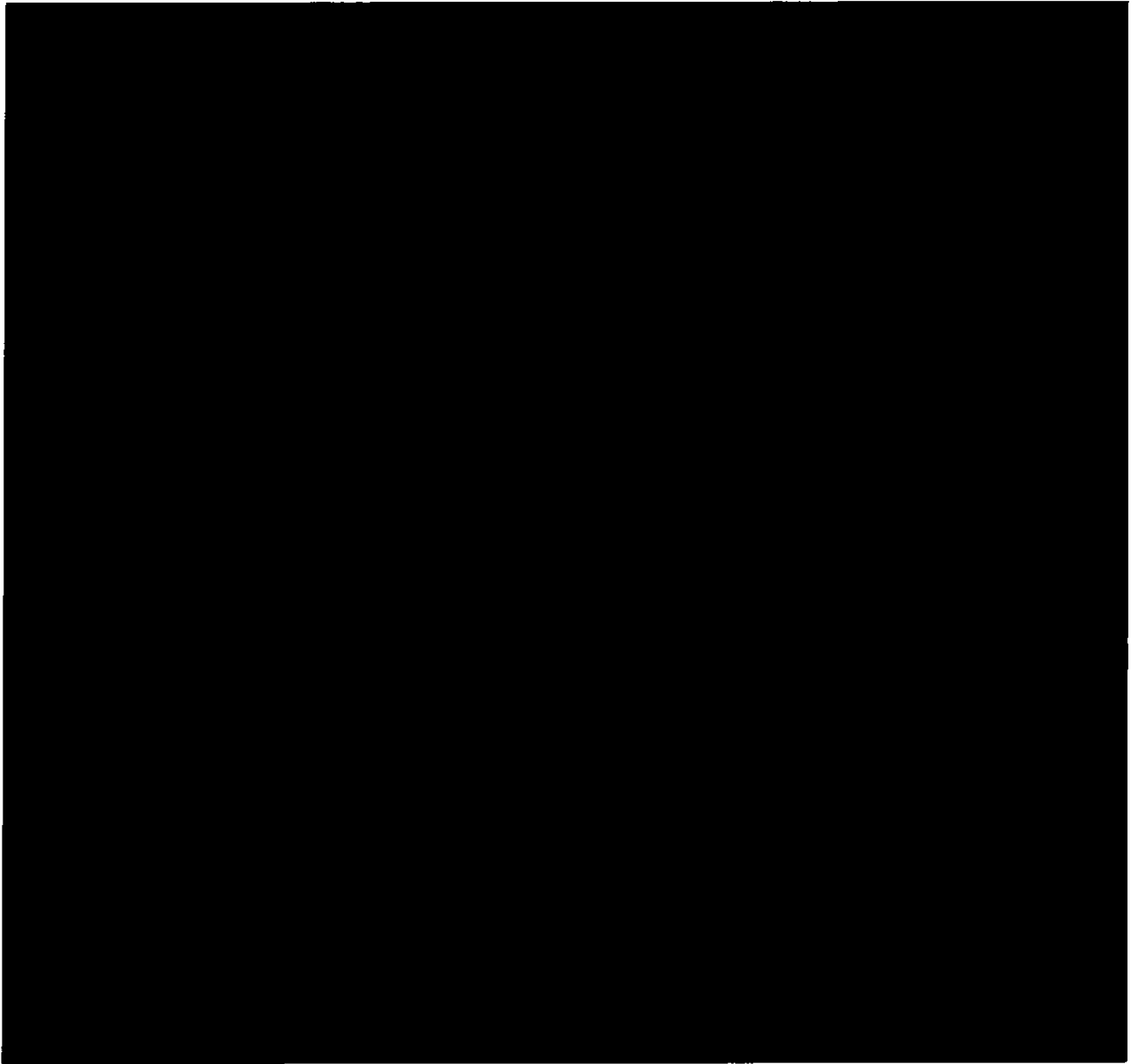
All withheld information exempt under b(1) and b(3) except as otherwise noted.



~~SECRET~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.



~~SECRET~~





\_\_\_\_\_

~~SECRET//ORCON,NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

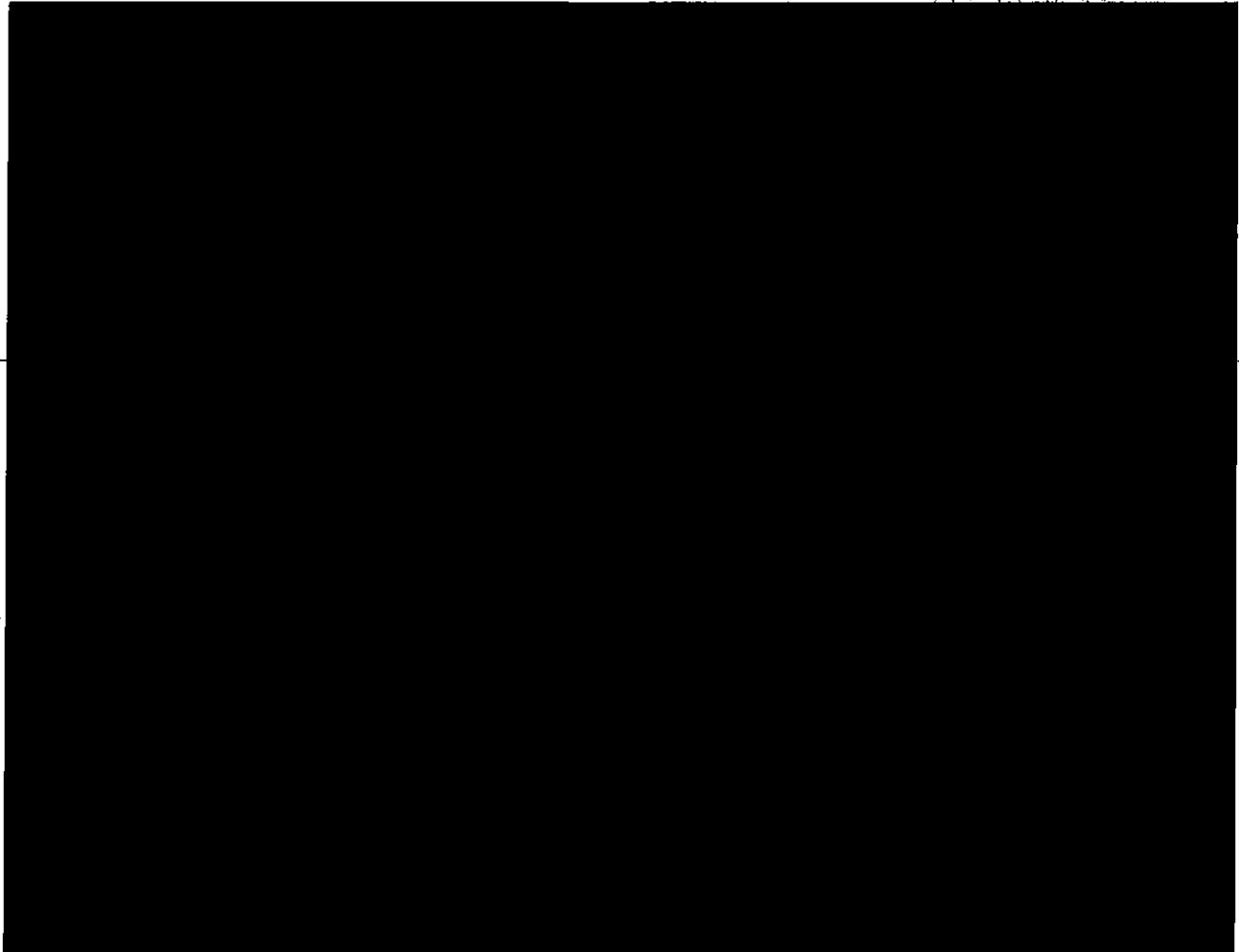
UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2011 JUN -1 PM 4:47

WASHINGTON, D.C.

LEEANN FLYNN HALL  
CLERK OF COURT



NOTICE OF FILING OF GOVERNMENT'S RESPONSE  
TO THE COURT'S BRIEFING ORDER OF MAY 9, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached factual and legal response to the

~~SECRET//ORCON,NOFORN~~

Classified by:

Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ

Reason:

1.4(c)

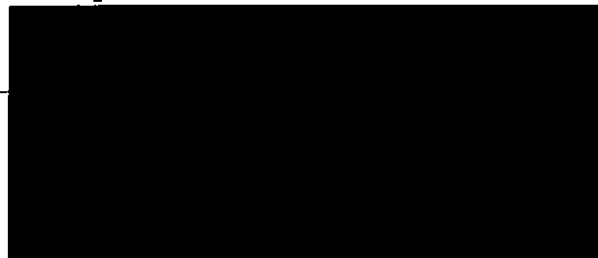
Declassify on:

1 June 2036

~~SECRET//ORCON,NOFORN~~

questions posed by this Court in its Briefing Order of May 9, 2011, concerning the above-referenced matters. The Government may seek to supplement and/or modify its response as appropriate during any hearing that the Court may hold in the above-captioned matters. (S//OC,NF)

Respectfully submitted,



National Security Division  
United States Department of Justice

~~SECRET//ORCON,NOFORN~~



~~SECRET//ORCON,NOFORN~~

VERIFICATION

I declare under penalty of perjury that the facts set forth in the attached Government's Response to the Court's Briefing Order of May 9, 2011, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 1<sup>st</sup> day of June, 2011. (S)



Signals Intelligence Directorate Compliance Architect  
National Security Agency

~~SECRET//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~GOVERNMENT'S RESPONSE TO THE  
COURT'S BRIEFING ORDER OF MAY 9, 2011

1. The government's May 2 Letter can be read to take the position that [REDACTED] [REDACTED] are communications authorized for collection under the Section 702 Certifications that have previously been approved by the Court. (TS//SI//NF)
- a. For how long has NSA been acquiring [REDACTED] through its upstream collection? (TS//SI//NF)

Under the Section 702 Certifications, NSA acquires, *inter alia*, "Internet communications." E.g., DNI/AG 702(g) Certification [REDACTED] Affidavit of General Keith B. Alexander, Director, National Security Agency (NSA), filed Apr. 20, 2011, at ¶ 4. As described by General Alexander, Internet communications "include, but are not limited to, [REDACTED]"

E.g., *id.* (TS//SI//NF)

In the context of NSA's upstream collection techniques, NSA acquires Internet communications in the form of "transactions," which in this filing refers to a complement of "packets" traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device.<sup>1</sup> A "transaction" might contain information or data representing either a discrete communication (e.g., an e-mail message), or multiple discrete communications [REDACTED]. As further described in the response to question 2 below, whenever a tasked selector is present within a transaction, NSA's "upstream" Internet collection techniques are designed to identify and acquire that transaction. (TS//SI//NF)

<sup>1</sup> While the terms "Internet communication" and "transmission" have been used to describe the types of communications NSA acquires, NSA believes that, in the context of upstream collection, "transaction" is the more precise term from a technical perspective, because "transmission" could be understood to mean all data being exchanged on the Internet within a specific time period by a specific device, and an "Internet communication" may actually contain multiple logically separate communications between or among persons. (TS//SI//NF)

The transactions discussed herein -- whether they contain single or multiple discrete communications having a commonality of a single user -- should not be confused with the two [REDACTED] compliance incidents initially reported to the Court on April 19, 2011, and further discussed below in the Government's response to question 6, which involved the [REDACTED] unrelated communications [REDACTED]

(TS//SI//NF)

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20360501

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

At the time of acquisition, NSA's upstream Internet collection devices are, with limited exceptions further described below, not presently capable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector.<sup>2</sup> Thus, in order to acquire transactions containing one or more communications to, from, or about a tasked selector, it has been necessary for NSA to employ these same upstream Internet collection techniques throughout the entire timeframe of all certifications authorized under Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter "FISA" or "the Act"), and the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007) (hereinafter "PAA"). It was also necessary for NSA to employ these upstream collection techniques to implement the electronic surveillance authorized in *In re* [REDACTED]

[REDACTED] Docket No. [REDACTED] and *In re* [REDACTED]

Docket No. [REDACTED] (TS//SI//NF)

b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: (TS//SI//NF)

i. comports with the government's representations to the Court regarding the scope of upstream collection under Section 702 and the approvals granted by the Court in reliance upon those representations in Dockets 702(i) 08-01, [REDACTED] (see, e.g., Docket No. 702(i)-08-01, Aug. 27, 2008 Hearing Transcript at 19-26, 40-41 and Sept. 4, 2008 Memorandum Opinion at 15-20, 38); (TS//SI//NF)

The Government has concluded, after a careful review of the record, that its prior representations to the Court regarding the steps NSA must take in order to acquire single, discrete communications to, from, or about a tasked selector did not fully explain all of the means by which such communications are acquired through NSA's upstream collection techniques. The Government will attempt through this filing to provide the Court with a more thorough explanation of this technically complex collection. This notwithstanding, the Government respectfully submits that for the reasons set forth in its responses to questions 2.ii.,

<sup>2</sup> Specifically, as is discussed in the Government's response to questions 2(c) and (d) of the Court's briefing order, NSA does have the ability to identify and acquire discrete communications to, from, or about a tasked selector in certain cases [REDACTED]

(TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

2.iii., and 5 below, NSA's prior and ongoing acquisition of information utilizing its upstream collection techniques is consistent with the Court's prior orders, meets the requirements of Section 702, and is consistent with the Fourth Amendment. ~~(TS//SI//NF)~~

b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: ~~(TS//SI//NF)~~

ii. meets the requirements of Section 702, including, but not limited to, the requirement that targeting procedures must be reasonably designed to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States"; and, ~~(TS//SI//NF)~~

**NSA'S TARGETING PROCEDURES ARE REASONABLY DESIGNED TO PREVENT THE INTENTIONAL ACQUISITION OF COMMUNICATIONS AS TO WHICH THE SENDER AND ALL INTENDED RECIPIENTS ARE KNOWN AT THE TIME OF ACQUISITION TO BE LOCATED IN THE UNITED STATES. (S)**

Under Section 702, the Government targets "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). The Government determines whether the targeting of a person is consistent with Section 702 by applying Court-approved targeting procedures. 50 U.S.C. § 1881a(d). These targeting procedures must be "reasonably designed to (A) ensure that any acquisition authorized under subsection [702(a)] is limited to targeting persons reasonably believed to be located outside the United States; and (B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). (U)

**A. The User of a Tasked Selector is the Person Being Targeted by all Acquisitions by NSA's Upstream Collection, Including Transactions That Contain Multiple Discrete Communications—~~(TS//SI//NF)~~**

As previously explained to the Court, the Government "targets" a person by tasking for collection a "selector" (e.g., an e-mail account) believed to be used by that person. *See, e.g., In re DNI/AG Certification* [REDACTED] Docket No. 702(i)-08-01, Mem. Op. at 8 (USFISC Sept. 4, 2008) (hereinafter "[REDACTED] Mem. Op."). NSA acquires foreign intelligence information through the tasking of selectors by collecting communications to or from a selector used by a targeted person (hereinafter "to/from communications") and by collecting communications that refer to or are about a selector used by a targeted person (hereinafter "abouts communications"). *Id.*

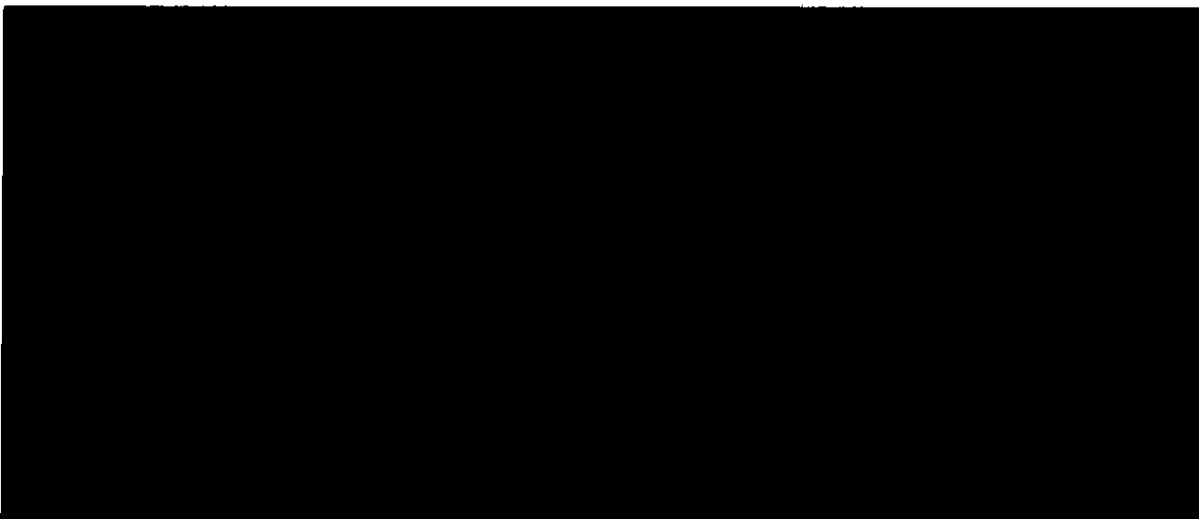
~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

In both of these types of acquisition, the person being "targeted" is the user of the tasked selector, who, by operation of the targeting procedures, is a non-United States person reasonably believed to be located outside the United States. Specifically, "the persons targeted by acquisition of to/from communications are the users of the tasked selectors," because "their communications are intentionally selected for acquisition." [REDACTED] Mem. Op. at 15. Similarly, the person being targeted by acquisition of abouts communications is also the user of the tasked selector, "because the government's purpose in acquiring about communications is to obtain information about that user." *Id.* at 18 (citation omitted). (TS//SI//NF)

This remains true for all acquisitions conducted by NSA's upstream collection -- including transactions containing several discrete communications, only one of which may be to, from, or about the user of a tasked selector. As discussed above, the fact that there also may be communications to, from, or about persons other than the target in the transaction does not mean that those persons are also being targeted by the acquisition. The sole reason a transaction is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been subjected to NSA's targeting procedures.<sup>3</sup> Indeed, at the time a transaction is acquired, NSA cannot always know whether the transaction includes other data or information representing communications that are not to, from, or about the target, let alone always have knowledge of the parties to those communications. *Cf.* [REDACTED] Mem. Op. at 18-19 (noting that with respect to abouts communications, "the government may have no knowledge of [the parties to a communication] prior to acquisition"). It therefore cannot be said that the acquisition of a transaction containing multiple discrete communications results in the intentional targeting of any of the parties to those communications other than the user of the tasked selector. *Cf. United States v. Bin Laden*, 126 F. Supp. 2d 264, 281 (S.D.N.Y. 2000), *aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008), *cert. denied sub nom. El-Hage v. United States*, 130 S.Ct. 1050 (2010) (acknowledging that in light of *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990), and Title III "incidental interception" case law, overseas surveillance of a United States person terrorism suspect would have posed no Fourth Amendment problem "if the Government had not been aware of [his] identity or of his complicity in the [terrorism] enterprise"). (TS//SI//OC,NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

**B. NSA's Targeting Procedures are Reasonably Designed to Prevent the Intentional Acquisition of Communications as to Which the Sender and All Intended Recipients Are Known at the Time of Acquisition to be in the United States (S)**

In conducting acquisitions targeting the user of a tasked selector, the Government "may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a(b)(4). As noted above, the targeting procedures must be reasonably designed to prevent such intentional acquisitions. With respect to to/from communications, "because a user of a tasked selector is a party to every to/from communication acquired by NSA, a reasonable belief that the users of tasked selectors are outside the United States will ensure that NSA does not intentionally acquire any to/from communication 'as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.'" [REDACTED] Mem. Op. at 15 (citation omitted). With respect to upstream collection that may contain abouts communications, NSA's targeting procedures provide that:

[REDACTED]

4

E.g., Amendment 1 to DNI/AG 702(g) Certification [REDACTED] Docket No. 702(i)-[REDACTED] Ex. A, filed Aug. 12, 2010, at 1-2 (hereinafter "NSA Targeting Procedures"). Although these provisions on their face suggest separate technical means might apply only to the "abouts" aspect of NSA's upstream collection, in practice these provisions currently apply to any Internet transaction collected upstream. (TS//SI//OC,NF)

The Government has previously represented that "the operation of the IP address filters or [REDACTED] prevents the intentional acquisition of communications 'about' the target as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." *In re DNI/AG 702(g) Certification* [REDACTED] Docket No. 702(i)-08-01, Government's Preliminary Response to Questions Posed by the Court, filed Aug. 26, 2008, at 3. The Government also has represented that these IP filters "have been effective in limiting the collection to communications with at least one communicant located outside the United States."

<sup>4</sup> This provision has remained identical throughout every set of NSA's Section 702 targeting procedures approved for use by the Court, and is also the same in the proposed targeting procedures submitted with DNI/AG 702(g) Certifications [REDACTED] (S//OC,NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

*Id.* at 4. Except in one circumstance previously reported to the Court,<sup>5</sup> the Government is not aware of a case where an about collection resulted in the acquisition of a communication where both ends were inside the United States. NSA therefore continues to believe that these prior representations remain accurate. Accordingly, for the reasons described below, the Government respectfully submits that NSA's targeting procedures are reasonably designed to prevent, in the context of NSA's upstream collection, "the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States," including Internet communications [REDACTED] that have not been previously described to the Court. 50 U.S.C. § 1881a(d)(1)(B). ~~(TS//SI//OC,NF)~~

### 1. How NSA's IP Filters Work (S)

NSA acquires Internet communications by collecting the individual packets of data that make up those communications. [REDACTED]

~~(TS//SI//OC,NF)~~

5

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

6

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

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

(TS//SI//OC,NF)

[REDACTED]

Additionally, at the time of acquisition, NSA's upstream Internet collection devices are, with limited exceptions further described below, not presently capable of distinguishing transactions containing only a single discrete communication to, from or about a targeted selector from transactions containing multiple discrete communications.<sup>7</sup> Accordingly, NSA cannot prevent the acquisition of, or even mark for separate treatment, those types of transactions that may feature multiple discrete communications [REDACTED]. (TS//SI//OC,NF)

[REDACTED]


<sup>7</sup> See Government's response to questions 2(c) and (d) *infra*. (U)


[REDACTED]

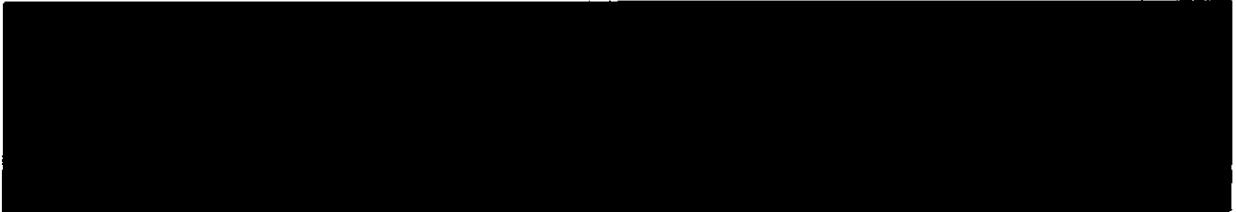
(TS//SI//NF)


~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~  
<sup>10</sup> ~~(TS//SI//OC,NF)~~

Except for the one instance noted above concerning an error by an electronic communication service provider, NSA is not aware of any instance in which its upstream collection on  or are subject to an IP filter nevertheless resulted in the acquisition of a communication as to which the sender and all intended recipients were known at the time of acquisition to be located in the United States.<sup>11</sup> This includes those situations in which NSA might collect unrelated communications when acquiring Internet communications that include multiple, discrete communications. ~~(TS//SI//NF)~~

  
~~(TS//SI//OC,NF)~~  
~~(TS//SI//OC,NF)~~

<sup>11</sup> It is noteworthy that the provider error that resulted in the acquisition of domestic communications was first identified not by the provider, but by an NSA analyst who recognized a domestic communication in NSA's repositories, realized that such a domestic communication should not have been acquired, and properly reported the communication through NSA channels. NSA investigated this matter and found that domestic communications had been acquired not due to any theoretical limitations in its IP filter technology, but instead because . The domestic overcollection caused by this incident represented a very small portion of NSA's collection during the time period of the overcollection, and an even smaller portion of NSA's collection since the initiation of its Section 702 acquisitions, but the error was still discovered and remedied. It is therefore particularly noteworthy that no NSA analyst has otherwise yet discovered a wholly domestic communication in NSA's repositories collected through NSA's upstream collection systems.

~~(TS//SI//OC,NF)~~~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

In May 2011, NSA conducted two tests of its Section 702 upstream collection in order to determine the likelihood of collecting an Internet transaction between a user in the United States and [REDACTED]. The first test included [REDACTED]

The second test included [REDACTED]

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

The first test sample included no records where both the sender and receiver IP addresses were in the United States [REDACTED]

[REDACTED] NSA analysis further revealed that only [REDACTED] of the more than [REDACTED] (0.028%) had characteristics consistent with a person in the United States accessing a [REDACTED]

[REDACTED] For the second dataset, NSA analysis discovered that only [REDACTED] out of more than [REDACTED] total records (0.0016%) included a non-targeted user likely accessing the Internet from an IP address in the United States. [REDACTED]

[REDACTED] NSA assesses, based on analysis of the underlying data, that this activity in fact was [REDACTED] copies of the same Internet transaction, [REDACTED]

[REDACTED] There is no indication that NSA collected any wholly domestic communications through its acquisition of this transaction.

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

In sum, the Government submits that the two test samples discussed above, coupled with the fact that, except as noted above, no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication collected through NSA's upstream collection systems, strongly suggests that NSA's acquisition of transactions or single Internet communications between users in the United States and [REDACTED] currently occurs only in a very small percentage of cases. Even those rare cases, moreover, won't necessarily involve a user in the United States receiving from the [REDACTED] a transaction containing a communication from a person known at the time of acquisition to be located in the United States.<sup>12</sup> ~~(TS//SI//NF)~~

<sup>12</sup> Additionally, as discussed elsewhere herein, even if the sender is located in the United States, the communication likely will not contain any reliable information that would enable NSA to determine at the time of acquisition the sender's location. ~~(TS//SI//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

2. The [REDACTED] Means by Which NSA Prevents the Intentional Acquisition of Communications as to Which the Sender and All Intended Recipients Are Known to be Located In the United States at the Time of Acquisition Are Reasonable (S)

This Court has found that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications in which the sender and all intended recipients are known at the time of acquisition to be located in the United States. In approving DNI/AG 702(g) Certification [REDACTED], with respect to NSA's upstream collection of "abouts" communications, in particular, the Court noted that NSA "relies on [REDACTED] means of ensuring that at least one party to the communication is located outside the United States." [REDACTED] Mem. Op. at 19. As described above, those [REDACTED] means are NSA's use of "an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas" and NSA's [REDACTED] NSA Targeting Procedures at 1-2; *see also* [REDACTED] Mem. Op. at 19. Relying on the Government's representations that these [REDACTED] means had prevented the acquisition of wholly domestic communications under the PAA, and recognizing that it is "theoretically possible that a wholly domestic communication could be acquired as a result of the [REDACTED]" the Court found that these [REDACTED] means were "reasonably designed to prevent the intentional acquisition of communications as to which all parties are in the United States." [REDACTED] Mem. Op. at 20 & n.17. The Government respectfully submits that there is no aspect of NSA's upstream collection, as further described herein, that would prevent the Court from continuing to find that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be in the United States.

~~(TS//SI//OC,NF)~~

Two aspects of NSA's upstream collection activity that have not been specifically addressed by the Court are discussed herein: first, the fact that NSA acquires some communications [REDACTED]

[REDACTED] and second, the fact that NSA could acquire [REDACTED] -- whether retrieving a single, discrete communication, or a transaction containing several discrete communications -- possibly resulting in the acquisition of wholly domestic communications. ~~(TS//SI//OC,NF)~~

a. Acquisition of Communications that [REDACTED]

(S)

First, [REDACTED]

[REDACTED] -- NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

States. [REDACTED]

~~(TS//SI//OC,NF)~~**b. Theoretical Acquisition of Wholly Domestic Communications Through**~~(TS//SI//NF)~~

With respect to the above-discussed theoretical cases in which NSA could acquire a [REDACTED] NSA's targeting procedures also are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. As discussed above, NSA assesses that [REDACTED]

[REDACTED] only in a minute percentage of cases. Yet even in those rare cases, there would be no way for NSA to know at the time of acquisition that the sender and intended recipient are located in the United States. [REDACTED]

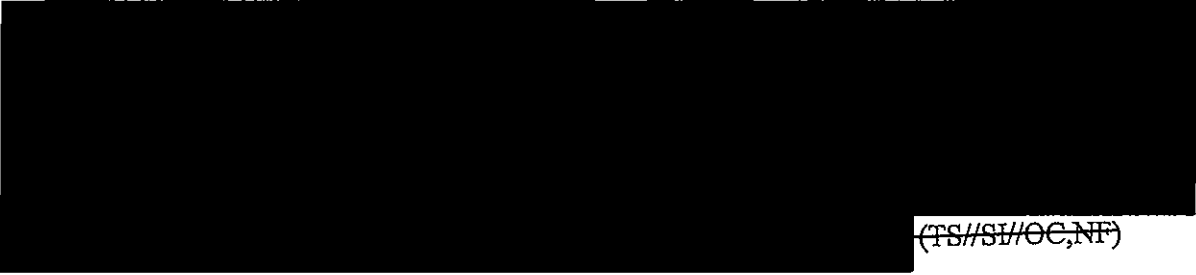
[REDACTED] NSA cannot at that point know the location of the intended recipient, who has yet to receive the message. Likewise, [REDACTED]

[REDACTED] it is highly unlikely that the communication would contain information useful in determining the sender's true location.<sup>13</sup> In any event, it is currently not possible for NSA's IP filters to [REDACTED]

[REDACTED] Because NSA's filters will be looking at the best available information, [REDACTED] it cannot be said that the sender and all intended recipients of those communications are known at the time of acquisition to be located in the United States. Similarly, in the case of NSA's [REDACTED]


13 [REDACTED]

~~(TS//SI//OC,NF)~~~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~  
(TS//SI//OC,NF)

Accordingly, NSA has designed its systems so that it should never intentionally acquire a communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. To the extent that NSA does unintentionally acquire such communications, NSA must treat those communications in accordance with its minimization procedures -- just as it must for other types of communications that it is prohibited from intentionally collecting under subsection 702(b), but nevertheless sometimes does unintentionally acquire, such as communications acquired from a target while that target is located inside the United States. (TS//SI//OC,NF)

**c. Conclusion (U)**

Although for different reasons than those discussed above, the Court has recognized that it is "theoretically possible that a wholly domestic communication could be acquired" through NSA's upstream collection of "abouts" communications.  Mem. Op. at 20 n.17. For the reasons outlined above, the Government respectfully submits that, despite the theoretical scenarios under which NSA could acquire communications through its upstream collection as to which the sender and all intended recipients are located in the United States, NSA's targeting procedures are reasonably designed to prevent such acquisitions where the location of the sender and all intended recipients is known at the time of acquisition. (TS//SI//OC,NF)

*The remainder of this page intentionally left blank.*

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: ~~(TS//SI//NF)~~

iii. is consistent with the Fourth Amendment. ~~(TS//SI//NF)~~

**NSA's ACQUISITION OF TRANSACTIONS CONTAINING MULTIPLE DISCRETE COMMUNICATIONS IS CONSISTENT WITH THE FOURTH AMENDMENT.**  
(TS//SI//NF)

Section 702 requires the Attorney General (AG) and the Director of National Intelligence (DNI) to execute a certification attesting, among other things, that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(A)(iv). In reviewing a certification, Section 702 in turn requires the Court to enter an order approving the certification and the use of the targeting and minimization procedures if the Court finds, among other things, that those procedures are consistent with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A). The issue for the Court in light of the above-described nature and scope of NSA's upstream collection is whether, in light of a governmental interest "of the highest order of magnitude," NSA's targeting and minimization procedures sufficiently protect the individual privacy interests of United States persons whose communications are inadvertently acquired. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008) (hereinafter "*In re Directives*"). ~~(TS//SI//NF)~~

The Fourth Amendment protects the right "to be secure . . . against unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As demonstrated below, the Fourth Amendment requires no warrant here, and the upstream collection conducted by NSA is a reasonable exercise of governmental power that satisfies the Fourth Amendment. ~~(TS//SI//NF)~~

**A. The Warrant Requirement Does Not Apply to NSA's Acquisition of Transactions Containing Multiple Discrete Communications.** ~~(TS//SI//NF)~~

The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotations omitted); *see also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (quoting *Griffin*). The Foreign Intelligence Surveillance Court of Review, in upholding the Government's implementation of the PAA, held that a foreign intelligence exception exists "when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

believed to be located outside the United States." *In re Directives*, 551 F.3d at 1012. See also *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002) ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). ~~(TS//SI//NF)~~

In approving a previous Section 702 certification, this Court has found that Section 702 acquisitions "fall within the exception recognized by the Court of Review" in that they "target persons reasonably believed to be located outside the United States who will have been assessed by NSA to possess and/or to be likely to communicate foreign intelligence information concerning a foreign power authorized for acquisition under the Certification" and are "conducted for national security purposes." ~~██████████~~ Mem. Op. at 35 (citations omitted). Specifically, this Court recognized that the Court of Review's rationale for applying a foreign intelligence exception "appl[ies] with equal force" to Section 702 acquisitions, in that the Government's purpose in conducting Section 702 acquisitions goes well beyond a normal law enforcement objective and involves "the acquisition from overseas foreign agents of foreign intelligence to help protect national security," a circumstance "in which the government's interest is particularly intense." *Id.* at 35-36 (quoting *In re Directives*, 551 F.3d at 1011). In addition, this Court, noting the likely volume of Section 702 acquisitions and the fact that those acquisitions involve targets who are attempting to conceal their communications, found that "[s]ubjecting ~~██████████~~ number of targets to a warrant process inevitably would result in delays and, at least occasionally, in failures to obtain perishable foreign intelligence information, to the detriment of national security." ~~██████████~~ Mem. Op. at 36; see also *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) ("attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy" such that "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, [and] in some cases delay executive response to foreign intelligence threats..."). The Court's previous finding that the foreign intelligence exception applies to Section 702 acquisitions remains equally applicable here. ~~(TS//SI//NF)~~

**B. NSA's Acquisition of Transactions Containing Multiple Discrete Communications is Reasonable Under the Fourth Amendment.** ~~(TS//SI//NF)~~

Where, as here, the foreign intelligence exception applies, "governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement." *In re Directives*, 551 F.3d at 1012. In evaluating the reasonableness of the Government's action, a court must consider the totality of the circumstances, see *United States v. Knights*, 534 U.S. 112, 118 (2001), taking into account "the nature of the government intrusion and how the intrusion is implemented." *In re Directives*, 551 F.3d at 1012 (citing *Tennessee v. Garner*, 471 U.S. 1, 8 (1985) and *United States v. Place*, 462 U.S. 696, 703 (1983)). In balancing these interests, the Court of Review has observed that "[t]he more important the government's interest, the greater the intrusion that may be constitutionally tolerated." *In re Directives*, 551 F.3d at 1012 (citing *Michigan v. Summers*, 452 U.S. 692, 701-05 (1981)). "If the protections that are in place for individual privacy interests are sufficient in light of the governmental interests at stake, the constitutional scales will tilt in favor of upholding the government's actions." *Id.* ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

**1. NSA's Acquisition of Transactions Containing Multiple Discrete Communications Implicates Fourth Amendment-Protected Interests.**

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

Although targeting under Section 702 is limited to non-United States persons reasonably believed to be located outside the United States, who are not entitled to protection under the Fourth Amendment, *see, e.g.*, [REDACTED] Mem. Op. at 37, this Court has recognized that conducting acquisitions under Section 702 creates a "real and non-trivial likelihood of intrusion on Fourth Amendment-protected interests" of United States persons or persons located in the United States who, for example, communicate directly with a Section 702 target, *id.* at 38.<sup>14</sup> In particular, as described herein, NSA's upstream collection may incidentally acquire information concerning United States persons within transactions containing multiple discrete communications, only one of which is to, from, or about a person targeted under Section 702. ~~(TS//SI//NF)~~

**2. The Government's Interest in the Foreign Intelligence Information Contained in All Transactions, Including Those Containing Multiple Discrete Communications, is Paramount. ~~(TS//SI//NF)~~**

On the other side of the ledger, it is axiomatic that the Government's interest in obtaining foreign intelligence information to protect the Nation's security and conduct its foreign affairs is paramount. *See, e.g., Haig v. Agee*, 453 U.S. 280, 307 (1981) ("[I]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." (citations omitted)). Equally indisputable is the Government's interest in conducting acquisitions of foreign intelligence information<sup>15</sup> under Section 702 of the Act. *See* [REDACTED] Mem. Op. at 37

<sup>14</sup> Although the scope of Fourth Amendment protection for e-mail is not settled, the Government has argued before this Court that United States persons have a reasonable expectation of privacy in the content of such electronic communications. *See, e.g., United States of America's Supplemental Brief on the Fourth Amendment*, Docket No. 105B(g) 07-01, filed Feb. 15, 2008, at 1. The Government likewise assumes for purposes of this filing that the collection of [REDACTED] implicates privacy interests protected by the Fourth Amendment. ~~(TS//SI//NF)~~

<sup>15</sup> "Foreign intelligence information" is defined as:

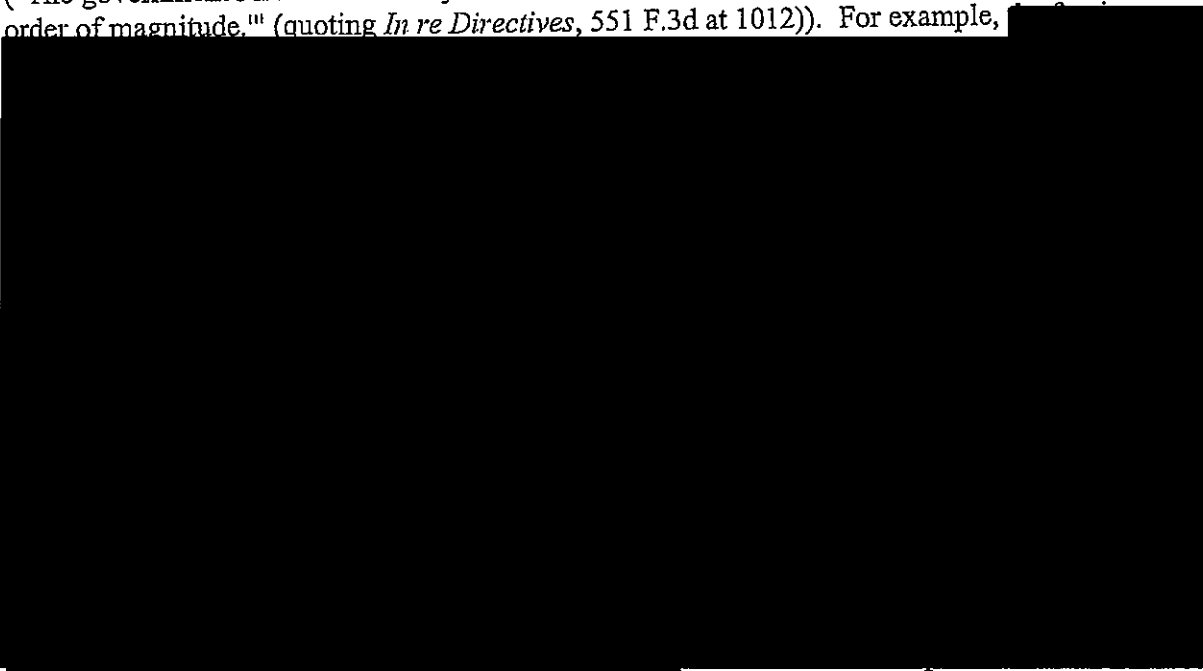
- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against --
  - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
  - (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
  - (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to --
  - (A) the national defense or the security of the United States; or
  - (B) the conduct of the foreign affairs of the United States.

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

("The government's national security interest in conducting these acquisitions 'is of the highest order of magnitude.'" (quoting *In re Directives*, 551 F.3d at 1012)). For example,

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

The Supreme Court has indicated that in addition to examining the governmental interest at stake, some consideration of the efficacy of the search being implemented -- that is, some measure of fit between the search and the desired objective -- is also relevant to the reasonableness analysis. *See, e.g., Knights*, 534 U.S. at 119 (noting that the reasonableness of a search "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which [the search] is needed for the promotion of legitimate governmental interests." (internal quotation marks omitted)); *see also Board of Educ. v. Earls*, 536 U.S. 822, 834 (2002) ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them.")). Here, NSA's acquisition of transactions through upstream collection is an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount governmental interest of protecting the Nation and conducting its foreign affairs.

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

The AG and DNI have attested that a significant purpose of all acquisitions under Section 702, which includes those conducted by NSA's upstream collection, is to obtain foreign intelligence information. These acquisitions are conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed "toward communications that are likely to yield the foreign intelligence information sought, and thereby

---

50 U.S.C. § 1801(e). (U)~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

afford a degree of particularity that is reasonable under the Fourth Amendment." [REDACTED] Mem. Op. at 39-40 (footnote omitted). Indeed, certain of the valuable foreign intelligence information NSA seeks to acquire through upstream collection of transactions simply cannot be acquired by any other means. (TS//SI/NF)

Specifically, as this Court has recognized, NSA's upstream collection "is particularly important because it is *uniquely capable* of acquiring certain types of targeted communications containing valuable foreign intelligence information," such as [REDACTED]

[REDACTED]  
Such foreign intelligence information is particularly useful, for example, [REDACTED]

<sup>16</sup> In

<sup>16</sup> More specifically, during the course of the Court's consideration of DNI/AG 702(g) Certification [REDACTED] the Government explained the unique value of NSA's [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

addition, NSA's upstream collection enables NSA to acquire foreign intelligence information from [REDACTED]

[REDACTED] All of these types of communications are intercepted in transactions acquired through NSA's upstream collection. Valuable foreign intelligence information such as this simply cannot be obtained by means other than the acquisition of transactions through NSA's upstream collection. (TS//SI//NF)

**3. The Acquisition of Foreign Intelligence Information Contained in Transactions is Conducted Using the Least Intrusive Means Available.**

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

The fact that NSA's upstream collection acquires transactions that may contain several discrete communications, only one of which is to, from, or about a tasked selector, does not render NSA's upstream collection unreasonable. See *In re Directives*, 551 F.3d at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted); see also *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful [Title III] surveillance is not violative of the Fourth Amendment."); cf. *Scott v. United States*, 436 U.S. 128, 140 (1978) (recognizing that "there are surely cases, such as the one at bar [involving a Title III wiretap], where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable"). Indeed, the Supreme Court has repeatedly rejected suggestions that reasonableness requires "the least intrusive search practicable." *City of Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010) (quotation marks omitted); see, e.g., *Earls*, 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers." (internal quotation marks omitted)); *Vernonia*, 515 U.S. at 663 ("We have repeatedly refused to declare

[REDACTED]

[REDACTED] (TS//SI//OC,NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." (TS//SI//NF)

Although not demanded by the Fourth Amendment, NSA is nevertheless conducting "the least intrusive search practicable" when it acquires a single transaction which may contain several discrete communications, only one of which may contain foreign intelligence information because it is to, from, or about a tasked selector. [REDACTED]

[REDACTED] Accordingly, at the time of acquisition, NSA generally cannot know whether a transaction contains only a single communication to, from, or about a tasked selector, or whether that transaction contains that single communication along with several other communications.<sup>17</sup> [REDACTED]

[REDACTED] also render the information technologically infeasible for NSA's upstream collection systems to extract only the discrete communication that is to, from, or about a tasked selector. The only way to obtain the foreign intelligence information contained within that discrete communication, therefore, is to acquire the entire transaction in which it is contained. The fact that other, non-pertinent information within the transaction may also be incidentally and unavoidably acquired simply cannot render the acquisition of the transaction unreasonable. See *United States v. Wuagneux*, 683 F.2d 1343, 1352-53 (11th Cir. 1982) (observing that "a search may be as extensive as reasonably required to locate the items described in the warrant," and on that basis concluding that it was "reasonable for the agents [executing the search] to remove intact files, books and folders when a particular document within the file was identified as falling within the scope of the warrant"); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence sought may be seized"). (TS//SI//NF)

At the same time, NSA is making every reasonable effort to ensure that its upstream collection acquires this singularly valuable foreign intelligence information in a manner that minimizes the intrusion into the personal privacy of United States persons to the greatest extent possible. As discussed above, these acquisitions are conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed only "toward communications that are likely to yield the foreign intelligence information sought." [REDACTED] Mem. Op. at 39-40 (footnote omitted). The application of the targeting procedures further ensures that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that United States person information will be obtained." [REDACTED] Mem. Op. at 23; cf. *In re Directives*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC April 25, 2008) (recognizing that "the vast majority of persons who are located overseas are non United States persons and that most of their communications are with other, non-United States persons, who are located overseas") (footnote omitted), *aff'd*, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008). Lastly, to the extent that United States person information is incidentally acquired in the acquisition of a whole transaction by NSA's upstream collection,

<sup>17</sup> See Government's response to questions 2(c) and (d) *infra*. (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

such information will be handled in accordance with strict minimization procedures, as discussed in more detail below. ~~(TS//SI//NF)~~

**4. United States Person Information Acquired Incidentally Through NSA's Acquisition of Transactions Containing Multiple Discrete Communications is Protected by NSA's Section 702 Minimization Procedures.** ~~(TS//SI//NF)~~

As discussed above, the fact that NSA's upstream collection may result in the incidental acquisition of communications of United States persons cannot, by itself, render the overall collection unreasonable. Instead, courts have repeatedly found support for the constitutionality of foreign intelligence activities resulting in the incidental acquisition of United States person information in the existence and application of robust minimization procedures. *See, e.g., In re Directives*, 551 F.3d at 1015 (recognizing that minimization procedures are a "means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons");

~~Mem. Op. at 40 (concluding that minimization procedures meeting the definition in 50 U.S.C. § 1801(h)(1) "constitute a safeguard against improper use of information about United States persons that is inadvertently or incidentally acquired, and therefore contribute to the Court's overall assessment that the targeting and minimization procedures are consistent with the Fourth Amendment").~~ As explained below, NSA's current Section 702 minimization procedures, which this Court previously has found to satisfy the definition of minimization procedures in 50 U.S.C. § 1801(h)(1),<sup>18</sup> adequately protect the privacy interests of United States persons whose communications may be incidentally acquired through NSA's upstream collection and thus contribute significantly to the overall reasonableness of that collection. ~~(TS//SI//NF)~~

At the outset, it is worth noting that NSA's acquisition of Internet transactions containing multiple discrete communications does not necessarily increase the risk that NSA will incidentally acquire United States person information. For example, as discussed above, the ~~means by which NSA ensures it does not intentionally acquire wholly domestic communications limits the acquisition of certain transactions such as~~ to persons located outside the United States, who reasonably can be presumed to be non-United States persons. Thus, to the extent that the ~~of those non-United States persons contain communications that are not to, from, or about a targeted selector, those communications are unlikely to be United States person communications.~~ *See In re Directives*, Docket No. 105B(g):07-01, Mem. Op. at 87 (recognizing that "the vast majority of persons who are located overseas are non United States persons and that most of their communications are with other, non-United States persons, who are located overseas") (footnote omitted). For this same reason, the risk that United States person information would be obtained through the acquisition of a ~~is no greater than in the acquisition of a~~

<sup>18</sup> 50 U.S.C. § 1801(h)(1) defines "minimization procedures" as "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~  
~~(TS//SI//NF)~~

#### a. Acquisition (U)

As discussed above, with limited exceptions,<sup>19</sup> it is technologically infeasible for NSA's upstream collection to acquire only the discrete communication to, from, or about a tasked selector that may be contained in a transaction containing multiple discrete communications. That does not mean, however, that the minimization procedures governing NSA's upstream collection do not adequately minimize the acquisition of any United States person information that may be contained in those transactions. Specifically, minimization procedures must be reasonably designed to minimize the acquisition of nonpublicly available information concerning unconsenting United States persons "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1). As discussed above, the *only* way to obtain the foreign intelligence information contained within a discrete communication is to acquire the entire transaction in which it is contained. Thus, to the extent that United States person information may be contained within other discrete communications not to, from, or about the target in that transaction, the acquisition of such United States person information would be "consistent with the need of the United States to obtain . . . foreign intelligence information." ~~(TS//SI//NF)~~

Congress has recognized that "in many cases it may not be possible for technical reasons to avoid acquiring all information" when conducting foreign intelligence surveillance. H.R. Rep. No. 95-1283, pt. 1, at 55 (1978); *see also id.* at 56 ("It may not be possible or reasonable to avoid acquiring all conversations."); *cf. Scott*, 436 U.S. at 140 (recognizing that Title III "does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such as manner as to 'minimize' the interception of such conversations"). Rather, in situations where, as here, it is technologically infeasible to avoid incidentally acquiring communications that are not to, from, or about the target, "the reasonable design of the [minimization] procedures must emphasize the minimization of retention and dissemination." H.R. Rep. No. 95-1283, pt. 1, at 55. ~~(TS//SI//NF)~~

#### b. Retention (U)

In addition, for reasons discussed more fully below, nothing in the statutory definition of minimization procedures obligates NSA to immediately destroy any United States person information in a communication that is not to, from, or about a tasked selector within a transaction acquired by NSA's upstream collection. ~~(TS//SI//NF)~~

<sup>19</sup> See *supra* footnote 6. (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

i. **Destruction Is Not Technologically Feasible** ~~(TS//SI//NF)~~

First, Congress intended that the obligation to destroy non-pertinent information would attach only if the destruction of such information is feasible. See H.R. Rep. No. 95-1283, pt. 1, at 56 ("By minimizing retention, the committee intends that information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed *where feasible*." (emphasis added)). That is because Congress recognized that in some cases, the pertinent and non-pertinent information may be co-mingled in such a way as to make it technologically infeasible to segregate the pertinent information from the non-pertinent information and then destroy the latter. See *id.* ("The committee recognizes that it may not be feasible to cut and paste files or erase part of tapes where some information is relevant and some is not."). ~~(TS//SI//NF)~~

A transaction containing several communications, only one of which contains the tasked selector, is to NSA's systems technologically indistinguishable from a transaction containing a single message to, from, or about a tasked selector. That is true both for NSA's collection systems and for the NSA systems that process and then route Section 702-acquired information to NSA's corporate stores. Thus, unlike other instances where it is technologically possible for certain kinds of communications to be recognized, segregated, and prevented from being routed to NSA's corporate stores, the transaction as a whole, including all of the discrete communications that may be included within it, is forwarded to NSA corporate stores, where it is available to NSA analysts. ~~(TS//SI//NF)~~

The transaction is likewise not divisible into the discrete communications within it even once it resides in an NSA corporate store. That is because NSA assesses that it is not technologically feasible to extract, post-acquisition, only the discrete communication that is to, from, or about a tasked selector within a transaction without destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including the single, discrete communication which is to, from or about the tasked selector. Thus, an NSA analyst cannot, for example, simply cut out any pertinent part of the transaction (i.e., the discrete communication that contains the tasked selector), paste it into a new record, and then discard the remainder. In this way, the transactions at issue here are a present-day version of the very same problem that Congress recognized over thirty years earlier -- i.e., that in some cases, "it might not be feasible to cut and paste files . . . where some information is relevant and some is not." H.R. Rep No. 95-1283, pt. 1, at 56. Given that Congress recognized it might be necessary to retain all acquired information regardless of its pertinence because destruction of the non-pertinent information may not be feasible, minimization procedures that permit the retention of transactions in their entireties because their further divisibility is infeasible (if not technologically impossible) are consistent with the statutory requirement that such procedures minimize the retention of United States person information. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

ii. Retention of United States Person Information Can Be Effectively Minimized Through Restrictions on its Retrieval ~~(TS//SI//NF)~~

Second, although it is not required that all non-pertinent United States person information be destroyed, NSA's retention of non-pertinent information concerning innocent United States persons is not without bounds. FISA's legislative history suggests that the retention of such information could still be effectively minimized through means other than destruction. See H.R. Rep. No. 95-1283, pt. 1, at 56 ("There are a number of means and techniques which the minimization procedures may require to achieve the purposes set out in the definition."). Of particular relevance here, Congress recognized that minimizing the retention of such information can be accomplished by making the information "not retrievable by the name of the innocent person" through the application of "rigorous and strict controls." *Id.* at 58-59. Those "rigorous and strict controls," however, need only be applied to the retention of United States person information "for purposes other than counterintelligence or counterterrorism." *Id.* That is because Congress intended that "a significant degree of latitude be given in counterintelligence and counterterrorism cases with respect to the retention of information." *Id.* at 59. ~~(TS//SI//NF)~~

NSA's current Section 702 minimization procedures flatly prohibit the use of United States person names or identifiers to retrieve any Section 702-acquired communications in NSA systems. See, e.g., Amendment 1 to DNI/AG 702(g) Certification [REDACTED] Ex. B, filed [REDACTED] 2010, § 3(b)(5) (hereinafter "NSA Section 702 minimization procedures"). This "rigorous and strict control[]" applies even to United States person information that relates to counterintelligence or counterterrorism, despite Congress's stated intent that agencies should have "a significant degree of latitude . . . with respect to the retention of [such] information." H.R. Rep. No. 95-1283, pt. 1, at 59; see *id.* at 58-59 (recognizing that "for an extended period it may be necessary to have information concerning [the] acquaintances [of a hypothetical FISA target] retrievable" for analytic purposes, even though "[a]mong his contacts and acquaintances . . . there are likely to be a large number of innocent persons"). NSA's current Section 702 minimization procedures thus require the retention of information concerning United States persons (innocent or otherwise) to be minimized to a significantly greater degree than is necessary for those procedures to be reasonable. ~~(TS//SI//NF)~~

Of course, the Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. E.g., DNI/AG 702(g) Certification [REDACTED] Ex. B, filed Apr. 20, 2011, § 3(b)(5). Under these revised NSA Section 702 minimization procedures, the use of such selection terms must be approved in accordance with NSA procedures. *Id.* The Government is still in the process of developing the NSA procedures governing the use of United States person identifiers as selection terms. Until those procedures are completed, NSA analysts will not begin using United States person identifiers as selection terms. The Government will ensure that these NSA procedures contain "rigorous and strict controls" on the retrieval of United States person information consistent with statutory requirements and Congressional intent. H.R. Rep. No. 95-1283, pt. 1, at 59. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



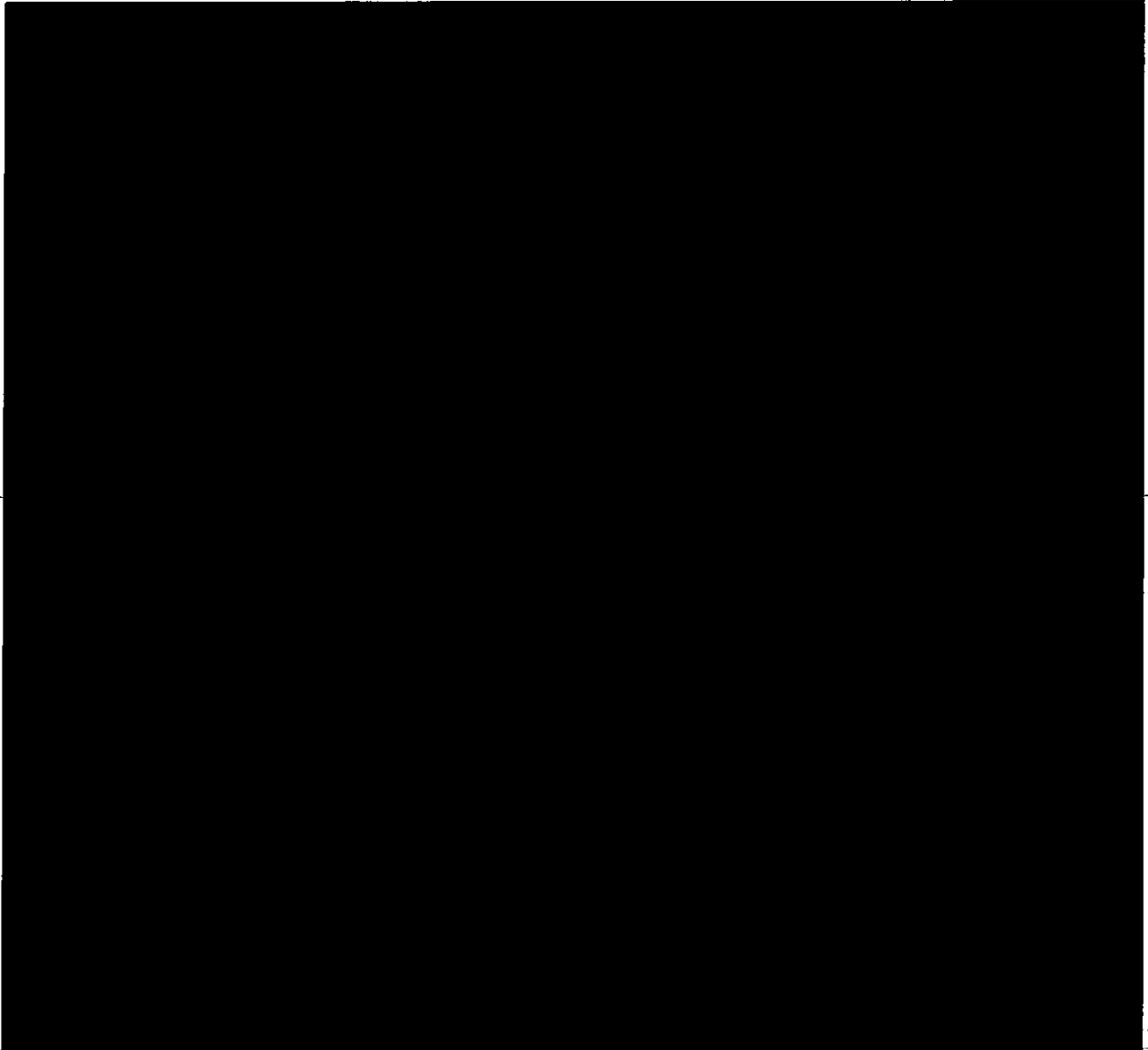
~~TOP SECRET//COMINT//ORCON,NOFORN~~

## c. Dissemination (U)

As discussed above, the NSA current Section 702 minimization procedures prohibit the use of United States person identifiers to retrieve any Section 702-acquired communications in NSA systems. Accordingly, the only way incidentally acquired United States person information currently will be reviewed by an NSA analyst is if that information appears in a communication that the analyst has retrieved using a permissible query term -- i.e., one that is reasonably likely to return information about non-United States person foreign intelligence targets. See NSA Section 702 minimization procedures, § 3(b)(5). Any identifiable United States person information contained in a communication retrieved in this manner would be subject to the dissemination restrictions in the NSA Section 702 minimization procedures, which operate to ensure that any dissemination of United States person information is consistent with the Act. These restrictions apply regardless of whether the United States person information is contained in a discrete communication that is to, from, or about a tasked selector. Moreover, the same dissemination restrictions will continue to apply to any United States person information retrieved through the use of a United States person identifier as a selection term in accordance with NSA's revised 702 minimization procedures. Indeed, given the small probability that an incidentally acquired communication of a United States person that is not to, from, or about a tasked selector would contain foreign intelligence information or evidence of a crime, it is highly unlikely that NSA would disseminate any information from that incidentally acquired communication, let alone information concerning the United States person. (TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



20

[Redacted text block]

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

21

[Redacted text block]

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

<sup>22</sup> See footnote 22 below. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

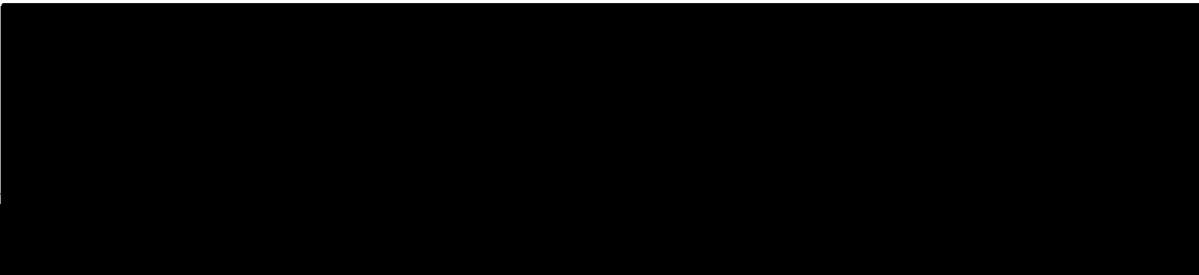
~~TOP SECRET//COMINT//ORCON,NOFORN~~



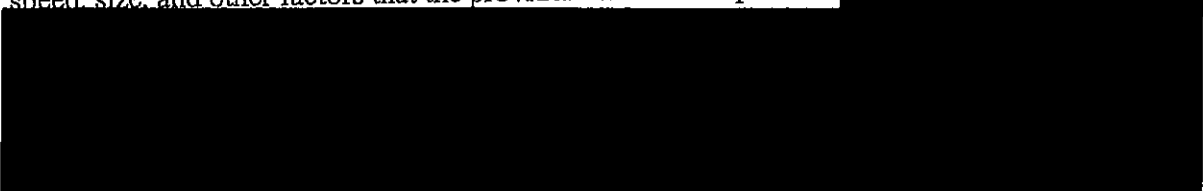
~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

- c. The May 2 Letter states that NSA is not presently capable of "separating out individual pieces of information" contained within [REDACTED] May 2 Letter at 3. Please explain why and state whether it would be feasible for NSA to implement such capability, either at the time of acquisition or thereafter. ~~(TS//SI//NF)~~
- d. Can [REDACTED] be identified as distinct from other, discrete communications between users, either at the time of acquisition or thereafter? If so, can NSA filter its Section 702 collection on this basis? ~~(TS//SI//NF)~~



Except as described above, at the time of acquisition, NSA is not presently capable of separating out transactions that contain multiple electronic communications into logical constituent parts without destabilizing -- and potentially rendering unusable -- some or all of the entire collected transaction, including any particular communication therein which is in-fact to, from, or about the tasked selector. Each electronic communication service provider develops protocols that perform the services being provided in a manner designed to be economical in speed, size, and other factors that the provider considers important. [REDACTED]



<sup>25</sup> An NSA analyst would, however, be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system, such as an analytic store. Even so, the original transaction from which that copy was made would be retained in the corporate store in its original state, which cannot be altered for the reasons discussed below. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Each of the major providers change protocols often to suit their own business purposes, and it is therefore generally not possible for NSA to isolate or separate out individual pieces of information contained within single transactions at the time of NSA acquisition. Any protocol in use today could easily be changed by the provider tomorrow ( [REDACTED] )

[REDACTED]

[REDACTED]

[REDACTED] In short, except in cases involving [REDACTED] described above, at the time of acquisition it is not technologically feasible for NSA to extract any particular communication that is to, from, or about a tasked selector within a transaction containing multiple discrete communications. (TS//SI//NF)

For the same reasons that protocol volatility and myriad user settings prevent the extraction of only discrete communications at the point of acquisition, it is not technologically feasible to extract, post-acquisition, only the specific communication(s) to, from, or about a tasked selector within a transaction without destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including any particular communication therein which is to, from, or about the tasked selector. Thus, an NSA analyst cannot, for example, simply cut out the discrete communication that contains the tasked selector, paste it into a new record, and then discard the remainder. (TS//SI//NF)

3. The May 2 Letter notes that NSA uses Internet Protocol (IP) filtering and [REDACTED] to prevent the intentional acquisition of communications as to which the sender and all known recipients are inside the United States. May 2 Letter at 3. (TS//SI//NF)

a. Please describe how NSA applies IP filtering in the context of [REDACTED]

[REDACTED] (TS//SI//NF)

i. [REDACTED] (TS//SI//NF)


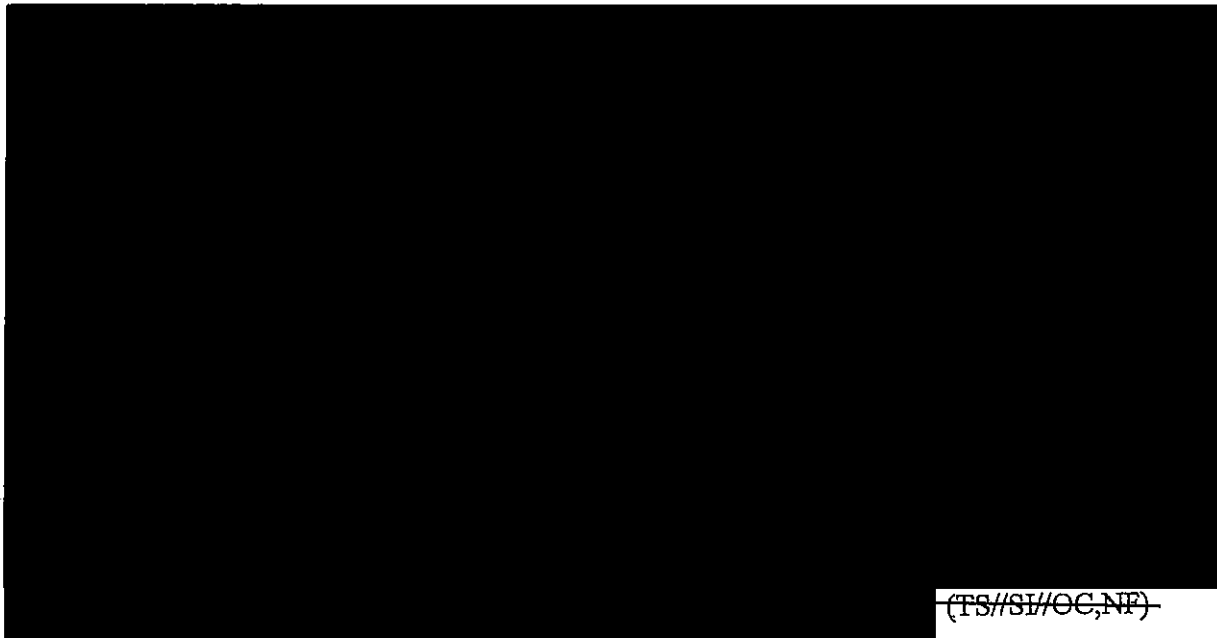
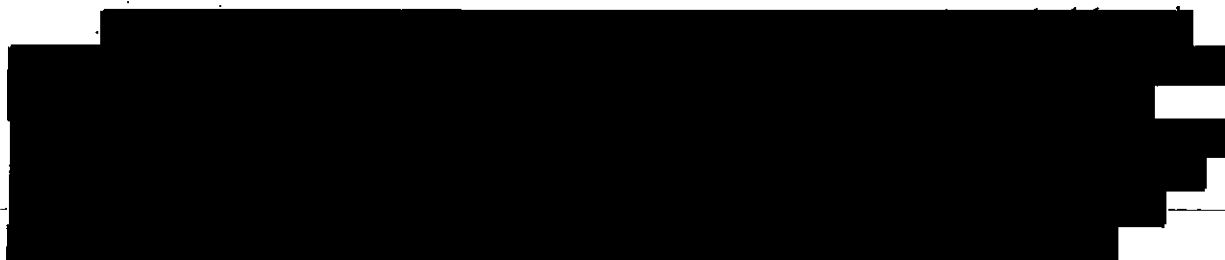
ii. [REDACTED]

(TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

NSA acquires Internet communications by collecting the individual packets of data that make up those communications. As required by NSA's targeting procedures, all Internet communications data packets that may contain abouts information that NSA intercepts through its Section 702 upstream collection must either pass through an "Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," or

~~(TS//SI//OC,NF)~~~~(TS//SI//OC,NF)~~~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] Accordingly, NSA cannot prevent the acquisition of, or even mark for separate treatment, those types of transactions that may feature multiple discrete communications ([REDACTED]) (TS//SI//OC,NF)

- b. In the collection of "to/from" communications, are the communicants always the individual users of particular facilities [REDACTED], or does NSA sometimes consider [REDACTED] Please explain. (TS//SI//NF)

In the collection of "to/from" communications, NSA considers the communicants as being the individual users of particular selectors. More particularly, NSA considers those individual users to be the senders and intended recipients of "to/from" communications. Conversely, NSA does not consider [REDACTED]

(TS//SI//NF)

4. How, in terms of numbers and volume, does NSA's collection of [REDACTED] under Section 702 compare with the collection of discrete Internet communications (such as e-mail messages) between or among individual users? (TS//SI//NF)

As a result of the present technological limitations [REDACTED] NSA cannot precisely measure the number of transactions that might contain information or data representing several discrete communications [REDACTED] for purposes of comparing that figure with transactions containing a single, discrete communication [REDACTED] without manually examining each transaction that NSA has acquired. However, in an attempt to provide an estimate of the volume of such collection at the Court's request, NSA performed a series of queries into the SIGINT Collection Source System of Record that holds the relevant transactions in question. [REDACTED]

Results were sampled manually to confirm collection of [REDACTED]

Results were reviewed for three randomly selected days in April, averaged to produce an estimated figure of collection of [REDACTED] for the month of April. This figure was then compared to the total take of Section 702 upstream collection of web activity for the month. From this sample, NSA estimates that approximately 9% of the monthly Section 702 upstream collection of [REDACTED]<sup>26</sup> It is important

<sup>26</sup> NSA notes that it is likely that this 9% figure includes [REDACTED] of the user of the targeted selector him/herself. (TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

to note that this was a manually intensive and imprecise means to quantify the volume of [REDACTED] collection and should not be interpreted to suggest that any technological method of pre-filtering can be applied to the collection before it is available to the analyst. ~~(TS//SI//NF)~~

5. Given that some of the information acquired through upstream collection is likely to constitute "electronic surveillance" as defined in 50 U.S.C. § 1801(f)(2) that has not been approved by this Court, how does the continued acquisition of, or the further use or dissemination of, such information comport with the restrictions of 50 U.S.C. § 1809(a)(1) and (a)(2)? ~~(TS//SI//NF)~~

I. **THE CONTINUED ACQUISITION, USE, AND DISSEMINATION OF INFORMATION ACQUIRED THROUGH UPSTREAM COLLECTION DOES NOT VIOLATE 50 U.S.C. § 1809.** ~~(TS//SI//NF)~~

A. Introduction (U)

Section 702 of FISA, as codified at 50 U.S.C. § 1881a, provides that "[n]otwithstanding any other provision of law," upon the issuance of an appropriate Order from the Court, the Attorney General (AG) and the Director of National Intelligence (DNI) may jointly authorize the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information as long as certain conditions set out in subsection 702(b) are met. The joint authorizations of the AG and the DNI authorized NSA's upstream acquisition of communications that are to, from, or about a tasked selector. The Court, in turn, approved the implementing certifications as well as the use of proffered targeting and minimization procedures. Accordingly, because the acquisition of communications to, from, or about a tasked selector was authorized by the AG and DNI, and the Court approved the certifications and procedures used to implement those authorizations, NSA's acquisition of such communications upstream does not constitute unauthorized electronic surveillance and, therefore, does not violate the terms of 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

As noted above, the Government readily acknowledges that it did not fully describe to the Court that the upstream collection technique would result in NSA acquiring [REDACTED] types of Internet transactions that could include multiple individual, discrete communications [REDACTED]. As discussed below, however, this omission does not invalidate the AG and DNI's prior authorizations. Nor does it mean that the incidental acquisition of communications that are not to, from, or about a tasked selector as a consequence of obtaining communications that are to or from a tasked selector or contain reference to a tasked selector, exceeds the scope of those authorizations. For the same reasons, the Government respectfully suggests that the Orders of

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

this Court upon which those authorizations rely likewise remain valid. Thus, Section 1809 is not implicated by NSA's upstream collection activities under Section 702. ~~(TS//SI//NF)~~

## B. Statutory Framework (U)

### i. Section 1809 (U)

Under Subsection 1809(a), a person is guilty of a criminal offense if he or she "intentionally (1) engages in electronic surveillance under color of law, except as authorized by this Act . . . ; or (2) disclose[s] or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act."<sup>27</sup> (U)

For purposes of Section 1809 the issue is whether the Government's prior failure to fully explain to the Court the steps NSA must take in order acquire communications to, from, or about a tasked selector, and certain technical limitations regarding the IP address filtering it applies, means that the acquisition of such communications was not authorized by the DNI and AG, and inconsistent with Court approval of the targeting and minimization procedures. ~~(TS//SI//NF)~~

### ii. Section 702 Collection Authorizations ~~(S)~~

Pursuant to 50 U.S.C. § 1881a(a), "notwithstanding any other provision of law," the AG and the DNI may jointly authorize for a period of up to one year the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, subject to targeting and minimization procedures approved by this Court, and certain limitations set out in § 1881a(b). Authorizations are premised on certifications to the Court, in which the AG and DNI attest to the fact that, among other things, the targeting and minimization procedures comply with certain statutory requirements and the Fourth

<sup>27</sup> This Court has previously noted that the legislative history of this provision focuses on a predecessor bill that was substantially different from the provision subsequently enacted and codified. See [REDACTED] Mem. Op. at 6-7 (Dec. 10, 2010). Yet, both the predecessor bill and the codified provision use the word intentionally, which has been described as "carefully chosen" and intended to limit criminal culpability to those who act with a "conscious objective or desire" to commit a violation. See H.R. Rep. No. 95-1283, pt.1, at 97 (1978) ("The word 'intentionally' was carefully chosen. It is intended to reflect the most strict standard for criminal culpability. . . . The Government would have to prove beyond a reasonable doubt both that the conduct engaged in was in fact a violation, and that it was engaged in with a conscious objective or desire to commit a violation."). Based upon discussions between responsible NSA officials and the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) and DOJ and ODNI's review of documents related to this matter, DOJ and ODNI have not found any indication that there was a conscious objective or desire to violate the authorizations here. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Amendment. 50 U.S.C. § 1881a(g)(2). Authorizations become effective “upon the issuance of an order [of this Court]” approving the certification and the use of the targeting and minimization procedures as consistent with the statute and the Fourth Amendment. *Id.* §§ 1881a(a) (AG and DNI authorizations go into effect upon “issuance of an order”); 1881a(i)(2)-(3) (laying out scope of FISC review).<sup>28</sup> ~~(TS//SI//NF)~~

Thus, if an acquisition is authorized by the AG and DNI, and the certification and targeting and minimization procedures which implement that authorization are approved by the Court, and the authorization remains valid, then the acquisition does not constitute unauthorized electronic surveillance under 50 U.S.C. § 1801(f)(2) and is not a violation of 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

**C. At a Minimum, the Upstream Acquisition of Single, Discrete Communications To, From, or About a Tasked Selector Was Authorized by the AG and the DNI**

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

The relevant AG and DNI authorizations and the targeting procedures the AG approved explicitly permit the acquisition of Internet communications that are to, from, or about a tasked selector. *See, e.g.*, NSA Targeting Procedures at 1 (describing the safeguards used in the acquisition of “about” as compared with “to/from” communications). In addition, the accompanying Affidavits of the Director of NSA described upstream collection in a paragraph detailing the various methods of obtaining such acquisitions. *See, e.g.*, DNI/AG 702(g) Certification [REDACTED] Affidavit of General Keith B. Alexander, Director, NSA, filed July 16, 2010, ¶ 4. Thus, it is clear that the authorizations permit – at a minimum – the upstream acquisition of single, discrete communications to, from, or about a tasked selector. ~~(TS//SI//NF)~~

As described in detail in response to questions 2 and 3 above, due to certain technological limitations, in general the only way NSA can currently acquire as part of its upstream collection single, discrete communications to, from, or about a tasked selector [REDACTED] is by obtaining the Internet transactions of which those communications are a part. An Internet transaction can include either a single, discrete communication to, from, or about a tasked

<sup>28</sup> For reauthorizations, the AG and the DNI submit, to the extent possible, a certification to the FISC laying out, among other things, the targeting and minimization procedures adopted at least 30 days prior to the expiration of the prior authorization. The prior authorization remains in effect, notwithstanding the otherwise applicable expiration date, pending the FISC’s issuance of an order with respect to the certification for reauthorization. 50 U.S.C. § 1881a(i)(5). The scope of the court’s review is the same for reauthorizations as it is for initial authorizations. *Id.* § 1881a(i)(5)(B). (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

selector [REDACTED], or several discrete communications, only one of which may be to, from, or about a tasked selector [REDACTED] (TS//SI//NF)

Where an Internet transaction includes multiple communications, not all of which are to, from, or about a tasked selector, it currently may not be technologically feasible for NSA to separate out, at the time of acquisition or thereafter, the discrete electronic communications within that transaction that are to, from, or about a tasked selector. Indeed, at the time of acquisition, NSA's upstream Internet collection devices are, with limited exception, not capable of distinguishing or further separating discrete electronic communications [REDACTED] within a single Internet transaction. Thus, in some cases, NSA can collect communications to, from, or about a tasked selector, as authorized by the certification, only by obtaining the Internet transaction of which those communications may be just a part. (TS//SI//NF)

In this respect, the upstream acquisition of Internet transactions which contain multiple, discrete communications not all of which are (and, in some instances, only one of which is) to, from or about a tasked selector is akin to the Government's seizure of a book or intact file that contains a single page or document that a search warrant authorizes the government to seize. In *United States v. Wuagnewx*, 683 F.2d 1343, for example, the Eleventh Circuit rejected appellants' argument that a search was unreasonable because the agents seized an entire file, book, or binder if they identified a single document within the file, book, or binder as being within the authorization of the warrant. As the court explained, "a search may be as extensive as reasonably required to locate items described in the warrant." *Id.* at 1352. It was therefore "reasonable for the agents to remove intact files, books and folders when a particular document within the file was identified as falling within the scope of the warrant." *Id.* at 1353. See also *United States v. Rogers*, 521 F.3d 5, 10 (1st Cir. 2008) (concluding that a videotape is a "plausible repository of a photo" and that therefore a warrant authorizing seizure of "photos" allowed the seizure and review of two videotapes); *United States v. Christine*, 687 F.2d 749, 760 (3d Cir. 1982) (*en banc*) (emphasizing that "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision. Nor does the Fourth Amendment prohibit seizure of an item, such as a single ledger, merely because it happens to contain other information not covered by the scope of the warrant."); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence may be seized"). (TS//SI//NF)

That the certifications by the AG and DNI did not specifically describe this aspect of NSA's upstream collection does not mean that collection was unauthorized by the AG and DNI. Again, case law involving the reasonableness of searches conducted pursuant to criminal search warrants is instructive on this point. For example, in *Dalia v. United States*, 441 U.S. 238, 259 (1979), the Supreme Court recognized that "[o]ften in executing a warrant the police may find it

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant." *Id.* at 257. See *United States v. Grubbs*, 547 U.S. 90, 98 (2006) ("Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.") (quoting *Dalia*, 441 U.S. 238, 257 (1979)). This is especially true where, as in *Dalia*, "[t]here is no indication that [the] intrusion went beyond what was necessary" to effectuate the search authorized. *Dalia*, 441 U.S. at 258 n. 20. ~~(TS//SI//NF)~~

Like the seizure of an entire book or file simply because it contained a single page or document within the scope of the warrant, NSA only acquires an Internet transaction containing several discrete communications if at least one of those communications within the transaction is to, from, or about a tasked selector. Moreover, unlike the agents in *Wuagneux*, who presumably ~~could have opted to seize only the responsive pages out of the books and files searched, except in~~ limited circumstances, NSA has no choice but to acquire the whole Internet transaction in order to acquire the to, from, or about communication the DNI and AG authorized NSA to collect. NSA only acquires an Internet transaction if *in fact* it contains at least one communication to, from, or about a tasked selector. NSA's acquisition of Internet transactions containing several discrete communications, only one of which is to, from, or about a tasked selector, is therefore "as extensive as reasonably required to locate the items described" in the DNI and AG's authorization, and thus cannot be said to exceed the scope of that authorization. ~~(TS//SI//NF)~~

Moreover, as described in response to questions 1(b)(ii) and (iii), the Government has concluded that such collection fully complies with the statutory requirements and the Fourth Amendment. Having now considered the additional information that is being presented to this Court, the AG and DNI have confirmed that their prior authorizations remain valid. Accordingly, Government personnel who rely on those authorizations to engage in ongoing acquisition are not engaging in unauthorized electronic surveillance, much less doing so "intentionally." ~~(TS//SI//NF)~~

#### **D. The Court Approved the Certifications and Targeting and Minimization Procedures Used to Implement the Authorizations of the AG and DNI** ~~(TS//SI//NF)~~

A second issue concerns whether this Court's orders cover the full scope of the authorizations, and, if not, whether that affects the validity of the AG and DNI authorizations. Like the AG and DNI authorizations, in approving the applicable certifications and the use of the proffered targeting and minimization procedures this Court's Opinions and Orders clearly contemplated and approved some upstream collection of communications to, from, or about a target. See, e.g., [REDACTED] Mem. Op. at 15-17 (describing acquisition of communications to, from,

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

and about a target).<sup>29</sup> Thus, for the reasons described above, the acquisition of Internet transactions that include at least one communication to, from, or about a target falls within the scope of the Court's Orders – even if additional communications are also incidentally acquired due to limits in technology. ~~(TS//SI//NF)~~

The fact that the Government did not fully explain to the Court all of the means by which such communications are acquired through NSA's upstream collection techniques does not mean that such acquisitions are beyond the scope of the Court's approval, just as in the criminal context a search does not exceed the scope of a warrant because the Government did not explain to the issuing court all of the possible means of execution, even when they are known beforehand and could possibly implicate privacy rights. *See Dalia*, 441 U.S. at 257 n.19 (noting that "[n]othing in the decisions of this Court . . . indicates that officers requesting a warrant should be constitutionally required to set forth the anticipated means for execution even in those cases where they know beforehand that [an additional intrusion such as] unannounced or forced entry likely will be necessary."). In addition, as discussed herein, the incidental acquisitions do not go beyond what is reasonably necessary to acquire the foreign intelligence information contained in a communication to, from, or about a targeted selector within a transaction. *See id.* at 258 n. 20. ~~(TS//SI//NF)~~

In any event, the Government believes that the additional information should not alter the Court's ultimate conclusion that the targeting and minimization procedures previously approved are consistent with the statutory requirements, including all the requirements of § 1881a(b), and the Fourth Amendment, and the Court's orders therefore remain valid. *Cf. Franks v. Delaware*, 438 U.S. 154 (1978) (establishing that a search warrant is valid unless it was obtained as the result of a knowing and intentional false statement or reckless disregard for the truth and the remaining content is insufficient to establish the requisite probable cause needed to obtain the warrant). ~~(TS//SI//NF)~~

Pursuant to § 1881a, the Court reviews the following issues: (i) whether the AG and DNI certifications contain all the required elements; (ii) whether the targeting procedures are consistent with the requirements of § 1881a(d)(1); (iii) whether the minimization procedures are consistent with § 1881a(i)(e)(1); and (iv) whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(2), (3). *See also id.* § 1881a(i)(5)(B) (specifying that reauthorizations are to be reviewed under the same

<sup>29</sup> Each of the relevant 2010 FISC Orders is based on the "reasons stated in the Memorandum Opinion issued contemporaneously herewith." These Opinions, in turn, rely on the analysis conducted by the Court in Dockets [REDACTED], which incorporate and rely on the analysis of earlier FISC Opinions, including Docket 702(i)-08-01. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

standards). The Government believes that the Court's ultimate conclusions with respect to each of these issues should not change based on the additional information provided. ~~(TS//SI//NF)~~

First, there is no suggestion that the prior certifications failed to contain all the required elements. ~~(TS//SI//NF)~~

Second, while the Government acknowledges that it did not fully explain to the Court the steps NSA must take in order to implement its Section 702 upstream Internet collection techniques, and certain technical limitations regarding its IP address filtering, the Court did approve the DNI/AG certifications and the use of targeting and minimization procedures which authorized the acquisition of communications to, from, or about tasked selectors. As discussed above and in response to questions 1(b)(ii) (iii) and 3, Internet transactions are collected because they contain at least one discrete communication to, from, or about a tasked selector. Each tasked selector has undergone review, prior to tasking, designed to ensure that the user is a non-United States person reasonably believe to be located outside the United States. Moreover, with respect to "abouts" communications, for the reasons discussed in the response to question 1(b)(ii), NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of any communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.<sup>30</sup> Thus, NSA is targeting persons reasonably believed to be outside the United States and is not intentionally acquiring communications in which both the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//NF)~~

Third, as described throughout, in many cases, it is not technologically feasible for NSA to acquire only Internet transactions that contain a single, discrete communication to, from, or about a tasked selector that may be contained in an Internet communication containing multiple discrete [REDACTED] communications. As discussed in detail in response to questions 1(b)(ii) and (iii), this does not mean that NSA's procedures do not adequately minimize the acquisition of any U.S. person information that may be contained within those transmissions. Rather, the minimization procedures fully comport with all statutory requirements. ~~(TS//SI//NF)~~

<sup>30</sup> As the Court is aware, § 1881a(b)(4) provides that an acquisition authorized under section 702, "may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States . . ." Although this prohibition could be read at first glance to be absolute, another provision of Section 702 indicates otherwise. Specifically, § 1881a(d)(1)(B) provides that the targeting procedures that the AG, in consultation with the DNI, must adopt in connection with an acquisition authorized under section 702 need only be "reasonably designed to . . . prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Finally, as described in response to question 1(b)(iii), the targeting and minimization procedures fully comply with the Fourth Amendment. ~~(TS//SI//NF)~~

Thus, the additional information the Government has provided concerning details of its upstream collection does not – in the Government’s view – undercut the validity of the targeting or minimization procedures. ~~(TS//SI//NF)~~

**E. Compliance with the Authorizations: Use and Disclosure** ~~(TS//SI//NF)~~

As described above, § 1809(a)(2) criminalizes the intentional use and disclosure of electronic surveillance, “knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act.” Having concluded that the upstream collection conducted by NSA falls within the scope of the relevant authorizations, the Government respectfully submits that the continued use and disclosure of such information is likewise valid, so long as the minimization procedures approved by the Court (and discussed in detail in response to questions 1(b)(ii) and (iii)) are followed.<sup>31</sup> ~~(TS//SI//NF)~~

6. Please provide an update regarding the [REDACTED] over collection incidents described in the government’s letter to the Court dated April 19, 2011.

The April 19, 2011, notice to the Court described two overcollection incidents involving entirely unrelated communications that had been [REDACTED]. The notice also advised that as part of its continued investigation into these incidents, NSA would examine other systems to determine whether similar [REDACTED] issues occurred in those systems. ~~(TS//SI//NF)~~

The first incident described in the April 19 notice involved [REDACTED]. Each [REDACTED] contained at least one communication to, from, or about a Section 702-tasked selector, but also [REDACTED] unrelated communications. This overcollection started [REDACTED].

<sup>31</sup> Although this analysis has focused on acquisitions conducted pursuant to the 2010 Section 1881a Authorizations, the Government believes that, for all of the reasons discussed herein, the upstream collection conducted pursuant to previous certifications authorized under Section 1881a of the Foreign Intelligence Surveillance Act of 1978, as amended, the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007), [REDACTED]

[REDACTED] falls within the scope of the relevant authorizations and Orders of this Court. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~~~(TS//SI//NF)~~

All such communications will be processed in accordance with NSA's minimization procedures.<sup>32</sup> The Government will advise the Court of the final disposition of these communications.

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

The second-described incident involved overcollection. As described in the April 19 notice, on March 28, 2011, NSA discovered a of Section 702-acquired communications that had not been properly

In contrast to the communications overcollected between discussed above, the acquired as a result of the overcollection incident involved fewer communications

<sup>32</sup> In particular, section 3(b)(1) of NSA's Section 702 Minimization Procedures state:

Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications.

(Emphasis added). ~~(S//SI)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

As in the [REDACTED] incident, each [REDACTED] contains at least one communication that is to, from, or about a Section 702-task selector. (TS//SI//NF)

As of April 11, 2011, NSA began to sequester in its Collection Stores all communications involving the affected [REDACTED]

[REDACTED]. NSA was deliberately overinclusive in adding objects to the [REDACTED]; while some of these objects include [REDACTED] other objects consist of only one communication to, from, or about a Section 702-task selector.

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

Since the filing of the April 19 notice, NSA has continued to evaluate collection from [REDACTED] and has observed no evidence of [REDACTED] issues other than the above-described issues [REDACTED]

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

NSA has identified no reporting based upon overcollected communications and is currently exploring options to automate ways to accelerate identification of [REDACTED]

[REDACTED] NSA anticipates that it will be able to reach a decision by June 30, 2011, on whether this approach is effective. ~~(TS//SI//NF)~~

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

The April 19 notice also advised the Court that NSA would "examine [REDACTED] and other upstream collection systems to ensure that similar [REDACTED] problems are not occurring in those systems." NSA now reports that unlike the most recent [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

these other systems were designed [REDACTED]

33

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

**7. Are there any other issues of additional information that should be brought to the Court's attention while it is considering the certifications and amendments filed in the above-captioned dockets?**

At this time, the Department of Justice (DOJ) and Office of the Director of National Intelligence (ODNI) are currently investigating certain possible incidents of non-compliance about which the Department of Justice intends to file preliminary notices in accordance with the rule of this Court. These incidents do not relate to any of the matters discussed in this filing and, based on the information currently available to DOJ and ODNI, the Government does not believe that the nature of these incidents is sufficiently serious such that they would bear on the Court's consideration of the certifications and amendments filed in the above-captioned dockets.

~~(S//OC,NF)~~

<sup>33</sup> As discussed in response to question 2(c) and (d), NSA has the ability to separate out individual pieces of information in certain cases [REDACTED]. In the course of the investigation into the most recent [REDACTED] incident, NSA additionally identified [REDACTED]

[REDACTED] Though testing demonstrated the possibility that incompletely processed communications could have been forwarded through the SIGINT system, NSA has identified no actual overcollection that occurred as a result. NSA is currently in the process of developing a software fix designed to properly process such communications under the limited circumstances in which overcollections could occur. Until such a fix can be tested and deployed, NSA will continue to monitor [REDACTED] and other upstream Section 702 collection systems [REDACTED]

~~(TS//SI//NF)~~~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Follow-up Questions Regarding Section 702 Certifications

June 17, 2011

1. The government's Response to the Court's Briefing Order of May 9, 2011 ("June 1 Submission") states that Internet transactions acquired by NSA in its upstream collection may contain not only multiple discrete communications (some of which are neither to, from, nor about a tasked selector), but also [REDACTED]

[REDACTED] June 1 Submission at 25.

a. Please provide some examples of the [REDACTED]

For instance, could such acquisitions include [REDACTED]

b. What is the likelihood that such [REDACTED] pertain to persons other than the users of tasked selectors, including persons in the United States or U.S. persons?

2. The June 1 Submission states that "no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication." June 1 Submission at 9.

a. What is meant by "wholly domestic communication" in this statement? Does the term include the discrete communications that might be embedded within acquired transactions?

b. What is the likelihood that an analyst viewing information obtained through a transactional acquisition would have a basis for determining that a discrete communication embedded within the transaction is purely domestic?

3. a. Might the non-targeted portion of a transaction ever be the sole basis for that transaction being responsive to an analyst's query?

b. Upon retrieving information in response to a query, can an analyst readily distinguish that portion of a transaction that contains the targeted selector from other portions of a transaction?

4. a. Please describe the manner in which the government minimizes discrete communications and other information that is contained within acquired Internet transactions but that is neither to, from, nor about the user of a targeted selector.

b. In particular, please explain how the government applies the provisions of NSA's minimization procedures that use the term "communication" to the discrete communications and other non-target information contained within the transactions that are acquired. See, e.g., NSA Minimization Procedures § 2(c) (defining "[c]ommunications of a United States person"); § 2(e) (defining "foreign communication" and "domestic communication[]"), § 3(b)(4) (discussing determination whether a communication is "foreign" or "domestic"), and § 5 (discussing handling of domestic communications).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

- c. Would all communications and [REDACTED] within a transaction be treated the same when the minimization procedures are applied, or would there be different treatment?
5. a. Once NSA has identified a portion of a transaction that does not contain targeted information, is it possible to mask or otherwise minimize the non-target information contained within the transaction?  
b. Why is NSA unable to delete and replace, or alter, an original transaction that contains non-target information? See June 1 Submission at 27-28.
6. The government states that an Internet transaction that is acquired "is . . . not divisible into the discrete communications within it even once it resides in an NSA corporate store." June 1 Submission at 22. Please reconcile that statement with the government's acknowledgment that "an analyst would . . . be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system." Id. at 27 n.25.
7. Please reconcile the government's statement that the "communicants" of to/from communications are "the individual users of particular selectors" (see June 1 Submission at 30) with [REDACTED] elsewhere in its response to the Court's questions (see, e.g., id. at 6 (discussing application of IP filtering)).
8. What is the factual basis for NSA's assertions that "a United States person would use [REDACTED] only in a minute percentage of cases" and that "[REDACTED]"  
See June 1 Submission at 11, 12.
9. What is the factual basis for NSA's suggestion that [REDACTED]  
[REDACTED] See June 1 Submission at 8 n.9
10. The government repeatedly characterizes as "unintentional" NSA's collection of discrete non-target communications as part of transactional acquisitions, [REDACTED]. Assuming arguendo that such collection can fairly be characterized as unintentional, please explain how 50 U.S.C. § 1806(i) applies to the discrete, wholly domestic communications that might be contained within a particular transaction.
11. Please provide a thorough legal analysis supporting your view that the knowing and intentional acquisition of large volumes of Internet transactions containing discrete communications that are neither to, from, nor about a targeted selector (as well as other information not pertaining to the users of targeted selectors) is merely "incidental" to the authorized purpose of the collection as a whole, and therefore reasonable under the Fourth Amendment.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

12. The statute requires the targeting procedures to “be reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and [to] prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” 50 U.S.C. § 1881a(d)(1). How can procedures that contemplate the knowing acquisition of huge volumes of transactions that will include quantifiable amounts of information relating to non-targets, including information of or about U.S. persons abroad or persons located in the United States, meet this statutory requirement?

13. In its discussion of the Fourth Amendment, the government asserts that “upstream collection” in general is “an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs.” June 1 Submission at 16.

- a. To what extent can the same be said for the acquisition of Internet transactions [REDACTED] in particular?
- b. Is the acquisition of Internet transactions via upstream collection the only source for certain categories of foreign intelligence information? If so, what categories?
- c. Please describe with particularity what information NSA would acquire, and what information NSA would not acquire, if NSA were, in comparison to its current collection, to limit its acquisition of Internet communications to: (1) acquisitions conducted with the assistance of [REDACTED]; and (2) the upstream collection of discrete communications to, from, or about tasked selectors that are [REDACTED] (*id.* at 2, n.2).

14. The Fourth Amendment also requires the Court to examine the nature and scope of the intrusion upon protected privacy interests. How can the Court conduct such an assessment if the government itself is unable to describe the nature and scope of the information that is acquired or the degree to which the collection includes information pertaining to U.S. persons or persons located in the United States?

15. In light of the government’s emphasis on the limited querying of Section 702 acquisitions that is currently permitted (*see* June 1 Submission at 23), why is it reasonable and appropriate to broaden the targeting procedures to permit querying using U.S.-person identifiers?

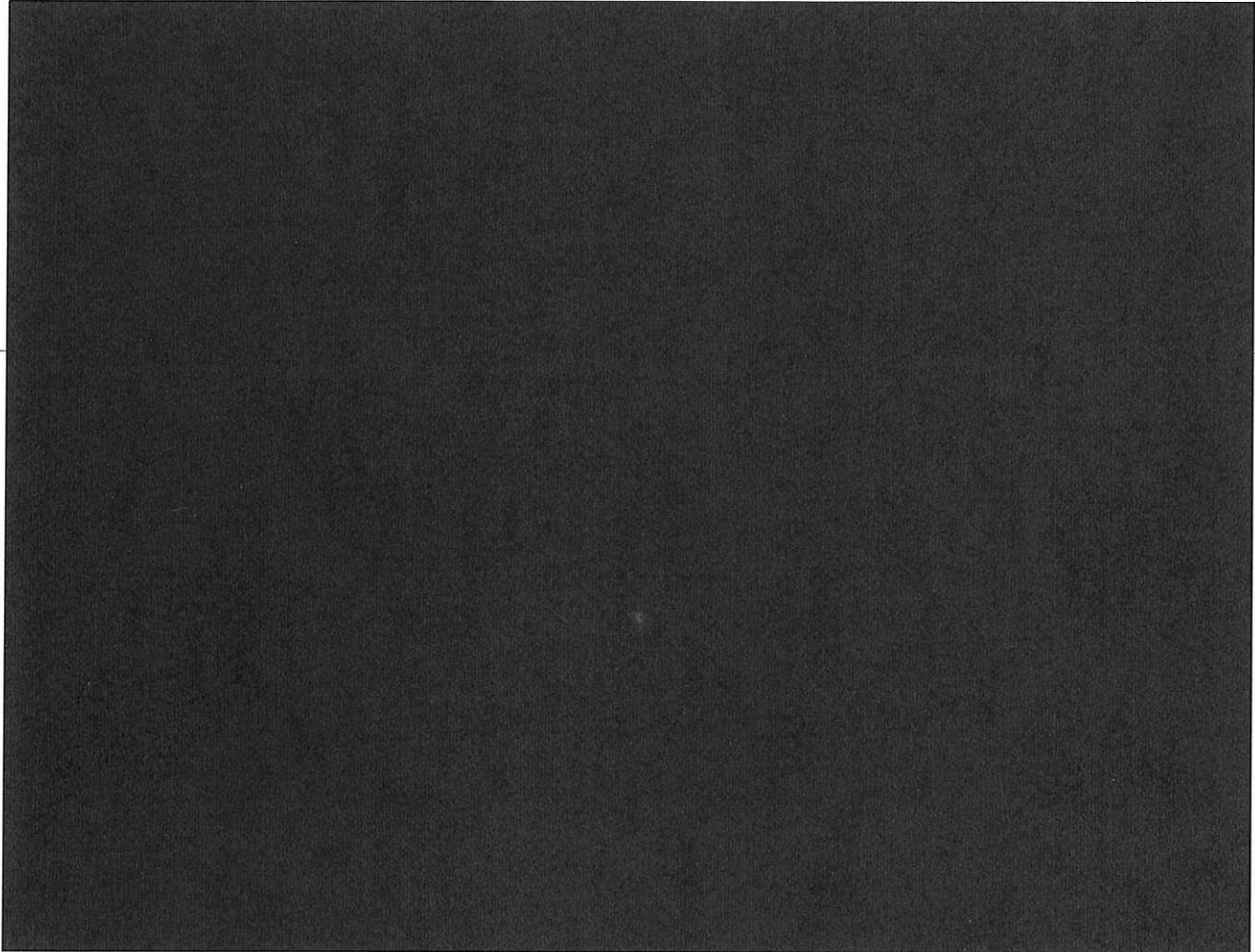
16. The government acknowledges that it previously “did not fully explain all of the means by which . . . communications are acquired through NSA’s upstream collection techniques” (June 1 Submission at 2), yet states that the “[Attorney General] and [Director of National Intelligence] have confirmed that their prior authorizations remain valid” (*id.* at 35). At the time of each previous Certification under Section 702, were the Attorney General and the Director of National Intelligence aware that the acquisitions being approved included Internet “transactions” [REDACTED]? If so, why was the Court not informed. If not, why are the prior Certifications and collections still valid?

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

JUN 28 PM 4:51  
RECEIVED  
FBI  
COURT



NOTICE OF FILING OF GOVERNMENT'S RESPONSE  
TO THE COURT'S SUPPLEMENTAL QUESTIONS OF JUNE 17, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of  
Justice attorney, respectfully submits the attached factual and legal response to the

~~SECRET//ORCON,NOFORN~~

Classified by: ~~Tashina Gauhar, Deputy Assistant~~  
~~Attorney General, NSD, DOJ~~  
Reason: ~~1.4(c)~~  
Declassify on: ~~28 June 2036~~

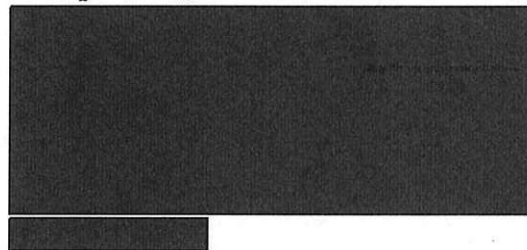


~~SECRET//ORCON,NOFORN~~

supplemental questions provided by this Court to the Government on June 17, 2011, concerning the above-referenced matters. Given the complex nature of the Court's questions and the Government's responses, the United States is prepared to provide any additional/supplemental information the Court believes would aid it in reviewing these matters. The Government may also seek to supplement and/or modify its response as appropriate during any hearing that the Court may hold in the above-captioned matters. ~~(S//OC,NE)~~

---

Respectfully submitted,




National Security Division  
United States Department of Justice

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

VERIFICATION

I declare under penalty of perjury that the facts set forth in the attached Government's Response to the Court's Supplemental Questions of June 17, 2011, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 28th day of June, 2011. (S)



---

Signals Intelligence Directorate Compliance Architect  
National Security Agency

~~SECRET//ORCON,NOFORN~~



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

GOVERNMENT'S RESPONSE TO THE  
COURT'S FOLLOW-UP QUESTIONS OF JUNE 17, 2011

1. The government's Response to the Court's Briefing Order of May 9, 2011 ("June 1 Submission") states that Internet transactions acquired by NSA in its upstream collection may contain not only multiple discrete communications (some of which are neither to, from, nor about a tasked selector), but also [REDACTED]

[REDACTED] June 1 Submission at 25.

a. Please provide some examples of the [REDACTED]

[REDACTED] instance, could such acquisitions include [REDACTED]

b. What is the likelihood that such [REDACTED] pertain to persons other than the users of tasked selectors, including persons in the United States or U.S. persons?

As was more fully explained in the Government's June 1 Submission, the presence of a tasked selector is required in order for the National Security Agency's (NSA) upstream Internet collection devices to identify and then acquire Internet communications in the form of transactions. See June 1 Submission at 1, 24-26. The Court's question in 1.a. further asks whether such transactions could include [REDACTED]

[REDACTED] s. Personal information, including that of persons other than a user of a tasked selector, could be acquired by NSA in relation to any one or more of these communication services to the extent it is included within a transaction. This, however, is true even with respect to discrete communications to, [REDACTED]

1 [REDACTED]

(S)

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

Classified by:

~~Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ~~

Reason:

~~1.4(c)~~

Declassify on:

~~28 June 2036~~



b6  
b7C  
b7D

[REDACTED]

(S//SI//NF)

Although personal information may be included in a transaction, the manner in which NSA conducts its upstream collection significantly diminishes the likelihood that such information would pertain to U.S. persons or persons in the United States. As discussed more fully in the Government's response to question 14 below, NSA acquires certain transactions because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's targeting procedures, is a non-United States person reasonably believed to be located outside the United States. NSA acquires transactions that contain a discrete communication about a tasked selector using technical means that are designed to ensure that such acquisition is directed at a person reasonably believed to be located outside the United States. The Court has previously recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC April 25, 2008) (footnote omitted) (hereinafter "*In re Directives to Yahoo!* Mem. Op."). Thus, it is reasonable to presume that most of the discrete communications that may be within an acquired transaction are between non-United States persons located outside the United States. ~~(TS//SI//OC/NF)~~

2. The June 1 Submission states that "no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication." June 1 Submission at 9.

a. What is meant by “wholly domestic communication” in this statement? Does the term include the discrete communications that might be embedded within acquired transactions?

By "wholly domestic communication" the Government means a communication as to which the sender and all intended recipients are located within the United States. The Government includes within this term any discrete communication within a transaction where the sender and all intended recipients of the discrete communication were located in the United States at the time the communication was acquired. With the previously described limited exception involving [REDACTED], NSA analysts have yet to identify a wholly domestic communication in any transaction acquired through NSA's upstream collection systems. ~~(TS//SI//NF)~~

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



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

b. What is the likelihood that an analyst viewing information obtained through a transactional acquisition would have a basis for determining that a discrete communication embedded within the transaction is purely domestic?

The likelihood that an NSA analyst would recognize that a transaction containing either a discrete communication (e.g., an e-mail message) or multiple discrete communications [REDACTED] contains a wholly domestic communication depends on a number of factors, including:

[REDACTED]

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

3.a. Might the non-targeted portion of a transaction ever be the sole basis for that transaction being responsive to an analyst's query?

Yes. All information acquired by NSA as a result of tasking the targeted foreign person's selector -- whether initially determined to be foreign intelligence information to, from, or about that targeted foreign person (or foreign intelligence information concerning other foreign persons or organizations) or incidentally acquired information concerning other currently non-targeted persons -- can be queried by analysts for foreign intelligence information. As a result, it is possible that any portion of a transaction could be the sole basis for that transaction being responsive to an analyst's foreign intelligence query of NSA databases. Such queries (which are subject to review), however, must be formulated by an analyst in accordance with NSA minimization procedures which require that computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, be limited to those selection terms reasonably likely to return foreign intelligence information. *See, e.g., Amendment 1 to*

2

~~(TS//SI//NF)~~~~TOP SECRET//COMINT//ORCON//NOFORN~~



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

DNI/AG 702(g) Certification [REDACTED] Ex. B, filed Aug. 12, 2010, § 3(b)(5) (hereinafter "Current NSA Minimization Procedures"). ~~(TS//SI//NF)~~

**3.b. Upon retrieving information in response to a query, can an analyst readily distinguish that portion of a transaction that contains the targeted selector from other portions of a transaction?**

Yes. The tasked selector that resulted in NSA's acquisition of any particular transaction is discernable by analysts reviewing information in response to a query. The analytic tools used to display an acquired transaction allow NSA analysts to identify the tasked selectors that resulted in the acquisition of the transaction, thereby enabling analysts to determine the portion(s) of the transaction in which that selector appears. In some instances, the analyst may need to review the entirety of the transaction (including the underlying metadata or raw data) to identify where the tasked selector appears, but even in these situations, the tasked selector is included and identifiable. [REDACTED]

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

**4.a. Please describe the manner in which the government minimizes discrete communications and other information that is contained within acquired Internet transactions but that is neither to, from, nor about the user of a targeted selector.**

**4.b. In particular, please explain how the government applies the provisions of NSA's minimization procedures that use the term "communication" to the discrete communications and other non-target information contained within the transactions that are acquired. See, e.g., NSA Minimization Procedures § 2(c) (defining "[c]ommunications of a United States person"); § 2(e) (defining "foreign communication" and "domestic communication[]"), § 3(b)(4) (discussing determination whether a communication is "foreign" or "domestic"), and § 5 (discussing handling of domestic communications).**

**4.c. Would all communications [REDACTED] within a transaction be treated the same when the minimization procedures are applied, or would there be different treatment?**

<sup>3</sup> The Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. See, e.g., DNI/AG 702(g) Certification [REDACTED], Ex. B, filed Apr. 20, 2011, § 3(b)(5) (hereinafter "Proposed NSA Minimization Procedures"). Under these revised NSA Section 702 minimization procedures, the use of such selection terms must be approved in accordance with NSA procedures designed to ensure that the selection terms are reasonably likely to return foreign intelligence information. *Id.* The Government is still in the process of developing the NSA procedures governing the use of United States person identifiers as selection terms. Until those procedures are completed, NSA analysts will not begin using United States person identifiers as selection terms. ~~(TS//SI//NF)~~

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



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

As required by FISA, *see* 50 U.S.C. §§ 1881a(e), 1801(h), and 1821(h), NSA's minimization procedures address the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons. *See* Current Minimization Procedures, § 1.<sup>4</sup> When NSA acquires an Internet transaction that contains multiple discrete communications, NSA considers each of those communications to be separate "communications" under its minimization procedures. Thus, for example, an NSA analyst would consider each discrete communication within a larger Internet transaction as a separate communication for purposes of determining whether the communication is a foreign or domestic communication under NSA's minimization procedures. *See, e.g.,* Current and Proposed NSA Minimization Procedures, § 2(e). ~~(TS//SI//OC/NF)~~

The manner in which acquisitions are conducted under Section 702 operates to minimize the acquisition of information about United States persons. First, certain transactions are acquired because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's FISC-approved targeting procedures, is a non-United States person reasonably believed to be located outside the United States. This Court has recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!* Mem. Op. at 87 (footnote omitted). Accordingly, it is reasonable to presume that most of the discrete communications that may be within the acquired transaction -- even those that are not to or from a tasked selector -- are between non-United States persons located outside the United States. Second, with respect to transactions that contain a discrete communication about a tasked selector, the technical means by which NSA prevents the intentional acquisition of wholly domestic communications are designed to ensure that the acquisition of transactions is directed at persons reasonably believed to be located outside the United States. As a result, these persons reasonably also can be presumed to be non-United States persons, and most of their communications -- including those that are not about a tasked selector -- can be presumed to be with other non-United States persons located outside the United States. *Id.* This combination of targeting non-United States persons located outside the United States and directing acquisitions at persons located outside the United States operates to significantly diminish the amount of information pertaining to United States persons or persons in the United States that NSA acquires through its upstream collection. *See* [REDACTED] Mem. Op. at 23 (recognizing that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that U.S. person information will be obtained"). ~~(TS//SI//OC/NF)~~

To be sure, it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain U.S. person information. The acquisition of such information is an unavoidable by-product of the acquisition of the foreign intelligence information (i.e., the communication to, from, or about a tasked selector) within the transaction. Yet it is important to note that, for purposes of the application of NSA's current and proposed minimization procedures, the Government does not consider its acquisition

<sup>4</sup> NSA's proposed minimization procedures currently before the Court address these same issues. *See* Proposed NSA Minimization Procedures § 1. ~~(S)~~

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



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

of a discrete communication within a transaction that is not to, from, or about a tasked selector to be "inadvertent." Subsection 3(b)(1) of NSA's current and proposed minimization procedures require inadvertently acquired communications to be destroyed if they are "identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or as not containing evidence of a crime which may not be disseminated under these procedures." Current and Proposed NSA Minimization Procedures, § 3(b)(1). ~~(TS//SI//NF)~~

As described below in the Government's response to question 10, the Government considers a discrete communication that is not to, from, or about a tasked selector within a transaction to be acquired "incidentally," rather than "inadvertently." In the context of minimization, "incidental" and "inadvertent" should not be considered synonymous. Given that the acquisition of the transaction is intentional, and given the Government's knowledge that such transactions may also include information that is not to, from, or about a tasked selector, the acquisition of this additional information is not "inadvertent." By contrast, the additionally acquired information is "incidental" in that it is not the basis for the collection but is rather a necessary yet unavoidable consequence of acquiring foreign communications to, from, or about a tasked selector. See [REDACTED] Mem. Op. at 40 (concluding that the Government's minimization procedures "constitute a safeguard against improper use of information about U.S. persons that is inadvertently *or* incidentally acquired") (emphasis added).<sup>5</sup> Otherwise, subsection 3(b)(1) of NSA's current and proposed minimization procedures would require the destruction of the *entire* transaction -- even the very foreign intelligence information that resulted in the transaction's acquisition in the first place -- if any discrete communication therein contained United States person information and was not to, from, or about a tasked selector. ~~(TS//SI//OC/NF)~~

Such an absurd result simply cannot be squared with Congress's explicit intent that non-pertinent information should be destroyed only if "feasible." See H.R. Rep. No. 95-1283, pt. 1, at 56 ("By minimizing retention, the committee intends that information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed *where feasible*." (emphasis added)). Congress recognized that in some cases, pertinent and non-pertinent information may be co-mingled in such a way as to make it technologically infeasible to segregate the pertinent information from the non-pertinent information and then

<sup>5</sup> The Government notes that at a single point in its June 1 Submission, it incorrectly described the acquisition of a discrete communication that is not to, from, or about a tasked selector within a transaction to be acquired "inadvertently." See June 1 Submission at 13 ("The issue for the Court in light of the above-described nature and scope of NSA's upstream collection is whether, in light of a governmental interest 'of the highest order of magnitude,' NSA's targeting and minimization procedures sufficiently protect the individual privacy interests of United States persons whose communications are inadvertently acquired."). However, the Government otherwise consistently described the acquisition of such communications as "incidental," see, e.g., *id.* at 15 ("NSA's upstream collection may incidentally acquire information concerning United States persons within transactions containing multiple discrete communications, only one of which is to, from, or about a person targeted under Section 702."); *id.* at 19 ("The fact that other, non-pertinent information within the transaction may also be incidentally and unavoidably acquired simply cannot render the acquisition of the transaction unreasonable."); *id.* ("[T]o the extent that United States person information is incidentally acquired in the acquisition of a whole transaction by NSA's upstream collection, such information will be handled in accordance with strict minimization procedures.").

~~(TS//SI//NF)~~~~TOP SECRET//COMINT//ORCON/NOFORN~~



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

destroy the latter. *See id.* ("The committee recognizes that it may not be feasible to cut and paste files or erase part of tapes where some information is relevant and some is not."). Here, it is not technologically feasible for NSA to extract, post-acquisition, only the discrete communication that is to, from, or about a tasked selector within a transaction. Thus, in order for NSA to retain the foreign intelligence information within a transaction, it must retain the entire transaction, including any incidentally acquired information about U.S. persons or persons in the United States contained therein. ~~(TS//SI//NF)~~

This incidentally acquired information in transactions is subjected to the same restrictions on use and dissemination that govern information obtained through other means pursuant to Section 702 (such as through collection at Internet Service Providers).<sup>6</sup> The Court has previously found these restrictions on use and dissemination in NSA's current minimization procedures to be consistent with the Act and the Fourth Amendment. *See, e.g., In re DNI/AG Certification* [REDACTED] Mem. Op. at 8-12 (USFISC [REDACTED] 2010); *In re DNI/AG Certification* [REDACTED] Mem. Op. at 8-15 (USFISC [REDACTED] 2009). Of course, the Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. As discussed in its response to question 14 below, the Government respectfully suggests that these revised NSA minimization procedures are also consistent with the Act and the Fourth Amendment. ~~(TS//SI//OC/NF)~~

In sum, NSA treats each discrete communication contained within a larger Internet transaction as a separate communication for purposes of its minimization procedures. Although it is possible that certain discrete communications containing United States person information will be retained, as described above, they remain subject to the same restrictions on use and dissemination imposed by NSA's minimization procedures. ~~(TS//SI//OC/NF)~~

**5.a. Once NSA has identified a portion of a transaction that does not contain targeted information, is it possible to mask or otherwise minimize the non-target information contained within the transaction?**

No. The analytic tools used to display the acquired data to NSA analysts do not have a capability to mask information or otherwise minimize the non-target information contained within a transaction. See additional details provided in response to question 6 below.  
~~(TS//SI//NF)~~

<sup>6</sup> Moreover, as discussed in response to question 3.b. above, NSA's inability to separate the discrete communications post-acquisition also means that the discrete communications are not displayed in NSA's SC-SSRs as separate communications, but rather clearly retain their connection to the entirety of the original transaction, making it more apparent to NSA analysts the discrete communication's relationship to a tasked selector.

~~(TS//SI//OC/NF)~~~~TOP SECRET//COMINT//ORCON//NOFORN~~



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

5.b. Why is NSA unable to delete and replace, or alter, an original transaction that contains non-target information? See June 1 Submission at 27-28.

The answer to this question is included in the response to question 6 below. ~~(TS//SI//NF)~~

6. The government states that an Internet transaction that is acquired "is... not divisible into the discrete communications within it even once it resides in an NSA corporate store." June 1 Submission at 22. Please reconcile that statement with the government's acknowledgment that "an analyst would . . . be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system." Id. at 27 n.25.

As discussed in the example of [REDACTED] information on pages 27-28 of the June 1 Submission, the data within such transactions is organized in a fashion meant to be displayed using [REDACTED], which is not necessarily a format in which discrete communications that may be contained within the transaction are distinguishable. In order for NSA to identify and separate a transaction containing multiple communications into those component parts, the transaction would require processing, parsing, and reformatting for those components intended for subsequent retention as separate communications. This is true at the point of acquisition and at any point post-acquisition, including at the point of display to the analyst, whether the intent is to separate out a particular communication from the transaction for the purpose of deleting it, replacing it, masking it, or otherwise altering it.

[REDACTED]  
~~(TS//SI//OC/NF)~~

Absent [REDACTED] capabilities as discussed above, attempts by NSA analysts to delete, replace or otherwise alter (e.g., mask or otherwise minimize the non-target information contained within the transaction) a portion of a transaction intercepted through NSA's upstream collection techniques could similarly corrupt the integrity of the collection, destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including any particular communication therein for analytic or other purposes. Maintaining the integrity of original transactions is paramount to NSA's retention and dissemination processes. Specifically, NSA has developed and implemented a comprehensive purge process designed to improve the completeness of data purges. The efficacy of this process depends in large measure on NSA's ability to trace data back to the original object (such as a transaction) in a SIGINT Collection - Source Systems of Record (SC-SSR). Maintaining the integrity of original transactions is also important for ensuring quality control of NSA's foreign intelligence analysis of Internet communications, which frequently may contain more than one tasked selector or could be used by more than one analyst, depending on the target, mission, or specific foreign intelligence need to which it pertains. Thus, preserving the integrity of the data is dependent upon the retention of the original transaction in its original form as stored in the SC-SSR. ~~(TS//SI//OC/NF)~~

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



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

The government's representation that an Internet transaction that is acquired "is... not divisible into the discrete communications within it even once it resides in an NSA corporate store" was intended to convey that it is not technologically feasible for NSA to create [REDACTED] processes to divide transactions into discrete communications. Footnote 25 on page 27 of the June 1 Submission refers to the fact that it is possible for individual analysts to copy some of the information from a transaction in NSA corporate stores into a new document or file stored on a separate system, such as a [REDACTED]. See, e.g., DNI/AG 702(g) Certification Trans. of Proceedings at 20-21 ([REDACTED] 2010) (for a discussion of [REDACTED]). The fact that such a copy or extract can be made, however, does not mean that the underlying transaction can then be altered in the corporate store. For example, if an analyst copied a portion of a transaction from an SC-SSR into a [REDACTED] and then purged the transaction from the SC-SSR, the data copied into the [REDACTED] would likewise have to be purged -- even if it contained foreign intelligence information copied from a communication to, from, or about a tasked selector -- because it could no longer be traced back to an object present in an SC-SSR. ~~(TS//SI//OC/NF)~~

7. Please reconcile the government's statement that the "communicants" of to/from communications are "the individual users of particular selectors" (see June 1 Submission at 30) with [REDACTED] elsewhere in its response to the Court's questions (see, e.g., *id.* at 6 (discussing application of IP filtering)).

The Government believes its statement that [REDACTED] in the case of to/from communications is fully consistent with the Government's description of how NSA [REDACTED] to determine if one end of a to/from communication is outside of the United States. As stated on page 30 of the June 1 Submission, the communicants in to/from communications are the individual users who are the senders and intended recipients of those communications, rather than [REDACTED]. ~~(TS//SI//OC/NF)~~

With respect to IP filtering, however, in many instances it is not possible for NSA to [REDACTED]. See June 1 Submission at 6-7. [REDACTED]

See, e.g., *id.* at 11. ~~(TS//SI//OC/NF)~~

As described in the June 1 Submission, there are scenarios under which NSA could unknowingly and unintentionally acquire a to/from communication in which the sender and all intended recipients are in the United States at the time of acquisition -- for example, if that

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



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

communication [REDACTED]<sup>7</sup> In the unlikely event that NSA does unintentionally acquire such a communication, NSA will purge the communication unless its continued retention is authorized by the Attorney General in accordance with 50 U.S.C. § 1806(i). If the communication is itself contained within a transaction that contains other discrete communications, the whole transaction will be purged unless its continued retention is authorized by the Attorney General in accordance with 50 U.S.C. § 1806(i), regardless of whether those other discrete communications are foreign. ~~(TS//SI//OC/NF)~~

8. What is the factual basis for NSA's assertions that "a United States person would [REDACTED] only in a minute percentage of cases" and that [REDACTED]

[REDACTED] ? See June 1 Submission at 11, 12.

These factual assertions by NSA are based upon the assessments of NSA Signals Intelligence (SIGINT) personnel, who have been involved in NSA's Section 702 acquisitions since the initiation of that collection, and many of whom have experience [REDACTED] NSA's factual assertions in the June 1 Submission are also based on its review of a sampling of Section 702-acquired communications, which is described on page 9 of the June 1 Submission. As is more fully discussed in that filing, NSA's review of [REDACTED] records between these two tests revealed only [REDACTED] records indicative of a non-targeted user [REDACTED] in the United States. Further research revealed that these [REDACTED] records were actually copies of the same transaction, and NSA found no indication that any wholly domestic communications were within this transaction. NSA assesses that the results of these tests are consistent with the assessments made by NSA's SIGINT personnel in the June 1 Submission. ~~(TS//SI//OC/NF)~~

9. What is the factual basis for NSA's suggestion that [REDACTED] [REDACTED] ? See June 1 Submission at 8 n.9.

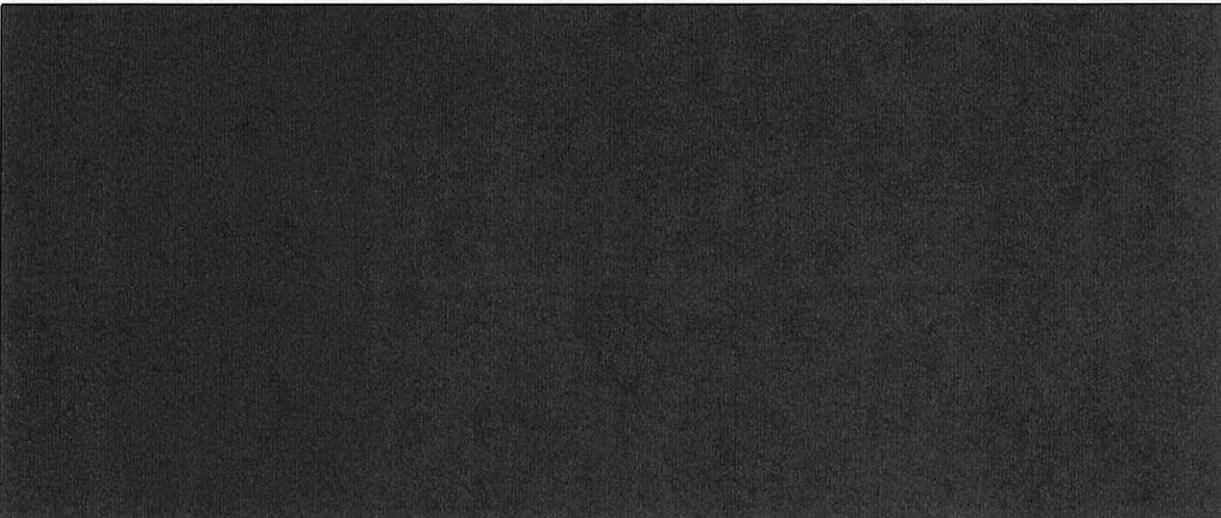
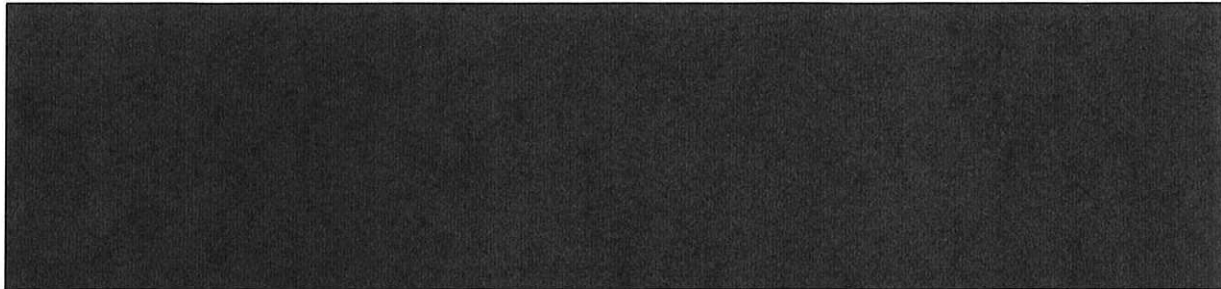
<sup>7</sup> As previously described, it would be very unlikely for [REDACTED] in which the sender and all intended recipients are located inside the United States. See June 1 Submission at 11. Moreover, with the previously described limited exception [REDACTED] see *id.* at 6 & n.5, NSA analysts have yet to identify a wholly domestic communication acquired through NSA's upstream collection systems. See *id.* at 9 (noting NSA's experience to date and describing NSA's test samples, stating that the only records possibly indicative of a United States-based user [REDACTED] did not reveal that any wholly domestic communications had been acquired).

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

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



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



10. The government repeatedly characterizes as “unintentional” NSA’s collection of discrete non-target communications as part of transactional acquisitions, [REDACTED] [REDACTED] Assuming arguendo that such collection can fairly be characterized as unintentional, please explain how 50 U.S.C. § 1806(i) applies to the discrete, wholly domestic communications that might be contained within a particular transaction.

Subsection 1806(i) provides that “[i]n circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication,<sup>8</sup> under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located in the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicates a threat of death or serious bodily harm to any person.” (U)

The Government’s June 1 Submission described for the Court that at the time of acquisition, NSA’s Section 702 upstream Internet collection devices are generally not capable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which

<sup>8</sup> Subsection 1806(i) originally covered only radio communications, but was amended in 2008 to cover all communications to make it technology neutral. See 154 Cong. Rec. S6133 (daily ed. June 25, 2008). (U)

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



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

may be to, from, or about a tasked selector at the time of acquisition.<sup>9</sup> See June 1 Submission at 7, 27-28. The Government considers the acquisition of communications within a transaction that are not to, from, or about a tasked selector to be incidentally acquired communications. However, the Government does not intend to acquire transactions containing communications that are wholly domestic in nature and in fact has implemented [REDACTED] means to prevent the acquisition of such transactions. While those [REDACTED] means could fail (as was the case involving the previously reported [REDACTED]), or be circumvented [REDACTED]

[REDACTED] NSA is nevertheless not intending to acquire wholly domestic communications. Thus, in the context of acquiring Internet transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector, the Government recognizes that subsection 1806(i) could potentially be implicated to the extent that one of those discrete communications is a communication in which the sender and all intended recipients were located in the United States at the time of acquisition. Accordingly, in the event NSA recognizes a wholly domestic communication which is not to, from, or about a tasked selector which it has unintentionally acquired in the course of conducting its Section 702 upstream Internet collection, NSA would handle the entire transaction in accordance with subsection 1806(i) and either purge it or, if appropriate, seek authorization from the Attorney General to retain it. ~~(TS//SI//OC/NF)~~

NSA's minimization procedures, adopted by the Attorney General in consultation with the Director of National Intelligence, allow the Director of NSA to execute a waiver permitting the retention of wholly domestic communications. See Current and Proposed NSA Minimization Procedures, § 5. However, this provision applies to the acquisition of domestic communications when the Government has a reasonable, but mistaken, belief that the target is a non-United States person located outside the United States because NSA is intentionally but mistakenly acquiring such communications.<sup>10</sup> This domestic communications carve-out does not apply to an unintentionally acquired transaction that contains a wholly domestic communication (when recognized as such by NSA) along with other discrete communications, which is not to, from, or about a tasked selector. As described previously, NSA's Section 702 upstream Internet collection devices are generally incapable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector at the time of acquisition; moreover, NSA cannot separate transactions containing multiple discrete communications into logical constituent parts post-acquisition. Thus, in the event that NSA's Section 702 upstream Internet collection resulted in the unintentional acquisition of a transaction containing a wholly domestic communication, consistent with subsection 1806(i), NSA would purge the entire transaction, unless the Attorney General has authorized its retention after first

<sup>9</sup> NSA additionally advised the Court that except in certain limited circumstances, NSA cannot separate transactions into logical constituent parts post-acquisition either without rendering the transaction unusable for analytic or other purposes. See June 1 Submission at 27 & n.27. ~~(TS//SI//OC/NF)~~

<sup>10</sup> See Government's Analysis of Section 1806(i), DNI/AG 702(g) Certification [REDACTED] Docket No. 702(i)-08-01, filed Aug. 28, 2008; [REDACTED] Mem. Op. at 25-27. ~~(TS//SI//OC/NF)~~

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



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

determining that its contents indicated a threat of death or serious bodily harm to any person.<sup>11</sup>

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

11. Please provide a thorough legal analysis supporting your view that the knowing and intentional acquisition of large volumes of Internet transactions containing discrete communications that are neither to, from, nor about a targeted selector (as well as other information not pertaining to the users of targeted selectors) is merely "incidental" to the authorized purpose of the collection as a whole, and therefore reasonable under the Fourth Amendment.

Fourth Amendment reasonableness is concerned only with the effect on Fourth Amendment protected interests. Thus, in evaluating reasonableness under the Fourth Amendment, the relevant issue for the Court in considering the acquisition of communications incidental to the purpose of this collection is the extent to which such incidental communications involve United States persons or persons located in the United States. Cf. [REDACTED] Mem. Op. at 37-38 (recognizing that non-U.S. persons outside the United States "are not protected by the Fourth Amendment" (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990))). For the reasons more particularly explained in the Government's responses to question 1 above and question 14 below, most of the communications incidentally acquired pursuant to this collection have no effect on any Fourth Amendment protected interests. The Government acknowledges that it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain information pertaining to United States persons or persons located in the United States. That, however, does not mean that the acquisition of multiple discrete communications is any more likely to result in the acquisition of United States person information than in the collection of single, discrete communications to, from, or about a non-United States person located outside the United States. This is particularly true because the technology NSA uses to prevent the acquisition of wholly domestic communications also acts to limit the acquisition of communications among and between United States persons.<sup>12</sup> ~~(TS//SI//OC/NF)~~

<sup>11</sup> See also the Government's response to question 7 above, which explains that there are other scenarios under which NSA could unknowingly and unintentionally acquire a wholly domestic communication. In the unlikely event that NSA does unintentionally acquire such a communication, NSA will purge the communication upon recognition unless its continued retention is authorized by the Attorney General in accordance with subsection 1806(i). If the communication is itself contained within a transaction that contains other discrete communications, the whole transaction will be purged unless its continued retention is authorized by the Attorney General in accordance with subsection 1806(i), regardless of whether those other discrete communications are foreign.

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

<sup>12</sup> For example, the Court has expressed particular concern regarding the acquisition of [REDACTED]

~~(TS//SI//OC/NF)~~~~TOP SECRET//COMINT//ORCON/NOFORN~~



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

Moreover, even with respect to those instances in which U.S. person information is acquired, courts in both the FISA and criminal (Title III) contexts have recognized that the acquisition of communications incidental to the purpose of a collection may be necessary to achieve the goal of a search or surveillance, as well as reasonable under the Fourth Amendment. See, e.g., *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1015 (Foreign Int. Surv. Ct. Rev. 2008) (hereinafter "*In re Directives*") ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted)); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000), *aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008), *cert. denied sub nom. El-Hage v. United States*, 130 S.Ct. 1050 (2010) ("[I]ncidental interception of a person's conversations during an otherwise lawful [Title III] surveillance is not violative of the Fourth Amendment."). ~~(TS//SI//OC/NF)~~

In cases where NSA acquires Internet transactions that include multiple discrete communications, the Government considers any discrete communications not to, from, or about the tasked selector to be incidentally acquired. Specifically, the Government's purpose in acquiring such a transaction is to acquire the foreign intelligence information likely contained within the discrete communication to, from, or about a tasked selector. However, because it is technologically infeasible for NSA's upstream collection systems to extract only the discrete communication that is to, from, or about a tasked selector, the only way to obtain the foreign intelligence information in that discrete communication is to acquire the entire transaction. Thus, the acquisition of the other discrete communications within the transaction is properly considered "incidental," because it is a necessary but unavoidable consequence of achieving the Government's goal of acquiring the foreign intelligence information contained within the discrete communication to, from, or about a tasked selector. See H.R. Rep. No. 95-1283, pt. 1, at 55 (1978) (noting that "in many cases it may not be possible for technical reasons to avoid acquiring all information" when conducting foreign intelligence surveillance); see also *id.* at 56 ("[I]t may not be possible or reasonable to avoid acquiring all conversations."); cf. *United States v. McKinnon*, 721 F.2d 19, 23 (1st Cir. 1983) ("Evidence of crimes other than those authorized in a [Title III] wiretap warrant are intercepted 'incidentally' when they are the by-product of a bona fide investigation of crimes specified in a valid warrant."). ~~(TS//SI//OC/NF)~~

That is not to say, however, that the acquisition of non-pertinent information is reasonable in all cases simply because the collection of that information is "incidental" to the purpose of the search. *United States v. Ulrich*, 228 Fed. Appx. 248, 252 (4th Cir. 2002) (noting that "fishing expeditions" or "a random exploratory search or intrusion" violate the Fourth Amendment) (quotation marks omitted). Here, NSA's acquisition of transactions is conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed "toward communications that are likely to yield the foreign intelligence information sought, and thereby afford a degree of particularity that is reasonable under the Fourth Amendment." [REDACTED] Mem. Op. at 39-40 (footnote omitted). The fact that such transactions may contain non-pertinent information -- even in significant amounts -- does not by itself render the acquisition of those transactions unreasonable under the Fourth Amendment. See *Scott v. United States*, 436 U.S. 128, 140 (1978) (recognizing that "there are surely cases,

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



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

such as the one at bar [involving a Title III wiretap], where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable"); *Abraham v. County of Greenville*, 237 F.3d 386, 391 (4th Cir. 2001) ("[I]ncidental overhearing is endemic to surveillance."); *United States v. Doolittle*, 507 F.2d 1368, 1372 (5th Cir. 1975) ("There is no question that some irrelevant and personal portions of gambling conversations were intercepted or that certain nonpertinent conversations were intercepted. But this is inherent in the type of interception authorized by Title III, and we do not view the simple inclusion of such conversations, without more, as vitiating an otherwise valid wiretap.")<sup>13</sup>; see also, e.g., *Board of Educ. v. Earls*, 536 U.S. 822, 837 (2002) ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotations marks omitted)).

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

As such, the incidental collection at issue here is reasonable under the Fourth Amendment because it is a necessary and unavoidable by-product of NSA's effort to obtain the foreign intelligence information contained within a discrete communication that is a part of a larger transaction which could contain non-pertinent communications. See *United States v. Wuagneux*, 683 F.2d 1343, 1352-53 (11th Cir. 1982) (observing that "a search may be as extensive as reasonably required to locate the items described in the warrant," and on that basis concluding that it was "reasonable for the agents [executing the search] to remove intact files, books, and folders when a particular document within the file was identified as falling within the scope of the warrant"); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence sought may be seized"). Moreover, as described in the response below, NSA takes the steps it can to ensure that it conducts its Section 702 upstream collection in a manner that minimizes the intrusion into the personal privacy of United States persons. ~~(TS//SI//OC/NF)~~

12. The statute requires the targeting procedures to "be reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and [to] prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). How can procedures that contemplate the knowing acquisition of huge volumes of transactions that will include quantifiable amounts of information relating to non-targets, including information of or about U.S. persons abroad or persons located in the United States, meet this statutory requirement?

<sup>13</sup> These cases upholding the Fourth Amendment reasonableness of Title III surveillances that resulted in the acquisition of significant amounts of nonpertinent communications are particularly noteworthy given that Title Iain's requirement to minimize the acquisition of such communications is considerably stricter than FISA's. See H.R. Rep. 95-1283, pt. 1, at 56 ("It is recognized that given the nature of intelligence gathering, minimizing acquisition should not be strict as under [Title III] with respect to law enforcement surveillances."). ~~(TS//SI//NF)~~

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



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

For the reasons more particularly discussed in its response to question 1.b.ii. in the June 1 Submission, which took into account the means by which communications to, from, or about a tasked selector are acquired through NSA's upstream Internet collection techniques, the Government respectfully submits that NSA's targeting procedures are reasonably designed to ensure that an authorized acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located within the United States. See June 1 Submission at 3-12, 20-24. As discussed in the Government's June 1 Submission, for acquisition of both to/from communications and abouts communications, the person being "targeted" is the user of the tasked selector, who, by operation of the targeting procedures, is a non-United States person reasonably believed to be located outside the United States. See June 1 Submission at 3-4. This remains true for all Section 702 upstream acquisitions, including the acquisition of transactions containing several discrete communications, only one of which may be to, from, or about the user of a tasked selector. ~~(TS//SI//NF)~~

Specifically, the sole reason a transaction is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been targeted in accordance with NSA's targeting procedures.<sup>14</sup> Indeed, at the time a transaction is acquired, NSA cannot always know whether the transaction includes other data or information representing communications that are not to, from, or about the target, let alone always have knowledge of the parties to those communications. Cf. [REDACTED] Mem. Op. at 18-19 (noting that with respect to abouts communications, "the government may have no knowledge of [the parties to a communication] prior to acquisition"). It therefore cannot be said that the acquisition of a transaction containing multiple discrete communications results in the intentional targeting of any of the parties to those communications other than the user of the tasked selector. Cf. *Bin Laden*, 126 F. Supp. 2d at 281 (acknowledging that in light of *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990), and Title III "incidental interception" case law, overseas surveillance of a United States person terrorism suspect would have posed no Fourth Amendment problem "if the Government had not been aware of [his] identity or of his complicity in the [terrorism] enterprise"). The fact that a transaction acquired pursuant to the targeting procedures may also contain communications to, from, or about persons other than the user of the tasked selector does not mean those persons are likewise being targeted by that acquisition. Cf. H.R. Rep. No. 95-1283, pt. 1, at 50 (explaining, with regard to electronic surveillance as defined by 50 U.S.C. § 1801(f)(1), that "[t]he term 'intentionally targeting' includes the deliberate use of surveillance techniques which can monitor numerous channels of communication among numerous parties, where the techniques are designed to select out from among those communications the communications to which a particular U.S. person located in the United States is a party, and where the communications are

<sup>14</sup> [REDACTED]

[REDACTED] ~~(TS//SI//NF)~~

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



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

selected either by name or by other information which would identify the particular person and would select out his communications"). Rather, as discussed in the response to question 11 above, the acquisition of such non-pertinent communications is incidental to the purpose of the collection as a whole and therefore reasonable under the Fourth Amendment. ~~(TS//SI//NF)~~

Similarly, to the extent that one of the discrete non-pertinent communications within an acquired transaction is a communication in which the sender and all intended recipients were located in the United States at the time of acquisition, the acquisition of this wholly domestic communication would be incidental and, as discussed in response to question 10 above, unintentional. NSA's targeting procedures require that, in conducting upstream collection of abouts communications, NSA either employ "an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas" or "[redacted] E.g., Amendment 1 to DNI/AG 702(g) Certification [redacted] Ex. A, filed [redacted] 2010, at 1-2; see also [redacted] Mem. Op. at 19. The Court has previously found that these [redacted] means were "reasonably designed to prevent the intentional acquisition of communications as to which all parties are in the United States," while recognizing that it is "theoretically possible that a wholly domestic communication could be acquired as a result of the [redacted] [redacted] Mem. Op. at 20 & n.17. As discussed in the June 1 Submission, apart from one exception involving [redacted] NSA analysts have yet to identify a wholly domestic communication acquired through NSA's upstream collection systems. See June 1 Submission at 8-9. Accordingly, the Government continues to believe that NSA's [redacted] means for preventing the acquisition of wholly domestic communications remain efficacious, and that the theoretical scenarios in which NSA would acquire a wholly domestic communication do not prevent the Court from continuing to find that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//OC/NF)~~

To the extent that NSA does unintentionally acquire and then recognize such a wholly domestic communication within an acquired transaction, as described in response to question 10 above, NSA would be required to purge the entire transaction, unless the Attorney General determined "that the contents indicate[d] a threat of death or serious bodily harm to any person." ~~(TS//SI//OC/NF)~~

13. In its discussion of the Fourth Amendment, the government asserts that "upstream collection" in general is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs." June 1 Submission at 16.

a. To what extent can the same be said for the acquisition of Internet transactions [redacted] [redacted] in particular?

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



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

b. Is the acquisition of Internet transactions via upstream collection the only source for certain categories of foreign intelligence information? If so, what categories?

c. Please describe with particularity what information NSA would acquire, and what information NSA would not acquire, if NSA were, in comparison to its current collection, to limit its acquisition of Internet communications to: (1) acquisitions conducted with the assistance of [REDACTED]; and (2) the upstream collection of discrete communications to, from, or about tasked selectors that are [REDACTED] (id. at 2, n.2).

The Government's assertion that upstream collection is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs" is equally applicable to its acquisition of Internet transactions. This is true because the Government's acquisition of Internet transactions is not a subset of its upstream collection of Internet communications. Instead, acquisition of Internet transactions is the technical means by which all upstream collection of Internet communications accounts are acquired. ~~(TS//SI//NF)~~

Section 702 upstream collection of Internet communications provides NSA with certain types of information (further described below) which are extremely valuable to its national security mission. Disseminated end product reports derived from this collection have proven to be of critical value to high-level customers, including the White House, State Department, Joint Chiefs of Staff, the National Counterproliferation Center, Central Intelligence Agency (CIA), Defense Intelligence Agency, Federal Bureau of Investigation (FBI), and others. In addition,

[REDACTED]

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

[REDACTED]

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

Section 702 upstream collection offers unique opportunities to detect target information, including but not limited to the following examples:

[REDACTED]

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



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

[REDACTED]

[REDACTED] (TS//SI//NF)

[REDACTED] As such, and as the Court has recognized, NSA's upstream collection is "*uniquely capable* of acquiring certain types of targeted communications containing valuable foreign intelligence information." *In re DNI/AG Certification* [REDACTED] Mem. Op. at 25-26 (USFISC [REDACTED] 2009) (emphasis added; internal citations omitted). (TS//SI//NF)

Additionally, NSA's Section 702 upstream collection would not acquire many of the above categories of communications, and thus the foreign intelligence contained within these communications, if NSA's upstream collection were limited to acquisition solely of discrete communications to, from, or about tasked selectors that are [REDACTED] referenced in footnote 2 on page 2 of the June 1 Submission. Currently,

[REDACTED] (TS//SI//NF)

15 [REDACTED] (TS//SI//NF)

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



~~TOP SECRET//COMINT//ORCON//NOFORN~~~~(TS//SI//NF)~~~~(TS//SI//NF)~~

The Court's question asks for "categories of foreign intelligence information" that can be obtained exclusively through NSA's acquisition of Internet transactions via upstream collection. This is a difficult question to answer, as types of foreign intelligence may be conveyed through a variety of communication means. For example,

as described above, it is entirely possible that this communication may only be acquired through NSA's Section 702 upstream collection of communications other than those

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

In an effort to fully answer the Court's question, however, the Government respectfully submits the following examples of instances where NSA has obtained substantial foreign intelligence information from Section 702 upstream collection. The examples detail only a few

~~(TS//SI//NF)~~~~TOP SECRET//COMINT//ORCON//NOFORN~~



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

of the many instances in which Section 702 upstream collection has provided such substantial foreign intelligence. In many of these examples, Section 702 upstream collection provided important leads that led to [REDACTED]. Although all forms of Section 702 upstream collection have proved to be of critical importance to the NSA's national security mission, the examples below involve the acquisition by Section 702 upstream collection of communications other than [REDACTED]

~~(TS//SI//NF)~~  
(S)~~(TS//SI//NF)~~  
(S)~~TOP SECRET//COMINT//ORCON//NOFORN~~



~~TOP SECRET//COMINT//ORCON/NOFORN~~~~(TS//SI//NF)~~~~(U//FOUO)~~

14. The Fourth Amendment also requires the Court to examine the nature and scope of the intrusion upon protected privacy interests. How can the Court conduct such an assessment if the government itself is unable to describe the nature and scope of the information that is acquired or the degree to which the collection includes information pertaining to U.S. persons or persons located in the United States?

Although, as discussed above, it is difficult for the Government to fully describe to the Court every possible type of information that may be contained within a transaction acquired through NSA's upstream collection, the Government respectfully suggests that the Court can nonetheless assess whether NSA's upstream collection of such transactions is reasonable under the Fourth Amendment. ~~(TS//SI//OC/NF)~~

First, the Supreme Court has recognized that an appreciation of all of the possible ways a search can intrude upon interests protected by the Fourth Amendment is not an indispensable component of assessing the reasonableness of the search. *See Dalia v. United States*, 441 U.S. 238, 257 (1979) ("Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."); *cf. Payton v. New York*, 445 U.S. 573, 601-02 (1980) (recognizing that "for Fourth Amendment purposes, an arrest warrant founded on probable cause implicitly carries with it the limited authority to enter a dwelling in which the suspect lives when there is reason to believe the suspect is within," even though "an arrest warrant requirement may afford less [privacy] protection than a search warrant requirement"). Thus, the Government respectfully suggests that the Court can assess the Fourth Amendment reasonableness of NSA's upstream collection even if the Government cannot fully describe every possible type of information that collection may acquire. ~~(TS//SI//OC/NF)~~

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

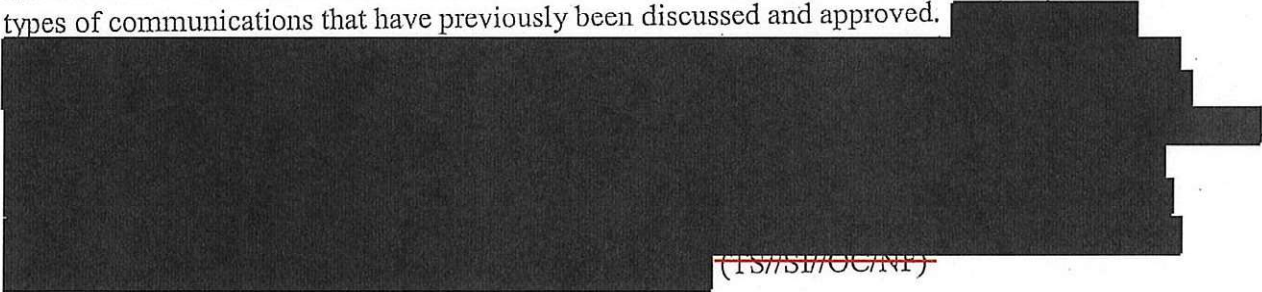


~~TOP SECRET//COMINT//ORCON/NOFORN~~

Moreover, while it may be difficult for the Government to describe the full scope of the types of information that may be acquired by NSA's upstream collection, it is nevertheless possible to ascertain the degree to which that information would pertain to United States persons or persons located in the United States. For the reasons discussed below, the Government does not believe that information about United States persons or persons located in the United States would be acquired through NSA's upstream collection of transactions to a greater degree, in relative terms, than other types of communications acquired under Section 702. ~~(TS//SI//OC/NF)~~

First, certain transactions are acquired because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's FISC-approved targeting procedures, is a non-United States person reasonably believed to be located outside the United States. This Court has recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!* Mem. Op. at 87 (footnote omitted). Accordingly, it is reasonable to presume that most of the discrete communications that may be within the acquired transaction are between non-United States persons located outside the United States. Second, with respect to transactions that contain a discrete communication about a tasked selector, the technical means by which NSA prevents the intentional acquisition of wholly domestic communications is to ensure that the acquisition of transactions is directed at persons reasonably believed to be located outside the United States. Again, these individuals reasonably can be presumed to be non-United States persons, and most of their communications can be presumed to be with other non-United States persons located outside the United States. *Id.* This combination of targeting non-United States persons located outside the United States and directing acquisitions at persons located outside the United States operates to significantly diminish the likelihood that information pertaining to United States persons or persons in the United States will be acquired. ~~(TS//SI//OC/NF)~~

To be sure, it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain information pertaining to United States persons or persons in the United States. That, however, does not by itself mean that the volume of such information in transactions will be greater than in the collection of other types of communications that have previously been discussed and approved.



Moreover, the fact that within an acquired transaction there may be multiple discrete communications containing information pertaining to United States persons or persons in the United States cannot by itself render the acquisition of that transaction unreasonable under the Fourth Amendment. As discussed above, the acquisition of such information is incidental to the purpose of the transaction's acquisition -- the acquisition of the discrete communication(s) to,

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



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

from, or about a tasked selector within the transaction. *See In re Directives*, 551 F.3d at 1015 (“It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.”) (citations omitted)). ~~(TS//SI//OC/NF)~~

In any event, any information pertaining to a United States person or person located in the United States present in a transaction containing multiple discrete communications would be handled under the NSA minimization procedures in the exact same manner as if that information appeared in a discrete communication to, from, or about a tasked selector. For example, the use and dissemination of United States person information acquired from a [REDACTED] would be subject to the same restrictions as United States person information acquired from [REDACTED]

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

**15. In light of the government’s emphasis on the limited querying of Section 702 acquisitions that is currently permitted (see June 1 Submission at 23), why is it reasonable and appropriate to broaden the targeting procedures to permit querying using U.S.-person identifiers?**

Although NSA’s current minimization procedures prohibit the use of United States person names or identifiers to retrieve any Section 702-acquired communications in NSA systems, *see* Current NSA Minimization Procedures, § 3(b)(5), the statute requires no such limitation. Rather, it is reasonable and appropriate for the Court to approve the Government’s proposal to enable NSA analysts to use United States person identifiers as selection terms because the request is consistent with the statutorily required minimization procedures. *See* Proposed NSA Minimization Procedures § 3(b)(5) (providing, in pertinent part, that “[c]omputer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Any United States person identifiers used as terms to identify and select communications must be approved in accordance with NSA procedures.”) (emphasis added). ~~(TS//SI//OC/NF)~~

Minimization procedures must be designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. 50 U.S.C. § 1801(h)(1). Where, as here, “it may not be possible for technical reasons to avoid acquiring all information,” Congress has recognized that minimization procedures “must emphasize the minimization of retention and dissemination.” H.R. Rep. No. 95-1283, pt. 1, at 55. Congress also acknowledged that “a significant degree of latitude be given in counterintelligence and counterterrorism cases” with respect to retention and dissemination of information. *Id.* at 59. In light of such latitude, “rigorous and strict controls” should -- and will -- be placed on the retrieval of United States person information and “its dissemination or use for purposes other than counterintelligence or counterterrorism.” *Id.*

~~(TS//SI//OC/NF)~~~~TOP SECRET//COMINT//ORCON//NOFORN~~



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

With respect to acquisition, the Government's proposal to use United States person identifiers as selection terms does not broaden the scope of what the Government can acquire under the certifications. Because, for the reasons detailed above, it is not possible "to avoid acquiring" the incidentally obtained information, the focus will be on the retention and dissemination provisions of the procedures. *Id.* at 55. As a general matter, NSA's minimization procedures contain detailed provisions regarding the retention and dissemination of United States person information that the Court has previously approved. *See, e.g.,* [REDACTED] mem. Op. at 21-32, 40-41. In addition, the Government's proposal provides that United States person identifiers may only be used "in accordance with NSA procedures" governing the circumstances under which U.S. person information can be queried. Although the Government is still developing such procedures, and NSA analysts will not begin using United States identifiers as selection terms until they are completed, the Government will ensure that the procedures contain "rigorous and strict controls" for the retrieval and dissemination of United States person information to ensure that only selection terms likely to produce foreign intelligence information are retrieved, and dissemination is limited to counterintelligence and counterterrorism purposes. Moreover, the Government's proposed changes to NSA's minimization procedures require that NSA maintain records of all United States person identifiers approved for use as selection terms and that NSD and ODNI conduct oversight of NSA's activities. *See Proposed NSA Minimization Procedures* § 3(b)(5). ~~(TS//SI//OC/NF)~~

16. The government acknowledges that it previously "did not fully explain all of the means by which . . . communications are acquired through NSA's upstream collection techniques" (June 1 Submission at 2), yet states that the "[Attorney General] and [Director of National Intelligence] have confirmed that their prior authorizations remain valid" (*id.* at 35). At the time of each previous Certification under Section 702, were the Attorney General and the Director of National Intelligence aware that the acquisitions being approved included Internet "transactions" [REDACTED]? If so, why was the Court not informed? If not, why are the prior Certifications and collections still valid?

The Government acknowledges that its prior representations to the Court -- and to the Attorney General and Director of National Intelligence -- regarding the steps NSA must take in order to acquire single, discrete communications to, from, or about a tasked selector did not fully explain all of the means by which such communications are acquired through NSA's upstream Internet collection techniques. *See June 1 Submission* at 2. That said, for the reasons described in the answer to question 5 in the June 1 Submission, both the prior Certifications and collection remain valid. *See June 1 Submission* at 31-38. ~~(TS//SI//OC/NF)~~

The Certifications executed by the AG and DNI and submitted to the Court for approval were based on an understanding that Section 702 collection would, at a minimum, acquire discrete communications that are to, from, or about a tasked selector. As described in detail previously, due to certain technological limitations, in general the only way that NSA can acquire certain Internet communications upstream that are to, from, or about a tasked selector is by acquiring an Internet transaction which may include a single, discrete communication to, from, or about a tasked selector (e.g., an e-mail message) or may include several discrete

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



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

communications, only one of which may be to, from, or about a tasked selector.<sup>17</sup> See June 1 Submission at 27-28. In this respect, the acquisition is comparable to the Government's seizure of a video, book, or intact file that contains a single photo, page, or document that a search warrant authorizes the Government to seize. See, e.g., *United States v. Rogers*, 521 F.3d 5, 10 (1st Cir. 2008) (concluding that a videotape is a "plausible repository of a photo" and that therefore a warrant authorizing seizure of "photos" allowed the seizure and review of two videotapes, even though warrant did not include videotapes); *Wuagneux*, 683 F.2d at 1353 (holding that it was "reasonable for the agents to remove intact files, books and folders when a particular document within the file was identified as falling within the scope of the warrant."); *United States v. Christine*, 687 F.2d 749, 760 (3d Cir. 1982) (*en banc*) (emphasizing that "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision. Nor does the Fourth Amendment prohibit seizure of an item, such as a single ledger, merely because it happens to contain other information not covered by the scope of the warrant."); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence may be seized"). None of these cases even hint that the warrant is somehow invalid because the magistrate did not know in advance that the search or seizure of authorized documents or photos would also encompass the search or seizure of additional, intermingled documents or photos, even in cases where such documents could have been physically separated from the larger files or books in which they were contained. Rather, it is well-established that warrants need not state with specificity the precise manner of execution, and, so long as it is reasonable, a search or seizure will be upheld even if conducted in a manner that invades privacy in a manner not considered at the time the warrant was issued. See *United States v. Grubbs*, 547 U.S. 90, 98 (2006) ("Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.") (citation omitted); *Dalia*, 441 U.S. at 259 ("Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."). ~~(TS//SI//OC/NF)~~

Moreover, having considered the additional information that is being presented to this Court, the AG and DNI have confirmed that the collection fully complies with the statutory requirements of Section 702, as well as the Fourth Amendment, and that therefore the prior Certifications and collection remain valid. See June 1 Submission at 35. ~~(TS//SI//OC/NF)~~

As discussed previously, transactions are only acquired if they contain at least one discrete communication to, from, or about a tasked selector. Each tasked selector has undergone review, prior to tasking, to ensure that the user is a non-United States person reasonably believed to be outside the United States. Moreover, with respect to "abouts communications," the targeting procedures are also reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known to be located in the

17

~~(TS//SI//OC/NF)~~~~TOP SECRET//COMINT//ORCON//NOFORN~~

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

United States at the time of acquisition. *See id.* at 3-12, 28-30. Just as the Government's acquisition of an entire book based on the fact that a single page falls within the scope of the warrant does not call into question the warrant's specificity, the incidental acquisition of additional communications that are not to, from, or about the tasked selector does not negate the validity of the targeting procedures that are relied on to acquire a particular transaction.

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

Moreover, the AG and DNI have confirmed that the additional information regarding incidentally acquired communications does not alter the validity of their prior Certifications. *See id.* at 35. As discussed in detail previously, the minimization and targeting procedures fully comport with all of the statutory requirements, including the requirement that the targeting procedures are reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located within the United States, *see id.* at 3-12, 20-24; and the procedures and guidelines are consistent with the requirements of the Fourth Amendment, *see id.* at 13-24. ~~(TS//SI//OC/NF)~~

---

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



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

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

2011 JUL 14 PM 12:40

LEAHY HALL

MOTION FOR ORDERS EXTENDING TIME LIMITS PURSUANT  
TO 50 U.S.C. § 1881a(j)(2) ~~(S)~~

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully moves the Court to issue orders pursuant to 50 U.S.C. § 1881a(j)(2) of the Foreign Intelligence Surveillance Act of 1978, as amended (the Act), extending to September 20, 2011, the time limits for the Court to complete its review of and issue orders concerning DNI/AG 702(g) Certifications [REDACTED] and the amendments to their respective predecessor certifications. As discussed below, the government respectfully submits that there is good cause for the extensions of the time limits, and that such extensions would be consistent with national security. ~~(S//OC/NF)~~

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

Classified by: ~~Lisa O. Monaco, Assistant Attorney General, NSD, DOJ~~  
Reason: ~~1.4(c)~~  
Declassify on: ~~14 July 2036~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

## I. Procedural Background ~~(S)~~

### A. The 2011 Reauthorization Certifications and Related Amendments ~~(S)~~

On April 20, 2011, the government submitted to the Court DNI/AG 702(g)

Certification [REDACTED]

[REDACTED]

[REDACTED]. Included with DNI/AG 702(g)

Certification [REDACTED] were the targeting and minimization procedures to be used by the

National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Central

Intelligence Agency (CIA) under that certification. DNI/AG 702(g) Certification [REDACTED]

reauthorizes DNI/AG 702(g) Certification [REDACTED]

[REDACTED]

[REDACTED], which was set to expire on [REDACTED] 2011. In accordance with 50 U.S.C.

§ 1881a(g)(2)(D)(i), DNI/AG 702(g) Certification [REDACTED] also included an effective date

for the authorization that is at least thirty days after its submission to the Court -- i.e.,

[REDACTED] 2011. ~~(S//OC/NF)~~

DNI/AG 702(g) Certification [REDACTED] also included amendments to its predecessor

certifications, DNI/AG 702(g) Certifications [REDACTED]. Specifically, these

amendments authorize the use of the minimization procedures attached as Exhibits B

and E to DNI/AG 702(g) Certification [REDACTED] in connection with foreign intelligence

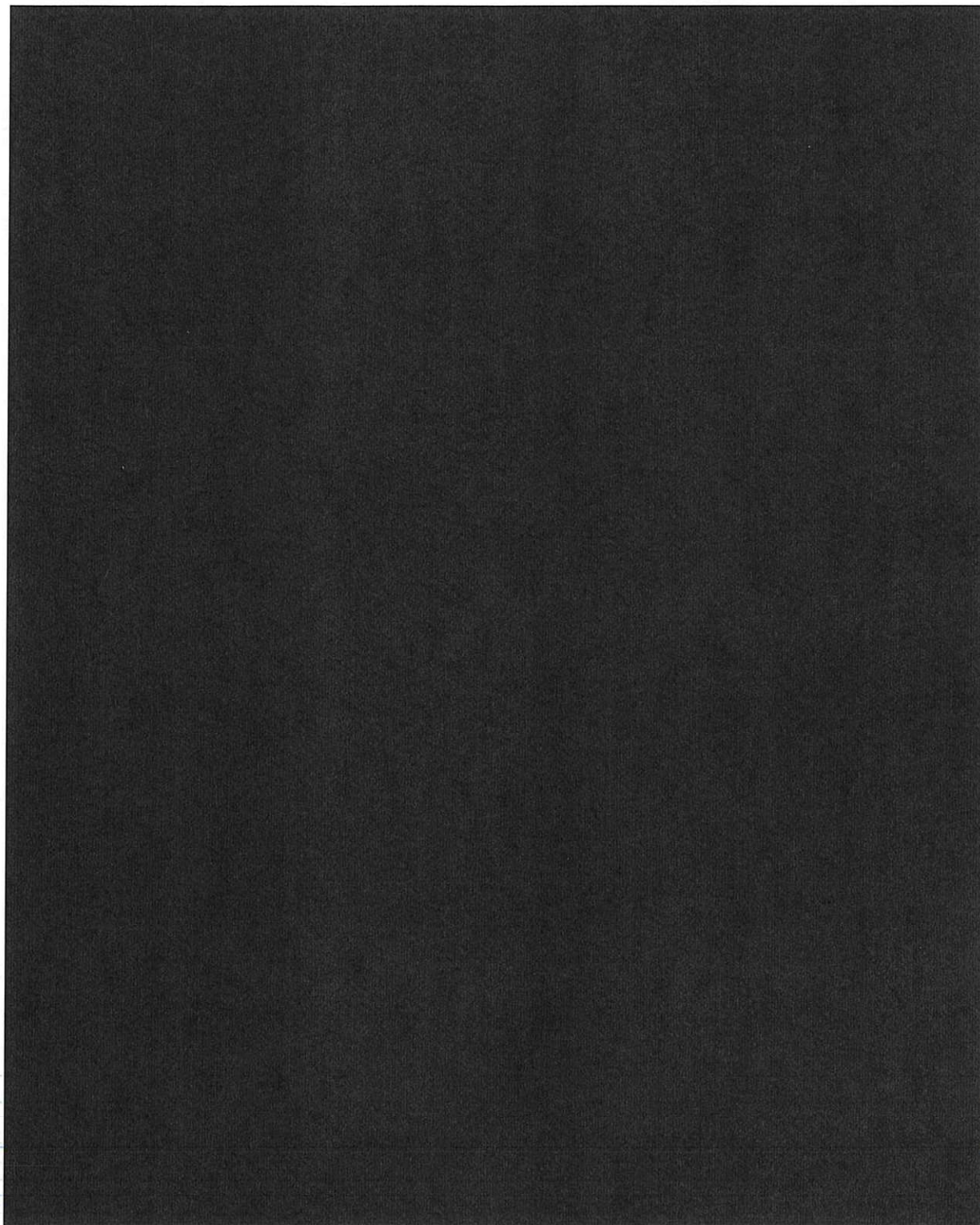
~~TOP SECRET//COMINT//ORCON,NOFORN~~



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

information acquired in accordance with DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] These amendments also have an effective date of [REDACTED] 2011. ~~(S//OC/NF)~~



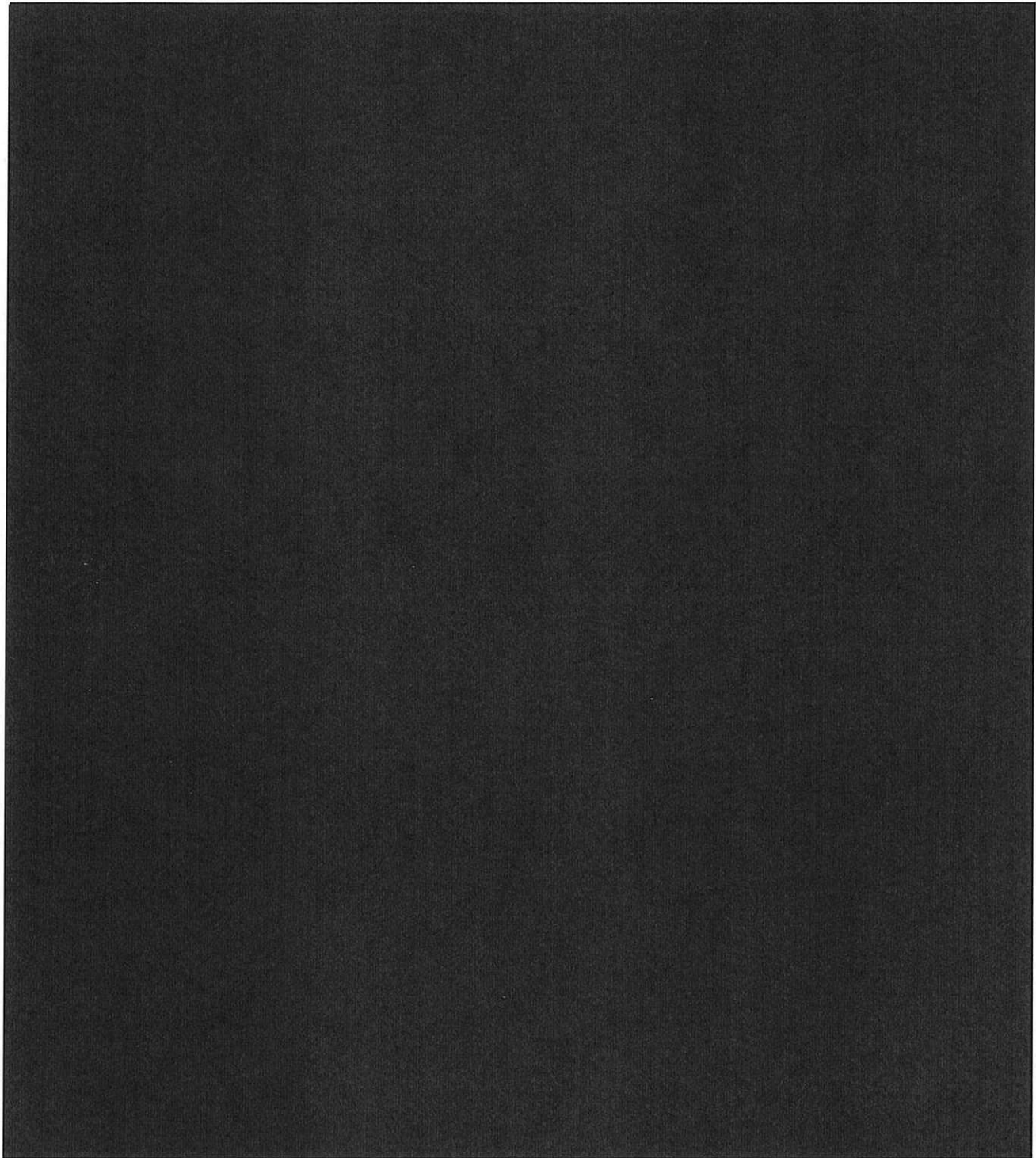
~~TOP SECRET//COMINT//ORCON/NOFORN~~



Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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



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

~~TOP SECRET//COMINT//ORCON,NOFORN~~**B. Two Matters Reported to the Court ~~(S)~~****1. Overcollection of [REDACTED] ~~(TS//SI//NF)~~**

On April 19, 2011, the government filed with the Court pursuant to Rule 13(b) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, a preliminary notice of two compliance incidents, both of which concern NSA's collection of [REDACTED] [REDACTED] that, in addition to targeted communications, contain communications that are not to, from, or about selectors tasked for acquisition in accordance with section 702 of the Act. One of these incidents concerns NSA's overcollection of [REDACTED] [REDACTED] because of [REDACTED] [REDACTED].<sup>1</sup> The government respectfully incorporates herein by reference this notice dated April 19, 2011. ~~(TS//SI//OC/NF)~~

**2. Clarification Concerning Upstream Collection ~~(TS//SI//NF)~~**

On May 2, 2011, the government filed, pursuant to Rule 13(a) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, a preliminary notice clarifying certain facts concerning NSA's upstream collection of electronic communications. Specifically, this notice provided the Court with additional details concerning one specified category of Internet communications NSA acquires through its upstream collection -- [REDACTED]

<sup>1</sup> The other incident reported in this notice concerned NSA's overcollection of [REDACTED] [REDACTED]. On March 15, 2011, NSA terminated collection [REDACTED] [REDACTED]. ~~(TS//SI//OC/NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~





~~TOP SECRET//COMINT//ORCON,NOFORN~~

regarding aspects of NSA's upstream collection. The government filed responses to these additional questions on June 28, 2011. The government respectfully incorporates herein by reference these four documents. ~~(TS//SI//OC/NF)~~

## II. The Issuance of Orders Under 50 U.S.C. § 1881a(j)(2) is Appropriate in These Cases ~~(S)~~

Upon the government's submission of DNI/AG 702(g) Certification [REDACTED] on April 20, 2011, [REDACTED] [REDACTED] the thirty-day time periods in which the Court is required to review the certifications began to run. See 50 U.S.C. § 1881a(i)(1)(B). The thirty-day time periods for the Court to review the amendments to the predecessor certifications also began to run on those same dates. See id. § 1881a(i)(C). Accordingly, the time limit for the Court to complete its review of DNI/AG 702(g) Certification [REDACTED] and the amendments to its predecessor certifications was May 20, 2011. [REDACTED]

[REDACTED]

[REDACTED]

~~(S//OC/NF)~~

The Court may, however, "extend[] that time as necessary for good cause in a manner consistent with national security." 50 U.S.C. § 1881a(j)(2). As discussed above, by orders dated May 9, 2011, the Court extended the time limits until July 22, 2011, to review DNI/AG 702(g) Certifications [REDACTED] and the amendments to their respective prior certifications. For the following reasons, the government

~~TOP SECRET//COMINT//ORCON,NOFORN~~



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

respectfully submits that there is good cause for further extensions of the time limits, and that such extensions would be consistent with national security. ~~(S//OC/NF)~~

**A. There Is Good Cause for the Court to Further Extend the Time Limits for Its Review ~~(S)~~**

The government believes that there is good cause for the Court to further extend the deadlines for the Court to complete its review of DNI/AG 702(g) Certifications [REDACTED], and the amendments to their respective predecessor certifications. Specifically, as explained below, the government intends to supplement the record concerning the matters discussed above in a manner that will aid the Court in its review and in making the determinations necessary to issue orders under 50 U.S.C. § 1881a(i)(3). However, the government will not be in a position to supplement the record until after July 22, 2011. ~~(S//OC/NF)~~

On July 8, 2011, the Court orally invited the Government to supplement the record in this matter by providing additional information further responding to the Court's June 17 questions about the nature and scope of the types of communications NSA acquires through its upstream collection systems. The Government is currently in the process of compiling this additional information. In addition, the Government is examining whether enhancements to NSA's systems or processes could be made to further ensure that information acquired through NSA's upstream collection is handled in accordance with the requirements of the Act. However, neither of these efforts will be completed until after July 22, 2011. ~~(S//OC/NF)~~

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

~~TOP SECRET//COMINT//ORCON,NOFORN~~

**B. Extending the Time Limit for the Court's Review Is Consistent with National Security. ~~(S)~~**

As this Court has recognized, "[t]he government's national security interest in conducting these acquisitions [under section 702] 'is of the highest order of magnitude.'" In re DNI/AG Certification [REDACTED], No. 702(i)-08-01, Mem. Op. at 37 (USFISC Sept. 4, 2008) (quoting In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008)). For example, the foreign intelligence information the government acquires under DNI/AG 702(g) Certification

[REDACTED] DNI/AG 702(g) Certification [REDACTED]

[REDACTED] Affidavit of Lt. General Keith B. Alexander, Director, NSA, ¶ 6. ~~(S//OC/NF)~~

Were the Court to issue orders under 50 U.S.C. § 1881a(j)(2) extending the time limits for its review of the certifications and related amendments so that the Court could consider these additional materials, the authorizations in the certifications being reauthorized, DNI/AG 702(g) Certification [REDACTED], would, by operation of 50 U.S.C. § 1881a(i)(5)(B), continue despite their expiration dates.<sup>2</sup> The

<sup>2</sup> The government's filing of DNI/AG 702(g) Certification [REDACTED] on April 20, 2011, [REDACTED], comported with 50 U.S.C. § 1881a(i)(5)(A), which requires that if the government seeks to reauthorize an authorization issued under 50 U.S.C. § 1881a(a), the government must, to the extent practicable, submit to the Court a new certification executed under 50 U.S.C. § 1881a(g), with supporting documents, at least thirty days before the expiration of the certification being reauthorized. If a new certification is filed in accordance with 50 U.S.C. § 1881a(i)(5)(A), 50 U.S.C. § 1881a(i)(5)(B) provides that the existing certification being reauthorized shall

~~TOP SECRET//COMINT//ORCON,NOFORN~~



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

government respectfully submits that this result would be consistent with national security, because it would allow the government's acquisition of vitally important foreign intelligence information under DNI/AG 702(g) Certification [REDACTED] to continue pending the completion of the Court's review of the reauthorization certifications, DNI/AG 702(g) Certification [REDACTED] respectively. ~~(S//OC/NF)~~

The government further submits that it would be consistent with national security for the Court to extend its consideration of the above-discussed amendments, which authorize the use of the NSA and CIA minimization procedures submitted with DNI/AG 702(g) Certifications [REDACTED] in connection with foreign intelligence information acquired in accordance with the predecessors of those certifications. The NSA and CIA minimization procedures currently approved for use under those predecessor certifications, however, differ in some respects from the NSA and CIA minimization procedures submitted with DNI/AG 702(g) Certification [REDACTED]. The government believes that authorizing NSA and CIA to use a single set of minimization procedures (i.e., each agency's respective minimization procedures submitted with DNI/AG 702(g) Certifications [REDACTED] for the entirety of each agency's holdings of foreign intelligence information acquired under section 702 will result in a more uniform application of minimization standards

remain in effect, notwithstanding its expiration date, until the Court issues an order under 50 U.S.C. § 1881a(i)(3) with respect to the new certification. ~~(S)~~

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

~~TOP SECRET//COMINT//ORCON,NOFORN~~

to that information. Authorizing each agency to use a single set of minimization procedures for that information also will significantly simplify oversight of each agency's adherence to those standards. ~~(S//OC/NF)~~

### III. Conclusion ~~(S)~~

For the foregoing reasons, the government respectfully submits that there is good cause for the Court to issue orders under 50 U.S.C. § 1881a(j)(2) extending to September 20, 2011, the time limit for the Court to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certification [REDACTED] and the amendments to their respective predecessor certifications, and that such an extension would be consistent with national security. The government also requests that the Court issue the proposed Notice of Extension, attached herewith. ~~(S//OC/NF)~~

Respectfully submitted,

[REDACTED]

[REDACTED]  
National Security Division  
United States Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

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

## APPROVAL

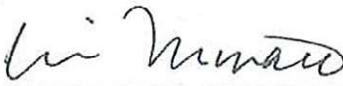
I find that this motion regarding DNI/AG 702(g) Certification [REDACTED]  
[REDACTED] and the amendments to their respective predecessor certifications satisfies the  
criteria and requirements set forth in the Foreign Intelligence Surveillance Act of 1978,  
as amended, and hereby approve its filing with the United States Foreign Intelligence  
Surveillance Court. ~~(S)~~

---

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

---

James M. Cole  
Deputy Attorney General of the United States

 JUL 14 2011

---

Lisa O. Monaco  
Assistant Attorney General for National Security

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



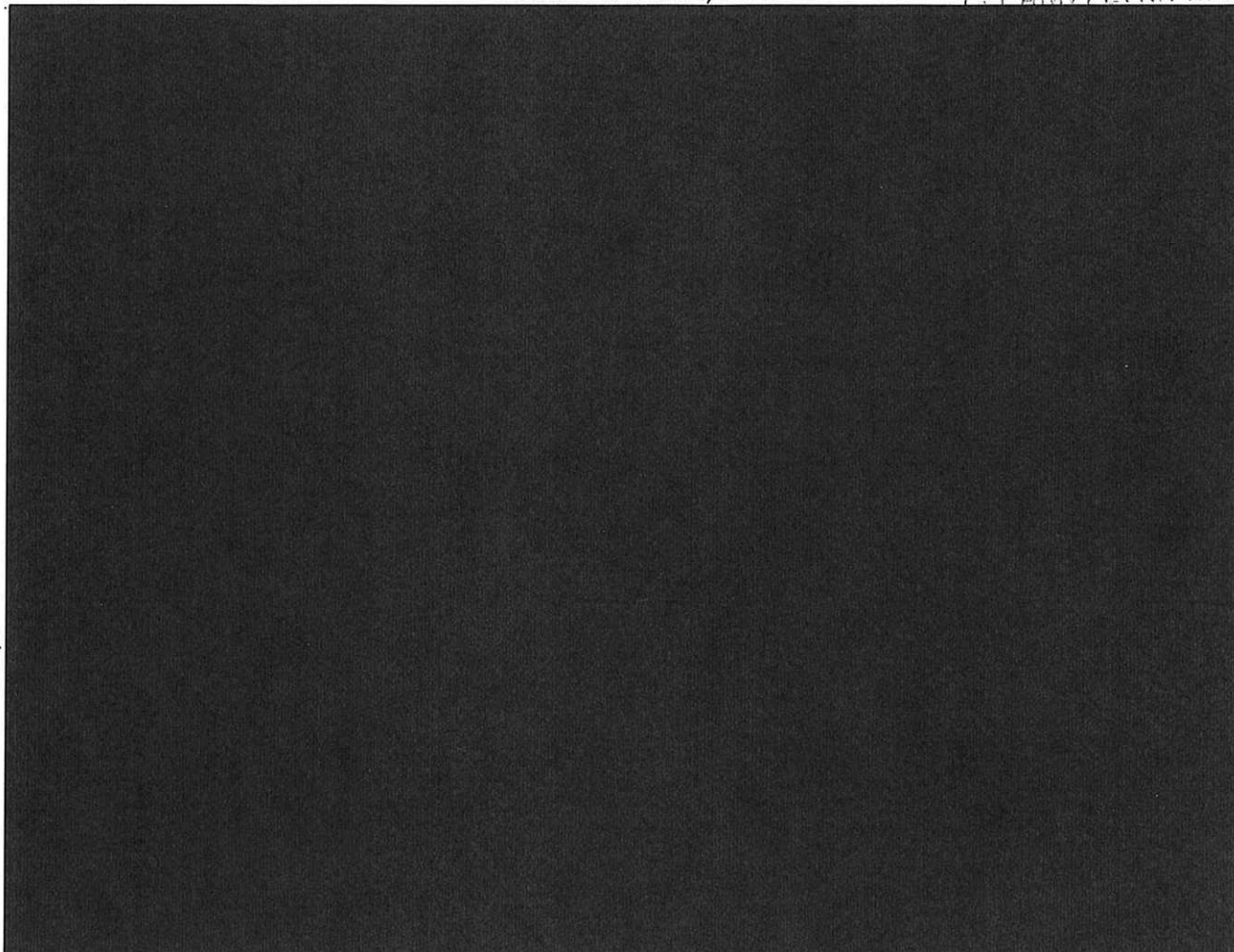
~~SECRET//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT 2011 AUG 16 PM 2:16

WASHINGTON, D.C.

LEAHN FLYNN HALL



NOTICE OF FILING OF GOVERNMENT'S SUPPLEMENT TO ITS SUBMISSIONS  
OF JUNE 1<sup>ST</sup> AND JUNE 28<sup>TH</sup>, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of  
Justice attorney, respectfully submits the attached supplement in further support of the

~~SECRET//ORCON,NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: 16 August 2036

~~SECRET//ORCON,NOFORN~~

arguments set forth in submissions of June 1<sup>st</sup> and June 28<sup>th</sup>, 2011, concerning the above-referenced matters. This supplement explains the methodology behind and sets forth the results of a manual review by the National Security Agency (NSA) of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's FISA Amendments Act Section 702 upstream collection during a six-month period. The Government respectfully submits that the data provided herein supplements and supports the Government's Responses to the Court's Briefing Order of May 9<sup>th</sup>, 2011, and supplemental questions of June 17, 2011, and will further assist the Court in concluding that the certifications and procedures submitted in the above-referenced matters satisfy the requirements of the Act and are consistent with the Fourth Amendment to the Constitution of the United States. ~~(S//OC,NF)~~

Given the complex nature of the information provided in this supplement, the United States is prepared to provide any additional information the Court believes would aid it in reviewing these matters. The Government may also seek to supplement and/or clarify the information provided herein as appropriate during any hearing that the Court may hold in the above-captioned matters. ~~(S//OC,NF)~~

Respectfully submitted,



National Security Division  
United States Department of Justice

~~SECRET//ORCON,NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~**(U//FOUO) NSA Characterization of Upstream Data: Process and Results****I. (U) Introduction**

~~(TS//SI//NF)~~ This report explains the methodology behind and provides the results of a manual review of a statistically representative sample of Internet communications acquired through NSA's FISA Amendments Act (hereinafter "FAA") section 702 upstream collection during a six-month period.<sup>1</sup> The purpose of this review was to assemble data to assist the Court in understanding the nature and scope of the communications acquired through NSA's upstream collection. The data assembled consisted of:

- The volume of transactions containing single, discrete communications to, from, or about a selector used by a person targeted in accordance with NSA's section 702 targeting procedures (hereinafter "tasked selector") versus transactions containing multiple communications (hereinafter "Multi-communication Transactions" or "MCT") not all of which may be to, from, or about a tasked selector;<sup>2</sup>
- The types of discrete communications contained within MCTs [REDACTED]; and

<sup>1</sup> ~~(TS//SI//NF)~~ Additionally, as described on pages 8-9 of the Government's June 1, 2011 Response to the Court's Briefing Order of May 9, 2011, NSA conducted two tests of FAA 702 upstream collection in May 2011 using information from NSA's technical databases in an attempt to determine the likelihood of collecting an Internet transaction between a user in the United States and [REDACTED]. NSA also attempted to further determine the extent to which those tests might be statistically representative of NSA's 702 upstream collection and repeated these tests in July 2011 using alternative data sets. Because of the technical limitations for automatically identifying transactions containing multiple communications, NSA assesses that the results of these tests are not comparable to each other or with the results of the separate manual analysis discussed herein. Furthermore, for the same reason of technical limitation, the results do not express as high a degree of granularity and accuracy as the manual analysis discussed herein, which took more than one month of careful review by experienced analysts to complete. None of the results discussed herein and in the Government's June 1 Response, however, are inconsistent.

<sup>2</sup> ~~(TS//SI//NF)~~ As described on pages 27-28 of the Government's June 1, 2011 Response to the Court's Briefing Order of May 9, 2011, NSA's inability to separate out individual pieces of information from Internet communications acquired by NSA's upstream collection systems does not extend to all forms of transactions. NSA has developed the capability to [REDACTED] identify transactions which [REDACTED] and, in certain other limited instances, transactions where an "active user" (as described more fully below) is a tasked selector. Based on a test of this capability from July 16th-29th 2011, NSA estimates that approximately only [REDACTED] of NSA's current upstream collection under FAA section 702 could be identified through [REDACTED] processes as communications to, from or about NSA's tasked selector. As reflected by the results of this manual review, this figure is significantly under-representative of the total proportion of NSA's upstream collection assessed to be communications to, from or about a tasked selector.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20360701

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



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

- The volume of MCTs that NSA assesses contain a wholly domestic communication not to, from, or about a tasked selector.<sup>3</sup>

## II. (U) How the Statistically Representative Sample Was Assembled

~~(TS//SI//NF)~~ NSA assembled the sample of communications acquired through its upstream collection by first identifying all Internet communications acquired under section 702 – i.e., both from NSA upstream collection and collection from Internet service providers either by or with the assistance of the Federal Bureau of Investigation (hereinafter "PRISM collection") -- during a six-month period from January 1st through June 30th, 2011, and present within [REDACTED] as of July 14, 2011. As of that date, 140,974,921 Internet communications were present within [REDACTED]. Of these, 127,718,854 (or approximately 91%) were acquired from PRISM collection, and 13,256,067 (or approximately 9%) were acquired through NSA's upstream collection.<sup>6</sup>

~~(TS//SI//NF)~~ The approximately 13.25 million Internet communications acquired through NSA's upstream collection (hereinafter "transactions") were then "shuffled" by NSA statisticians to ensure a random sample (i.e., any sample drawn would be statistically representative of the total 13.25 million transactions). NSA statisticians estimated that a manual review of a sample of approximately 50,000 of these randomized transactions would enable characterization of all 13.25 million transactions with a statistically high level of confidence and precision.<sup>7</sup>

## III. (U) How the Manual Review Was Conducted and the Results of the Review

~~(TS//SI//NF)~~ Under the leadership of NSA's Deputy Director, an experienced interdisciplinary team consisting of experienced intelligence analysts, attorneys from NSA's Office of General Counsel, representatives from NSA's Office of the Director of Compliance, NSA statisticians, representatives from NSA's Network Analysis Center, and representatives from NSA's Office of Oversight and Compliance was assembled to conduct the review described herein and compile this report. A team of experienced NSA

<sup>3</sup> ~~(TS//SI//NF)~~ This aspect of the review required analysts to perform intensive analysis on discrete communications which did not contain the target's selector within MCTs, to determine if the sender and all intended recipients of those discrete communications were located in the United States. Such in-depth analysis is not typically conducted by analysts in their daily foreign intelligence analysis. Instead, an analyst would tend to focus his or her attention on those discrete communications within the MCT that are to, from, or about their assigned target, and would only perform a deeper inspection of those communications to confirm they were not wholly domestic if they were in-fact pertinent to the analyst's evaluation of foreign intelligence information and therefore worth further analysis for potential use.

<sup>4</sup> ~~(TS//SI//NF)~~ [REDACTED]

<sup>5</sup> ~~(TS//SI//NF)~~ This figure does not include Internet communications that were acquired during this six-month period but were purged prior to July 14, 2011.

<sup>6</sup> ~~(TS//SI//NF)~~ See Figure A of Appendix A, attached hereto.

<sup>7</sup> ~~(TS//SI//NF)~~ Details for the basis for NSA's statistical assertions are set forth in Appendix B, attached hereto.

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

intelligence analysts was assigned to conduct a manual review of the transactions. Ultimately, that team of NSA intelligence analysts collectively reviewed a total of 50,440 individual transactions.

~~(TS//SI//NF)~~ In order to ensure consistency among the analysts in their review, before beginning the manual review, the team members were trained to recognize MCTs and how to characterize the discrete communications contained within them. The team members were given training materials created specifically for this effort, which included screenshots depicting typical examples of the types of transactions acquired through NSA's upstream collection. NSA's Office of General Counsel, Office of Oversight and Compliance, and Office of the Director for Compliance reviewed all training materials and provided guidance throughout the manual review.

~~(TS//SI//NF)~~ For quality assurance, some transactions (approximately 10 out of every 5,000) underwent independent reviews by more than one analyst. In addition, the team lead performed spot reviews of transactions that had already undergone review (approximately 1 out of every 100). The team lead also personally reviewed any transaction that team members were unable to immediately characterize as clearly being a discrete communication or an MCT; as well as any MCT identified as potentially concerning a person located in the United States. Both the quality assurance overlap and the reviews performed by the team lead revealed no discrepancies among how analysts characterized any of the transactions subjected to these overlapping reviews.

~~(TS//SI//NF)~~ In conducting the manual review, NSA analysts took the following steps and made the following findings:

1. **Determined if the transaction was a single, discrete communication or an MCT.**<sup>8</sup> If the transaction was determined to be a single, discrete communication, no further analysis was done. Transactions determined to be MCTs were further analyzed, as described below.
  - Of the 50,440 transactions reviewed, 45,359 (approximately 90%) were determined to be single, discrete communications. The remaining 5,081 transactions (approximately 10%) were determined to be MCTs.<sup>9</sup>
2. **Characterized the discrete communications within the 5,081 MCTs as being** [REDACTED]
  - Of the 5,081 MCTs reviewed, [REDACTED]

<sup>8</sup> ~~(TS//SI//NF)~~ For any objects that the initial reviewer was uncertain about how to characterize (e.g., if the transaction contained data requiring further processing to render it intelligible to the analyst), the team lead performed a second review. As a result, each of 50,440 transactions reviewed were able to be characterized as being either a single, discrete communication or an MCT.

<sup>9</sup> ~~(TS//SI//NF)~~ See Figure B of Appendix A.

<sup>10</sup> ~~(TS//SI//NF)~~ [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]



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

[REDACTED]

[REDACTED]<sup>12</sup>

3. **Determined whether the 5,081 MCTs contained any discrete communications as to which the sender and all intended recipients were located in the United States.** As discussed in more detail below, in many cases NSA analysts were able to make these determinations based on the location of the "active user" of the MCT.<sup>13</sup> In other cases, NSA had to rely on content analysis because the MCT did not contain technical information sufficient to identify the active user or to determine the active user's location. There were, however, instances where the MCT did not contain sufficient technical information or content for NSA to assess whether the MCT contained any wholly domestic communications.
- Of the 5,081 MCTs, 713 (approximately 14%) had a tasked selector as the active user [REDACTED]. No further analysis of these MCTs was done to determine whether they contained wholly domestic communications. That is because the user of the tasked selector, who by operation of the NSA targeting procedures is a person reasonably believed to be located outside the United States, would be either the sender or an intended recipient of each of the discrete communications contained within the MCT.<sup>14</sup> Accordingly, all of the discrete communications within those MCTs would have at least one communicant reasonably believed to be located outside the United States (i.e., the target) and thus would not be wholly domestic.
  - Of the 5,081 MCTs, 2,668 (approximately 52%) had an active user that was not a tasked selector but was nonetheless an electronic communications account/address/identifier

<sup>11</sup> ~~(TS//SI//NF)~~ See Figure C of Appendix A.

<sup>12</sup> ~~(TS//SI//NF)~~ [REDACTED]

<sup>13</sup> ~~(TS//SI//NF)~~ When NSA acquires an Internet transaction between an individual using an electronic communications account/address/identifier and his/her service provider, that individual is the "active user" for that transaction. Such transactions can have, at most, one "active user."

<sup>14</sup> ~~(TS//SI//NF)~~ In this context, a communication to or from the target includes communications to or from the tasked selector itself (e.g., an e-mail sent to a tasked e-mail account), as well as communications where the tasked selector appears in other communications attributable to the target [REDACTED]

See *In re DNI/AG Certification* [REDACTED]

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

reasonably believed to be used by a person located outside the United States.<sup>15</sup> No further analysis of these MCTs was done to determine whether they contained wholly domestic communications. That is because the foreign-based active user would be either a sender or intended recipient of each of the discrete communications within the transaction. Accordingly, all of the discrete communications within those MCTs would have at least one communicant reasonably believed to be located outside the United States (i.e., the foreign-based active user) and thus would not be wholly domestic.

- Of the 5,081 MCTs, 8 (approximately 0.16%) contained an electronic communication account/address/identifier of a non-targeted active user who appeared to be located in the United States, but none of the discrete communications within the MCT were determined to be wholly domestic because at least one of the communicants to each discrete communication was reasonably believed to be located outside the United States. Specifically, the 8 MCTs were determined to concern six non-targeted active users (i.e., two of the MCTs were duplicates):
  - Four MCTs (including both duplicates) [REDACTED] contained at least one e-mail message from a tasked selector as well as other e-mail messages from accounts/addresses/identifiers reasonably believed to be used by a person located outside the United States.<sup>16</sup> [REDACTED]
  - Three MCTs [REDACTED] with the users of accounts/addresses/identifiers who were reasonably believed to be located outside the United States.<sup>17</sup>
  - One MCT [REDACTED] where further technical analysis revealed that the active user was reasonably believed to be located outside the United States.
- Of the 5,081 MCTs, 10 (approximately 0.2%) contained an electronic communication account/address/identifier of a non-targeted active user who was located in the United States, and the MCTs contained at least one discrete communication that was wholly

<sup>15</sup> ~~(TS//SI//NF)~~ To determine the location of the non-targeted active user, NSA performed the same sort of [REDACTED] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

<sup>16</sup> ~~(TS//SI//NF)~~ To determine the location of the senders of each of these discrete e-mail messages, NSA performed the same sort of [REDACTED] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

<sup>17</sup> ~~(TS//SI//NF)~~ To determine the location of [REDACTED] NSA performed the same sort of [REDACTED] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.



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

domestic. Specifically, all 10 of these MCTs were [REDACTED] and all 10 involved U.S.-based persons using [REDACTED].<sup>18</sup> For all 10 of these MCTs, only [REDACTED] was present. The [REDACTED] did not include [REDACTED].

- 9 of the 10 [REDACTED] were attributed to a single U.S.-based user. Each of these 9 [REDACTED] 10 total e-mail messages. The 9 [REDACTED] were not completely duplicative, but many of the 10 e-mail messages [REDACTED] were duplicative:
  - ◆ Two of the messages [REDACTED] in each of the 9 [REDACTED] contained a tasked selector and thus were not assessed to be wholly domestic.
  - ◆ Three of the messages [REDACTED] in each of the 9 [REDACTED] were [REDACTED] which is located in the United States) and thus were assessed to be wholly domestic.
  - ◆ The remaining e-mail messages [REDACTED] were between the U.S.-based user and persons reasonably believed to be located outside the United States (and thus not assessed to be wholly domestic) or whose location was unknown.<sup>19</sup>
- The other [REDACTED] was attributed to a different U.S.-based user. This [REDACTED] 15 total e-mail messages:
  - ◆ One of the [REDACTED] e-mail messages was from a tasked selector and thus was not assessed to be wholly domestic.
  - ◆ One of the [REDACTED] e-mail messages appeared to be a message that the U.S.-based user sent to himself [REDACTED] and thus was assessed to be wholly domestic.
  - ◆ One of the [REDACTED] e-mail messages appeared to be a message sent by an associate [REDACTED] account and thus was assessed to be wholly domestic.
  - ◆ The remaining e-mail messages [REDACTED] were between the U.S.-based user and persons reasonably believed to be

<sup>18</sup> ~~(TS//SI//NF)~~ [REDACTED]

<sup>19</sup> ~~(TS//SI//NF)~~ To determine the location of the other communicants, NSA performed the same sort of [REDACTED] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

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

located outside the United States and thus were not assessed to be wholly domestic.<sup>20</sup>

- Of the 5,081 MCTs, 1,682 (approximately 33%) required further, in-depth [REDACTED] analysis because they lacked information sufficient for NSA to readily identify the active user or determine the active user's location. In most of these cases, the transactions did not contain enough information for NSA to readily determine which electronic communication account/address/identifier appearing in the transaction was that of the active user. In other cases, NSA was able to determine which electronic communication account/address/identifier appearing in the transaction was that of the "active user," but NSA was unable to determine the active user's location. NSA's further [REDACTED] analysis of these 1,682 MCTs revealed:
  - For 1,220 of these 1,682 MCTs, NSA analysis of [REDACTED] data indicated that they were characteristic of a foreign use [REDACTED]
  - For 152 of these 1,682 MCTs, NSA analysis of [REDACTED] data indicated that they were [REDACTED]
  - For 86 of these 1,682 MCTs, NSA analysis of a combination of technical data and content revealed that they appeared to contain communications of persons located outside the United States (e.g., through further content analysis, NSA analysts were able to identify the active users of some MCTs and information indicative of those users' locations).
- Of the 5,081 MCTs, NSA cannot determine whether 224 MCTs contained wholly domestic communications, because these MCTs lack information sufficient for NSA to identify the active user or determine the active user's location. Nevertheless, NSA has no basis to believe any of these MCTs contain wholly domestic communications.
  - For 182 of these 224 MCTs, NSA technical analysis indicates that they were characteristic of [REDACTED]
  - For 1 of these 224 MCTs, NSA initially determined that it contained an electronic communication account/address/identifier of a non-targeted active user who appeared to be located in the United States, but whose location could not be determined upon further technical analysis. Specifically, [REDACTED]

<sup>20</sup> ~~(TS//SI//NF)~~ To determine the location of the other communicants, NSA performed the same sort of [REDACTED] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.



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

- [REDACTED]
- 23 of these 224 MCTs were not further analyzed because, although they were present in [REDACTED] as of the date the sample was assembled, they were subsequently purged and/or placed on NSA's Master Purge List.
  - 18 of these 224 MCTs could not be further characterized by NSA analysts.

IV. (U) Conclusions Drawn from the Random Sample

~~(TS//SI//NF)~~ Based on a random sample of the approximately 13.25 million total Internet communications acquired by NSA through "upstream" techniques pursuant to FAA section 702 for the six-month period discussed, NSA assesses that the volume of transactions containing multiple communications not all of which may be to, from, or about a tasked selector is approximately between 1.29 and 1.39 million (9.70%-10.45%).<sup>21</sup> With respect to the types of discrete communications contained within multi-communication transactions manually reviewed by NSA analysts, [REDACTED]

~~(TS//SI//NF)~~ As described in Appendix B, which details NSA's Statistical Methodology for this review, the data compiled during the above-discussed manual review of a random sample of Internet communications acquired during a six-month period can be used to characterize with a statistically high degree of confidence (i.e., a simultaneous confidence level of 95% for these intervals collectively) the nature and scope of the entirety of the approximately 13.25 million Internet communications from

<sup>21</sup> ~~(TS//SI//NF)~~ As calculated in the attached Appendix detailing NSA's Statistical Methodology for this review, these figures are based on the 45,359 of the 50,440 transactions (89.93%) manually reviewed by NSA analysts as containing single, discrete communications and the 5,081 transactions (10.07%) manually reviewed by NSA analysts as containing multiple communications. See also Step 1, *supra* page 3.

<sup>22</sup> ~~(TS//SI//NF)~~ [REDACTED]

<sup>23</sup> ~~(TS//SI//NF)~~ [REDACTED]

<sup>24</sup> ~~(TS//SI//NF)~~ [REDACTED]

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

which the random sample was drawn. Specifically, NSA assesses that of these approximately 13.25 million Internet communications acquired through NSA upstream collection:

- between approximately 11.87 and 11.97 million (89.55%-90.30%) are transactions that contain only single, discrete communications to, from, or about a tasked selector;
- between 168,853 and 206,922 (1.27%-1.56%)<sup>25</sup> are transactions that contain multiple communications, all of which are either to or from a tasked selector;
- between 1,042,838 and 1,113,947 (7.87%-8.53%)<sup>26</sup> are transactions that contain multiple communications, at least one of which is to, from, or about NSA's tasked selector, but all of which are believed to either be to or from non-targeted persons reasonably believed to be located outside the United States;
- between 48,609 and 70,168 (0.37%-0.53%)<sup>27</sup> are transactions that contain multiple communications, at least one of which is to, from, or about NSA's tasked selector, and at least one of which is a communication between non-targeted persons (i.e., not to, from or about a tasked selector) that lacks sufficient information for NSA to identify the location of the sender and all intended recipients of that communication; and
- between 996 and 4,965 (0.0075%-0.0375%) contain a wholly domestic communication not to, from, or about a tasked selector.

~~(TS//SI//NF)~~ In sum, while there was insufficient information present for 224 multi-communication transactions for NSA analysts to characterize the likelihood that they may contain wholly domestic communications (the majority of which were attributable to [REDACTED] [REDACTED], for the reasons explained in detail

<sup>25</sup> ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 713 of the 5,081 MCTs (14.03%) and 50,440 total transactions (1.41%) reviewed by NSA analysts as containing a tasked selector as the active user [REDACTED]. See also Step 3, *supra* page 4.

<sup>26</sup> ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 4,134 of the 5,081 MCTs (81.36%) and 50,440 total transactions (8.19%) reviewed by NSA analysts as containing discrete communications believed to be to or from non-targeted persons located outside the United States. More specifically, this total includes the following MCTs manually reviewed by NSA analysts: 2,668 that had an active user reasonably believed to be a person located outside the United States; 8 that included at least one communicant reasonably believed to be located outside the United States for each communication therein; 1,220 that are characteristic of [REDACTED] 152 that are indicative of [REDACTED] and 86 that all communications contained therein were to or from persons located outside the United States. See Step 3, *supra* pages 4-6.

<sup>27</sup> ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 224 of the 5,081 MCTs (4.41%) and 50,440 total transactions (0.44%) reviewed by NSA analysts that lacked sufficient information to identify the active user or the active user's location. See Step 3, *supra* page 6.



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

above, NSA has no basis to believe any of the remaining Internet communications reviewed in the 50,440 sample are wholly domestic beyond those 10 discussed above.<sup>28</sup> Moreover, each of those 10 Internet communications has been placed on NSA's Master Purge List.

----- The remainder of this page intentionally left blank. -----

---

<sup>28</sup> ~~(TS//SI//NF)~~ See Figure D of Appendix A.

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

**(U) VERIFICATION**

(U) I declare under penalty of perjury that the facts set forth in the foregoing "NSA Characterization of Upstream Data: Process and Results" are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 16th day of August, 2011.



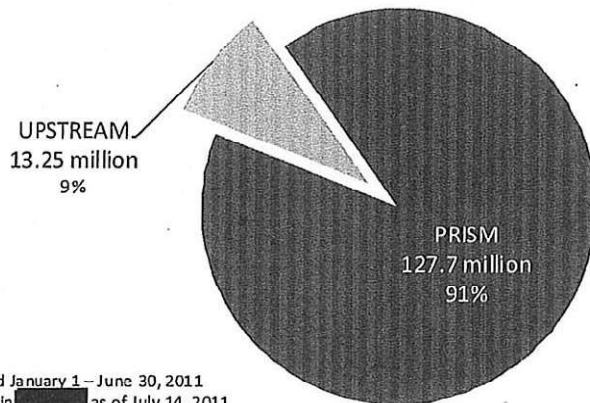
Signals Intelligence Directorate Compliance Architect  
National Security Agency

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

## Appendix A

Fig. A Total FAA 702

140,974,921 Internet Communications



Acquired January 1 – June 30, 2011  
Present in [redacted] as of July 14, 2011

Fig. B Total Upstream Sample

50,440 objects manually reviewed

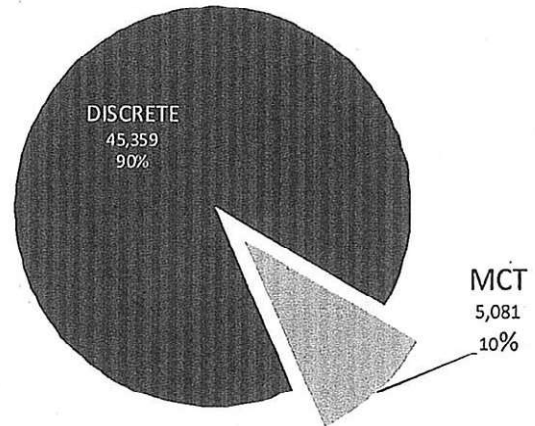


Fig. C MCT Type

5,081 objects

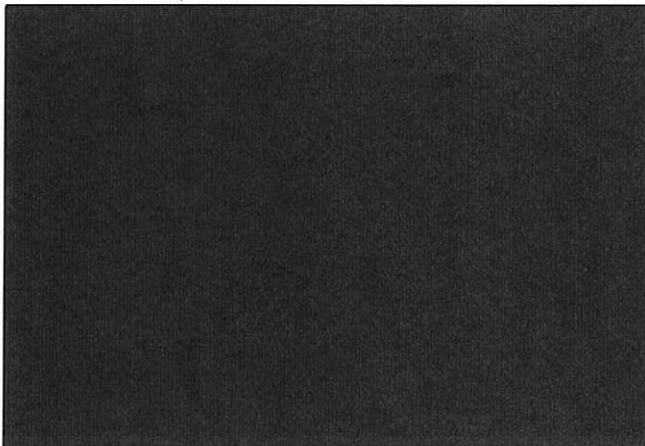
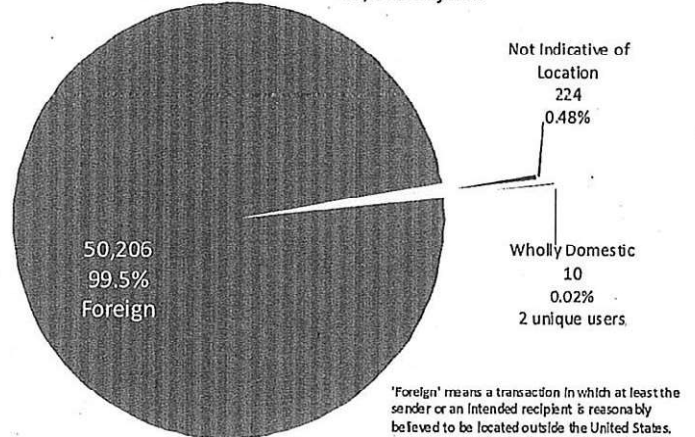


Fig. D Summary

50,440 objects



Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20360801

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



~~TOP SECRET//COMINT//NOFORN~~**Appendix B: Statistical Methodology – FAA Section 702 Upstream Manual Review**

~~(TS//SI//NF)~~ Using statistical analysis NSA determined the proportions of transactions satisfying certain criteria (e.g., proportion of FAA Section 702 upstream Internet transactions that are Multi-communication Transactions (MCT) versus transactions containing single, discrete communications). As further described below, transactions were categorized in various ways. The categorization process can be complex; to minimize categorization error, NSA used a statistical approach involving actual examination of an appropriate sample of transactions by experienced intelligence analysts. (The use of only a sample is a concession to the large volume of transactions and the labor-intensive nature of the categorization process.) That is, NSA traded "categorization error" for "statistical error"; the latter refers to the fact that by considering only a randomly sampled portion of the universe of transactions, NSA estimated the true proportions (as they exist in the universe) -- with error bounds and levels of confidence that can be stated justifiably.

~~(TS//SI//NF)~~ **THE SAMPLE.** As discussed more fully in the "NSA Characterization of Upstream Data: Process and Results," NSA identified 13,256,067 transactions acquired through NSA's FAA 702 upstream collection during a six-month period from January 1<sup>st</sup> through June 30<sup>th</sup>, 2011. Of those approximately 13.25 million transactions, a team of experienced intelligence analysts carefully examined 50,440 over a nearly one-month time period. The transactions were presented to the analysts in a randomized order, ensuring that a simple random sample would serve as the basis for conclusions – supported by statistical theory – about the true proportions of the 13.25 million-transaction universe.

~~(TS//SI//NF)~~ **ESTIMATES AND CONFIDENCE INTERVALS.** The proportions formed from the sampled transactions serve as unbiased estimates of the corresponding proportions of the 13,256,067-transaction universe. Further, for (six) selected proportions, NSA states a confidence interval for each. Collectively, these intervals have a simultaneous confidence level of 95%. This means that the intervals were produced by a procedure calibrated to produce, for at least 95% of the sample sets NSA could have drawn, intervals which all cover the corresponding true (i.e., universal) proportions. Individually, each interval has a higher level of confidence associated with it; component confidence levels are quoted below.

~~(TS//SI//NF)~~ For each of the six categories, NSA also states a confidence interval for the actual number of that category's transactions within the 13,256,067-transaction (January-June, 2011 upstream) universe. Such an interval is simply an equivalent representation of the corresponding proportion-interval (it is obtained by multiplying the endpoints of the proportion-interval by 13,256,067), and so the inclusion of such intervals does not affect the (95%) level of simultaneous confidence.

~~(TS//SI//NF)~~ Specifically: By sampling a subset of the universe (or *population*) of upstream transactions, NSA estimated the following six proportions. (Hereinafter,  $N$  denotes 13,256,067 – the size of that universe;  $M$  denotes the (unknown) actual number of MCTs in that universe).

- $M/N$ : the proportion of the population comprising MCTs;

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20360801

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



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

- $1-(M/N)$ : the proportion of the population comprising discrete transactions;
- the proportion of the population comprising MCTs in which all communications are either to or from NSA's tasked selector (hereinafter labeled "Target" MCTs);
- the proportion of the population comprising MCTs in which all communications are believed to either be to or from non-targeted persons located outside the United States (hereinafter labeled "Foreign" MCTs);
- the proportion of the population comprising MCTs in which the nature of one or more communications between non-targeted persons lacked sufficient information for NSA analysts to identify the location of the sender and all intended recipients (hereinafter labeled "Unknownable" MCTs);
- the proportion of the population comprising MCTs that NSA analysts assessed contain a wholly domestic not to, from, or about a tasked selector (hereinafter labeled "Confirmed Wholly Domestic").

~~(TS//SI//NF)~~ (The first of these proportions equals the total of the last four.) In the following, lower-case letters denote transaction counts as realized in the sample, in categories corresponding to their upper-case counterparts. That is,  $n$  is the number of transactions sampled (this turned out to be 50,440), and  $m$  is the number of MCTs in the sample.

~~(TS//SI//NF)~~ **OUTLINE OF PROCEDURE.** NSA designed a procedure that accepts a size- $n$  *simple random sample*<sup>1</sup> of the population, and produced from it estimates and confidence intervals for the six "true"<sup>2</sup> proportions NSA sought. The estimates NSA produced are simply the corresponding proportions as found in the sample – e.g., the sample proportion  $m/n$  was NSA's estimate of the population proportion  $M/N$ ; such a sample proportion is unbiased<sup>3</sup> for its population counterpart, meaning that were a sample proportion to be computed for each of the possible size- $n$  samples that could be drawn, the average of these sample proportions would equal the "true" (population) proportion.

<sup>1</sup> ~~(TS//SI//NF)~~ A simple random sample is one that is drawn in a way that ensures that all possible size- $n$  subsets of the (size- $N$ ) population have an equal chance of being selected; this sampling technique enables statistically justifiable claims by avoiding potential (known or unknown) sources of bias in the population (e.g., a periodic trend in the population over time).

<sup>2</sup> ~~(TS//SI//NF)~~ "True" refers to proportions that relate to the entire population, which cannot be determined for certain, as  $n$  is smaller than  $N$ .

<sup>3</sup> ~~(TS//SI//NF)~~ Unbiasedness means that the estimate is aiming for the right "target"; however, it indicates nothing about the precision of the estimate. An estimation procedure can be unbiased whether it is based on a small or large sample size  $n$ .

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



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

~~(TS//SI//NF)~~ To express precision appropriately, NSA designed its procedure to produce confidence intervals – one for each of the (six) population proportions of interest – having a simultaneous confidence level of 95%. This means that:

- Based on a sample, the procedure will produce a collection of intervals, each asserted to contain the true (population) proportion it targets.
- Because the procedure operates on a random sample, the interval endpoints are *random variables*; the particular collection of intervals a particular sample yields may fail to cover one or more of the population proportions it targets. But the procedure is designed so that this failure probability – *whatever* the true proportions are – is no more than 5%; that is, for at least 95% of the (size- $n$ ) simple random samples it might process, the procedure will produce intervals which *all* cover their targeted population proportions.
- In order to achieve this level of confidence about a collection of intervals simultaneously, the procedure is designed so that the respective failure probabilities associated with the component intervals total no more than 5%. In particular, this 5% was allocated as follows:
  - 2.5% to the proportion of “Confirmed Wholly Domestic”;
  - 0.67% to each of the “Target,” “Foreign,” “Unknown” proportions;
  - 0.5% to the proportion of MCT (i.e.,  $M/N$ ). As the proportions of discrete and MCT transactions are complementary (i.e., they total 1), the confidence interval for the proportion of discrete transactions is obtained by subtracting each of the endpoints for the MCT-interval from 1 – and it is the case that one of these intervals will cover its population target if and only if the other does. Therefore, there is no need to separately allocate “failure probability” to the proportion-of-discrete.

~~(TS//SI//NF)~~ The probability of drawing a sample resulting in one or more “failing” intervals is no more than the sum of the failure probabilities of the respective component intervals, hence the claim of 95% confidence for the procedure outlined here. The “no more” qualification makes this technique conservative: relationships (complicated and left unanalyzed) between the random variables involved may make the practical confidence level higher; 95% represents a worst-case claim. To achieve simultaneous 95% confidence, the 5% failure probability could have been allocated in any way. (Broadly: the lower the confidence level (i.e., the higher the failure probability), the narrower the intervals the procedure will produce. An extreme example: a procedure for 100% confidence intervals would produce uselessly wide intervals, as it would have to be able to claim that its intervals cover truth for *every* possible size- $n$  sample it could have received.) This procedure for simultaneous intervals is conservative in a further way: Just as the sum of the discrete and MCT proportions equals 1, so does the sum of the discrete, “Target,” “Foreign,” “Unknown,” and “Confirmed Wholly Domestic” proportions. It is difficult to exploit this latter constraint properly; NSA utilized the conservative method described here to ensure that its assertions about the procedure’s performance are valid.

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

~~(TS//SI//NF)~~ **CONFIDENCE-INTERVAL PROCEDURE FOR A SINGLE**

**PROPORTION.** As outlined above, the procedure for (95%) simultaneous confidence intervals was achieved by producing component confidence intervals based on (individually higher) levels of confidence (e.g., 99.5% for  $M/N$ ). The construction of component confidence intervals can be understood via the following example, using the  $M/N$  target. For the sample of size  $n$  to be observed,  $m$  represents the (random) number of MCTs to be realized in the sample. Formally,  $m$  has a *hypergeometric* distribution (arising from sampling transactions "without replacement"); to make the mathematical computations tractable, NSA approximated this distribution by a *binomial* distribution corresponding to sampling *with* replacement (in which each sampled transaction would be replaced after it is drawn, and hence would be eligible to be drawn multiple times). This approximation is uniformly conservative; i.e., it will result in wider intervals. The proportion to be estimated,  $M/N$ , appears as the (unknown) parameter (now denoted  $p$ ) of this binomial distribution. Treating  $m$  as a binomial random variable based on  $n$  trials, NSA used an accepted method (the *Clopper-Pearson* method) as the basis to devise its confidence-interval procedure for  $p$ . (Below, the notation  $B(n, q)$  refers to an  $n$ -trial binomial random variable having parameter  $q$ .) Upon observing  $m$ , NSA:

- Determines, for each of various proportions  $x$  between 0 and 0.5%, parameters  $q$  and  $r$  such that
  - $x$  is the probability that a  $B(n, q)$  random variable takes a value of at least  $m$  (but if  $m=0$ , take  $q$  to be 0);
  - $(0.5\% - x)$  is the probability that a  $B(n, r)$  random variable takes a value no larger than  $m$  (but if  $m=n$ , take  $r$  to be 1).

$r$  exceeds  $q$ ; the pair  $[q, r]$  determines an interval.

- Determines the narrowest of all such intervals  $[q, r]$  and reports it as the (99.5%) confidence interval for  $p = M/N$ .

~~(TS//SI//NF)~~ Practically, the  $q$ 's and  $r$ 's can be computed using *inverse Beta functions*, and computer software can find the narrowest interval efficiently.

*Remainder of this page intentionally left blank.*

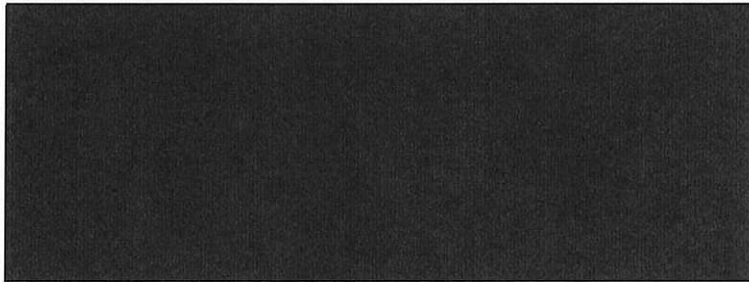


~~TOP SECRET//COMINT//NOFORN~~

## RESULTS:

	# of transactions in sample	Sample proportion (of 702 upstream)	Confidence interval for corresponding universal proportion	Confidence interval for the actual number (of the 13.25 million)
<b>Discrete</b>	45,359	0.8993	0.8955 – 0.9030	11,870,284 – 11,970,275
<b>MCT</b>	5,081	0.1007	0.0970 – 0.1045	1,285,792 – 1,385,783

	# of transactions in sample	Sample proportion (of MCT)	Confidence interval for corresponding universal (MCT) proportion	Confidence interval for the actual number (of the 13.25 million)
<b>TARGET</b>	713	0.01414	0.01274 – 0.01561	168,853 – 206,922
<b>FOREIGN</b>	4,134	0.08196	0.07867 – 0.08532	1,042,838 – 1,130,947
<b>UNKNOWABLE</b>	224	0.004441	0.003667 – 0.005293	48,609 – 70,168
<b>CONFIRMED WHOLLY DOMESTIC</b>	10	0.0001983	0.00007508 – 0.0003746	996 – 4,965



*Remainder of this page intentionally left blank.*

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

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

VERIFICATION

I declare under penalty of perjury that the facts set forth in this Appendix are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, Section 1746, on this 11<sup>th</sup> day of August, 2011.



[Statistician]  
National Security Agency

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

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

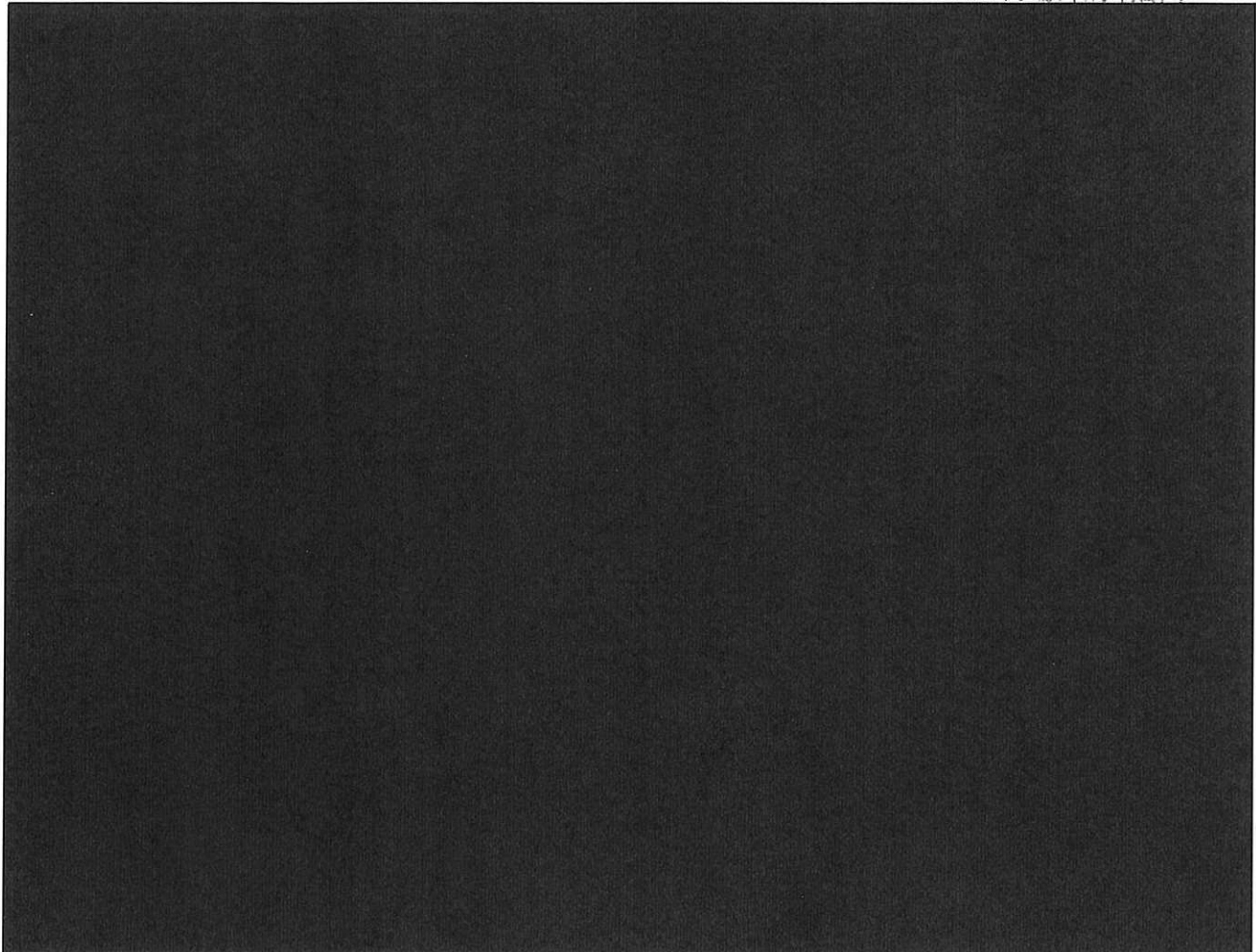
U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT 20 AUG 30 PM 4:12

WASHINGTON, D.C.

LEEANN FLYNN HALL



### NOTICE OF CLARIFICATIONS

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the following clarifications for the record in the above-referenced matters. The first two clarifications below concern certain statements

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

Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: 30 August 2036



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

made in documents previously submitted to this Court in the above-referenced matters.

The third and fourth clarifications below concern how the National Security Agency (NSA) will apply its section 702 minimization procedures to discrete communications within Multi-Communication Transactions (hereinafter "MCTs"). Specifically, outlined below is a multi-layered approach to help ensure that any United States person information contained within MCTs is treated in accordance with NSA's section 702 minimization procedures. This approach will not be altered without prior notice to this Court. ~~(TS//SI//NF)~~

## I. CLARIFICATIONS

### A. NSA Will Purge Any MCT Containing One or More Single, Discrete, Wholly Domestic Communications Upon Recognition. ~~(S)~~

As noted in the Government's submission of June 28, 2011, NSA does not intentionally acquire transactions containing wholly domestic communications, and has implemented [REDACTED] means which are reasonably designed to prevent the acquisition of such transactions. Notice of Filing of Government's Response to the Court's Supplemental Questions of June 17, 2011 (hereinafter "June 28th Submission") at 12. The June 28th Submission further asserted that "in the event NSA recognizes a wholly domestic communication<sup>[1]</sup> which is not to, from, or about a tasked selector which it has

---

<sup>1</sup> As noted in the Government's June 28th Submission, the Government defined a "wholly domestic communication" to be a communication as to which the sender and all intended recipients are located within the United States. The Government further noted that it included within that term any discrete communication within a transaction where the sender and all intended recipients of the discrete

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

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

unintentionally acquired in the course of conducting its Section 702 upstream Internet collection, NSA would handle the entire transaction in accordance with subsection 1806(i) and either purge it or, if appropriate, seek authorization from the Attorney General to retain it." *Id.* Accordingly, in the event that NSA's section 702 upstream collection of Internet communications resulted in the unintentional acquisition of a transaction containing a wholly domestic communication, NSA would purge the entire transaction upon recognition, unless the Attorney General authorized its retention after first determining that its contents indicated a threat of death or serious bodily harm to any person. ~~(TS//SI//NF)~~

To aid in the recognition of wholly domestic communications within an MCT, if an NSA analyst seeks to use a discrete communication within the MCT (for example, in a FISA application, intelligence report, or section 702 targeting), the analyst will first perform checks to determine the locations of the users of the electronic communications accounts/addresses/identifiers referenced in that discrete communication within the MCT to the extent reasonably necessary to determine whether that communication is wholly domestic. For example, if the "active user"<sup>2</sup> is a tasked selector, no checks need

---

communication were located in the United States at the time the communication was acquired. *See* June 28th Submission at 2. ~~(TS//SI//NF)~~

<sup>2</sup> As noted in the Government's filing on August 16, 2011, the Government defined the "active user" as follows: "[w]hen NSA acquires an Internet transaction between an individual using an electronic communications account/address/identifier and his/her service provider, that individual is the 'active user' for that transaction." NSA Characterization of Upstream Data: Process and Results, filed August 16, 2011 (hereinafter "August 16th Submission") at 4 n.13. ~~(TS//SI//NF)~~

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



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

be done, because the user of the tasked selector, who by operation of the NSA targeting procedures is a non-United States person reasonably believed to be located outside the United States, would be either the sender or an intended recipient of each of the discrete communications contained within the MCT. If the active user is not a tasked selector, NSA would attempt to determine the active user's location;<sup>3</sup> if that check indicates that the active user is located outside the United States, no further checks need be done, because the foreign-based active user would be either a sender or intended recipient of each of the discrete communications within the MCT. In the absence of a more efficient and effective means of recognizing the presence of a wholly domestic communication within an MCT, the Government submits that this process is reasonably designed to recognize and purge at the earliest practical point in the analytic process any unintentionally acquired wholly domestic communication. ~~(TS//SI//NF)~~

B. Clarification of Certain Information Contained within the Government's August 16, 2011 Submission. (S)

In the August 16th Submission, the Government advised the Court that NSA conducted a manual review of a statistically representative sample of Internet communications acquired through NSA's section 702 upstream collection. As explained in the August 16th Submission, NSA identified 5,081 transactions within the representative sample as being MCTs. NSA determined that of those 5,081 MCTs, 4,847

<sup>3</sup> To determine the location of the non-targeted active user, NSA would perform the same sort of [REDACTED] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its section 702 targeting procedures. ~~(TS//SI//NF)~~

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

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

contained discrete communications believed to be to or from persons located outside the United States and thus are not believed to contain any wholly domestic communications.<sup>4</sup> NSA further determined that 10 of the 5,081 MCTs appeared to contain at least one wholly domestic communication. However, NSA was unable to definitively determine whether the remaining 224 MCTs contained wholly domestic communications, because those MCTs lacked information sufficient to identify the active user or determine the active user's location. Nevertheless, NSA asserted that it had no basis to believe any of these 224 MCTs contained wholly domestic communications. ~~(TS//SI//NF)~~

As noted above, these 224 MCTs lack any definitive technical data or content that would enable NSA to characterize the communications within them as being wholly domestic. Despite the absence of such definitive information, it is nevertheless reasonable to presume that none of the discrete communications contained within these MCTs are wholly domestic. Specifically, each of these MCTs was acquired because it contained at least one discrete communication to, from, or about a tasked selector used by a person who, by operation of NSA's section 702 targeting procedures, is a non-U.S. person reasonably believed to be located outside the United States. With respect to MCTs that contain discrete communications to or from a tasked selector, it is reasonable

---

<sup>4</sup> This figure 4,847 is the sum of 713 MCTs reviewed by NSA analysts as containing a tasked selector as the active user and 4,134 MCTs reviewed by NSA analysts as containing discrete communications believed to be to or from non-targeted persons located outside the United States. See August 16th Submission at 5 nn.15 & 16. ~~(TS//SI//NF)~~

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



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

to presume, given the absence of information to the contrary, that the active user of the MCT is likewise a non-U.S. person reasonably believed to be located outside the United States. *See In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC Apr. 25, 2008) (hereinafter "Yahoo Directives Mem. Op.") (recognizing that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas") (footnote omitted). Similarly, because it is reasonable to presume that the active user of the MCT is a non-U.S. person reasonably believed to be located outside the United States, one can also reasonably presume, given the absence of information to the contrary, that the other persons with whom the active user has been in contact are also non-United States persons located outside the United States. ~~(TS//SI//NF)~~

Of note, an experienced team of NSA analysts manually reviewed the content of each of these 224 MCTs and did not observe any U.S. person information within any of the discrete communications contained therein. NSA analysts are trained to use their best judgment to recognize and identify U.S. person information that may be present within any SIGINT collection and to apply minimization procedures to such information as required by the authority under which that information was acquired.

While the technical information present for each of these transactions was not indicative of the location of the sender or all intended recipients of any communication other than

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

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

those more specifically to or from NSA's tasked selector, none of the information or data intelligible to those analysts conducting the review was identifiable as U.S. person information. ~~(TS//SI//NF)~~

Moreover, with respect to MCTs acquired because they contain discrete communications about a tasked selector, the [REDACTED] means by which NSA ensures it does not intentionally acquire wholly domestic communications limits, in all but a minute percent of cases, the acquisition of MCTs to persons located outside the United States, who reasonably can be presumed to be non-United States persons. Thus, to the extent that the MCTs of those non-United States persons contain discrete communications that are not to, from, or about a tasked selector, those communications are unlikely to be to or from United States persons or persons located in the United States. *Id.* To be sure, the [REDACTED] means by which NSA ensures it does not intentionally acquire wholly domestic communications are not perfect, and it is possible that NSA may unintentionally acquire MCTs containing wholly domestic communications. Indeed, as previously explained to the Court, NSA was able to identify MCTs containing wholly domestic communications in the representative sample. NSA was able to do so, however, only because the communications in those MCTs bore recognizable indicia of being wholly domestic (i.e., they contained concrete information contrary to the presumption). The 224 MCTs here lack any such indicia.

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



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

Accordingly, it is reasonable to presume that these 224 MCTs do not contain wholly domestic communications. ~~(TS//SI//NF)~~

C. Clarification Concerning How NSA Will Apply its Section 702 Minimization Procedures to Discrete Communications Within MCTs. ~~(S)~~

In order to help ensure that NSA intelligence analysts handle any United States person information they encounter within a discrete communication within an MCT<sup>5</sup> in accordance with NSA's section 702 minimization procedures, NSA will apply the following multi-layered approach:

- NSA will train its analysts to recognize MCTs and how to appropriately handle the discrete communications contained within them, as further described below.
- NSA analysts seeking to use a discrete communication within an MCT (for example, in a FISA application, intelligence report, or section 702 targeting) will assess whether the discrete communication is to, from, or about a tasked selector.
  - If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the NSA minimization procedures.
  - If the discrete communication is not to, from, or about a tasked selector, and also is not to or from an identifiable U.S. person, that communication

---

<sup>5</sup> NSA extracts metadata from Internet communications acquired through its section 702 upstream collection, including discrete communications within MCTs. NSA's architecture for the extraction, analysis, and storage of metadata from Internet communications acquired pursuant to section 702 differs markedly from the architecture NSA analysts use to analyze content from such communications. Currently, it is not operationally feasible in an effective or a timely manner for NSA analysts to identify and further evaluate the nature of upstream Internet communications from the extracted metadata within NSA's metadata repositories. Nevertheless, if an Internet communication has been identified for purge (for any reason, including its having been identified as containing a wholly domestic communication) in one of NSA's content repositories, any corresponding metadata extracted from that communication and stored in NSA's metadata repositories is also purged: ~~(TS//SI//NF)~~

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



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

(including any U.S. person information therein) will be handled in accordance with the NSA minimization procedures.

- If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person, that communication cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use.
- To reinforce training and awareness of these aspects of NSA upstream collection, NSA will add a cautionary banner to the tools NSA analysts use to view the content of communications acquired upstream under section 702.<sup>6</sup> The banner will direct analysts to consult guidance on how to identify MCTs and how to handle them.
- Prior to using any one or more discrete communications contained in an MCT (for example, in a FISA application, intelligence reporting, or section 702 targeting), an NSA analyst must:
  - verify either that the discrete communication is to, from, or about a tasked selector or that it is not to or from a U.S. person;<sup>7</sup>

<sup>6</sup> Because NSA currently lacks [REDACTED] means to reliably identify MCTs, the cautionary banner will be broadly displayed on tools NSA analysts use to view the content of all upstream transactions, except in those limited number of transactions that can be first identified [REDACTED]

[REDACTED] As noted in the August 16th Submission, however, the banner is over-applied to NSA's upstream collection the majority of the time (i.e., NSA estimates that the banner will be over-applied more than approximately 83% of the time to single, discrete communications in upstream collection). See August 16th Submission at 1 n.2. There will also be circumstances in which the banner is under-applied to NSA's upstream collection due to issues such as [REDACTED]

[REDACTED] In sum, NSA's experience has shown that there may be more efficient and effective means of handling MCTs in the long term and may seek to revise or discontinue use of the banner at a later time. Regardless, NSA will not implement any such revisions without prior notification of the Court. ~~(TS//SI//NF)~~

<sup>7</sup> To help determine whether a discrete communication not to, from, or about a tasked selector is to or from a U.S. person, NSA would perform the same sort of [REDACTED] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its section 702 targeting procedures. ~~(TS//SI//NF)~~

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

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

- verify that the discrete communication is not a wholly domestic communication; and
- appropriately document these verifications.

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

D. Clarification Concerning How NSA Will Conduct Queries of Communications Acquired Under Section 702 Using U.S. Person Identifiers. ~~(S)~~

Subsection 3(b)(5) of the NSA minimization procedures currently pending before the Court provide:

Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Any United States person identifiers used as terms to identify and select communications must be approved in accordance with NSA procedures.

As discussed in the previous filings, the Government acknowledged that "rigorous and strict controls" will be placed on the retrieval of U.S. person information consistent with statutory requirements and Congressional intent. *See* Government's Response to the Court's Briefing Order of May 9, 2011 (hereinafter "June 1st Submission") at 23; June 28th Submission at 24-25; *cf.* H.R. Rep. No. 95-1283, pt. 1 at 59 (1978) (Congress recognized that minimizing the retention of information concerning U.S. persons for counterintelligence or counterterrorism purposes can be accomplished through the application of "rigorous and strict controls"). In light of the results of NSA's manual review of upstream collection described in the Government's August 16th Submission,

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



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

NSA will limit the use of United States person identifiers as computer selection terms to identify and select communications for analysis to communications acquired from Internet service providers [REDACTED]

[REDACTED] unless NSA can later develop a capability or procedures to strictly limit such queries to portions of NSA's upstream collection that contain only discrete communications to, from, or about NSA's tasked selector.

Accordingly, United States person identifiers will not be used as computer selection terms for communications acquired through NSA's upstream collection unless such capabilities are later developed by NSA. NSA would not begin querying upstream collection using United States person identifiers without prior notice to the Court.

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

### III. CONCLUSION

As previously explained to the Court, the Government believes that NSA's upstream collection is consistent with the Act and the Fourth Amendment even though such collection may result in the acquisition of MCTs containing discrete communications that are not to, from, or about a tasked selector, or that are wholly domestic in nature. The Government respectfully submits, for the reasons explained in the previous filings and herein, including the multi-layered approach described above, that the results of NSA's analysis of a representative sample of its upstream collection provide a basis upon which the Court can approve, as consistent with the Act and the

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

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

Fourth Amendment, NSA's continued acquisition of foreign intelligence information through its section 702 upstream collection. ~~(TS//SI//NF)~~

First, the results of NSA's analysis of a representative sample of its upstream collection indicates that the scope of the intrusion into Fourth Amendment-protected interests caused by NSA's upstream collection is reasonable. Specifically, NSA's review revealed that the vast majority of the Internet communications acquired by NSA's upstream collection -- approximately 90% -- are single, discrete communications to, from, or about a tasked selector. See August 18th Submission at 3. Since the first DNI/AG 702(g) certification, this Court has consistently found the acquisition of such communications to be in accordance with the Act and the Fourth Amendment. See [REDACTED] Mem. Op. at 15-20, 32-41; see also, e.g., *In re DNI/AG Certification* [REDACTED] Docket No. [REDACTED] Mem. Op. at 22-27, 29 (USFISC Apr. 7, 2009). Contributing significantly to that finding, in the Court's view, was the application of robust minimization procedures similar to those used in other collections authorized under the Act. See, e.g., [REDACTED] Mem. Op. at 29-31, 40-41. ~~(TS//SI//NF)~~

NSA's review of its upstream collection further revealed that of the approximately 10% of Internet communications acquired through upstream collection that are MCTs, approximately 14% of those MCTs are those of persons targeted in accordance with NSA's targeting procedures. See August 18th Submission at 4. As such, all of the discrete communications within those MCTs are communications to or from

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



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

the target. This Court repeatedly has found that the acquisition of communications to or from the target to be consistent with the Act and the Fourth Amendment. *See, e.g.,* [REDACTED] Mem. Op. at 15-17, 33. The fact that multiple such communications may be acquired within a single MCT of a target should not alter that conclusion. ~~(TS//SI//NF)~~

NSA's review also found that approximately 52% of the other MCTs featured an active user who was located outside of the United States. *See* August 18th Submission at 4-5. Additionally, although approximately 33% of the other MCTs required further research, such research ultimately led NSA to conclude that all discrete communications in those MCTs included at least one user who was located outside of the United States.<sup>8</sup> *See id.* at 7. Although these two sets of communications -- which combined represent approximately 85% of all MCTs -- were not communications to or from a tasked selector, the Court has found that NSA's acquisition of single, discrete "abouts" communications featuring a tasked selector is consistent with the Act and the Fourth Amendment, *see, e.g.,* [REDACTED] Mem Op. at 17-20 & n.17, 32-41, and the Government has asserted that NSA's acquisition of MCTs containing such discrete communications is consistent with both the Act and the Fourth Amendment, *see* June 1st Submission at 3-24; June 28th Submission at 13-17, 22-24. Notably, the nature of these MCTs further supports assertions made by the Government in those previous filings. For instance, the

---

<sup>8</sup> Although no further substantive information is available on the 224 MCTs that NSA is otherwise unable to definitively determine are not wholly domestic, for the reasons more specifically discussed above, the Government submits that it is reasonable for the Court to presume that these 224 MCTs do not contain wholly domestic communications. ~~(TS//SI//NF)~~

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



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

Government asserted that "it is reasonable to presume that most of the discrete communications that may be within the acquired transaction -- even those that are not to or from a tasked selector -- are between non-United States persons located outside the United States." June 28th Submission at 5; *see also id.* at 23; *cf.* Yahoo Directives Mem. Op. at 87 (recognizing that "the vast majority of persons who are located overseas are non United States persons and that most of their communications are with other, non-United States persons, who are located overseas") (footnote omitted), *aff'd*, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008). ~~(TS//SI//NF)~~

In sum, NSA's review revealed that more than 99% of the MCTs it collects -- and therefore more than 99.9% of its overall upstream collection -- do not feature wholly domestic communications; the acquisition of such MCTs does not violate either the Act or the Fourth Amendment. Although NSA has determined that less than one percent the MCTs acquired through its upstream collection -- and thus less than 0.1% of its overall upstream collection -- likely include wholly domestic communications,<sup>9</sup> *see*

---

<sup>9</sup> Even in those cases where an MCT contained a wholly domestic communication, NSA's review indicated that a majority of the total discrete communications were not wholly domestic. For instance, of the 25 discrete communications included in the ten MCTs that did contain wholly domestic communications, a majority of those discrete communications (at least 15) were assessed to not be wholly domestic. *See* August 18th Submission at 5-7. This finding further bolsters some of NSA's assessments in the previous filings. For example, NSA assessed [REDACTED]

[REDACTED] " *See* June 1 Submission at 11. Similarly, NSA also assessed "that a United States-based user would [REDACTED] only in a minute percentage of cases." *Id.*; *see also id.* at 9 ("NSA's acquisition of transactions or single Internet communications between [REDACTED] currently occurs only in a very small percentage of cases."). ~~(TS//SI//OC,NF)~~

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

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

August 18th Submission, NSA's acquisition of such MCTs is nevertheless permissible under the Act and the Fourth Amendment. As described in detail in the previous filings, NSA is currently incapable of preventing the acquisition of MCTs, regardless of whether they contain wholly domestic communications, without ceasing its upstream collection entirely (except for [REDACTED]). See June 1st Submission at 27-28; June 28th Submission at 9-10. Given the significant foreign intelligence information obtained through NSA's upstream collection, along with the multi-layered approach described above -- including specialized training given to analysts, a banner applied to upstream collection containing MCTs, restrictions on use of MCTs, destruction of MCTs containing a wholly domestic communication, and a prohibition on using U.S. person identifiers to query section 702 upstream collection --

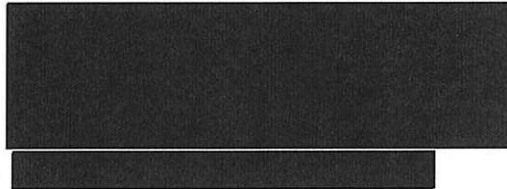
--- The remainder of this page intentionally left blank ---

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

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

the Government submits that NSA's acquisition of foreign intelligence information through upstream collection, including the acquisition of MCTs, is reasonable and consistent with the Act and the Fourth Amendment. ~~(TS//SI//NF)~~

Respectfully submitted,

A large black rectangular redaction box covering the signature and name of the official.

Office of Intelligence  
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 the foregoing "Notice of Clarifications" are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 30th day of August, 2011. (U)



Signals Intelligence Directorate Compliance Architect  
National Security Agency

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

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

OCT 31 PM 5:11

LEEANN FLYNN HALL  
CLERK OF COURT  
UNDER SEAL

GOVERNMENT'S EX PARTE REQUEST FOR ISSUANCE OF NOTICES ~~(S)~~

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully requests the Court to issue the notices attached hereto. These notices inform certain electronic communication services providers that have received directives pursuant to 50 U.S.C. § 1881a(h) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), that the Government's acquisition of foreign intelligence information under such directives may continue while this Court reviews amendments to the [REDACTED] above-captioned certifications.

~~(S//OC/NF)~~

1. On October 3, 2011, this Court issued a Memorandum Opinion and Order concerning the following matters: (1) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of

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

Classified by: Lisa O. Monaco, Assistant Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: 31 October 2036



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

Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [REDACTED]

which was filed on April 20, 2011; [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (S//OC/NF)

2. The Court's Order granted in part and denied in part the Government's request for the Court to approve DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] See Order at 2. In particular, the Court found that the certifications contained all of the required elements. See *id.* at 2-3. The Court further found that with respect to the acquisition of discrete Internet communications from Internet service providers [REDACTED]

[REDACTED]

[REDACTED] the targeting and minimization procedures were consistent with the requirements of the Act and the Fourth Amendment to the Constitution of the United States. See *id.* at 3. However, in the context of the National Security Agency's (NSA)

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

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

upstream collection,<sup>1</sup> with respect to the acquisition of certain Internet transactions featuring multiple, discrete communications, the Court found that NSA's minimization procedures did not meet the Act's definition of minimization procedures, and that NSA's targeting and minimization procedures were not consistent with the Fourth Amendment to the Constitution of the United States. See Order at 3. ~~(TS//SI//OC/NF)~~

3. On October 4, 2011, the Government respectfully requested, and the Court issued, secondary orders reflecting the Court's approval in part, as described in the Court's Memorandum Opinion and Order of October 3, 2011, to the electronic communication service providers who provide the Government with information, facilities, or assistance necessary to accomplish PRISM collection. [REDACTED]

[REDACTED] These secondary orders specified that, with respect to the acquisitions conducted with the assistance of these providers, the Court's October 3, 2011, Order found that the certifications contained all of the required elements and that the targeting and minimization procedures submitted with those certifications were consistent with the Act and the Fourth Amendment. ~~(S//OC/NF)~~

---

<sup>1</sup> Pursuant to its Section 702 authorities, NSA collects information from facilities (such as e-mail accounts) in two ways: through PRISM collection, with the assistance of Internet Service Providers [REDACTED] or by selecting for acquisition communications to, from, or about those facilities that are [REDACTED]

This second method of collection is referred to as NSA's "upstream" collection of communications. ~~(TS//SI//NF)~~

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

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

4. On October 5, 2011, the Government respectfully requested, and the Court issued, secondary orders reflecting the Court's approval in part, as described in the Court's Memorandum Opinion and Order of October 3, 2011, to the electronic communication service providers who provide the Government with information, facilities, or assistance necessary to accomplish NSA's upstream collection. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] These secondary orders specified that the Government could continue to acquire foreign intelligence information with the assistance of these electronic communication service providers during the time period that the Government was electing to either correct the deficiencies identified by the Court in its October 3, 2011, Opinion and Order within 30 days, or cease implementation of the certifications insofar as they permit the acquisition of certain Internet communications. ~~(TS//SI//OC/NF)~~

5. On October 31, 2011, the Attorney General, in consultation with the Director of National Intelligence (DNI), adopted amended NSA minimization procedures for use with DNI/AG 702(g) Certifications [REDACTED] On October 31, 2011, the Attorney General and DNI amended DNI/AG 702(g) Certifications [REDACTED] [REDACTED] to permit the use of the revised NSA minimization procedures under those certifications. The amendments to DNI/AG 702(g) Certifications [REDACTED]

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

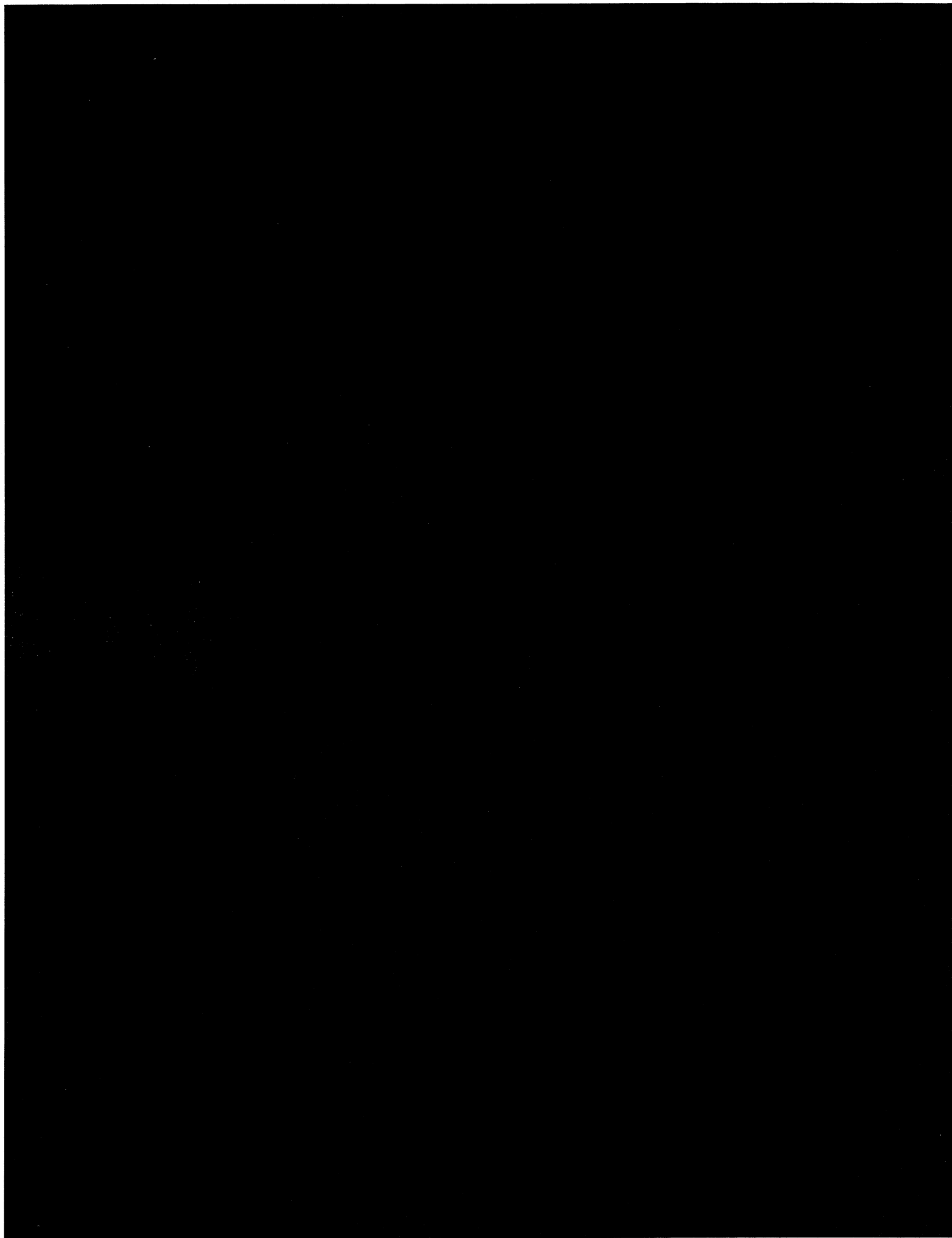


~~TOP SECRET//COMINT//ORCON//NOFORN~~

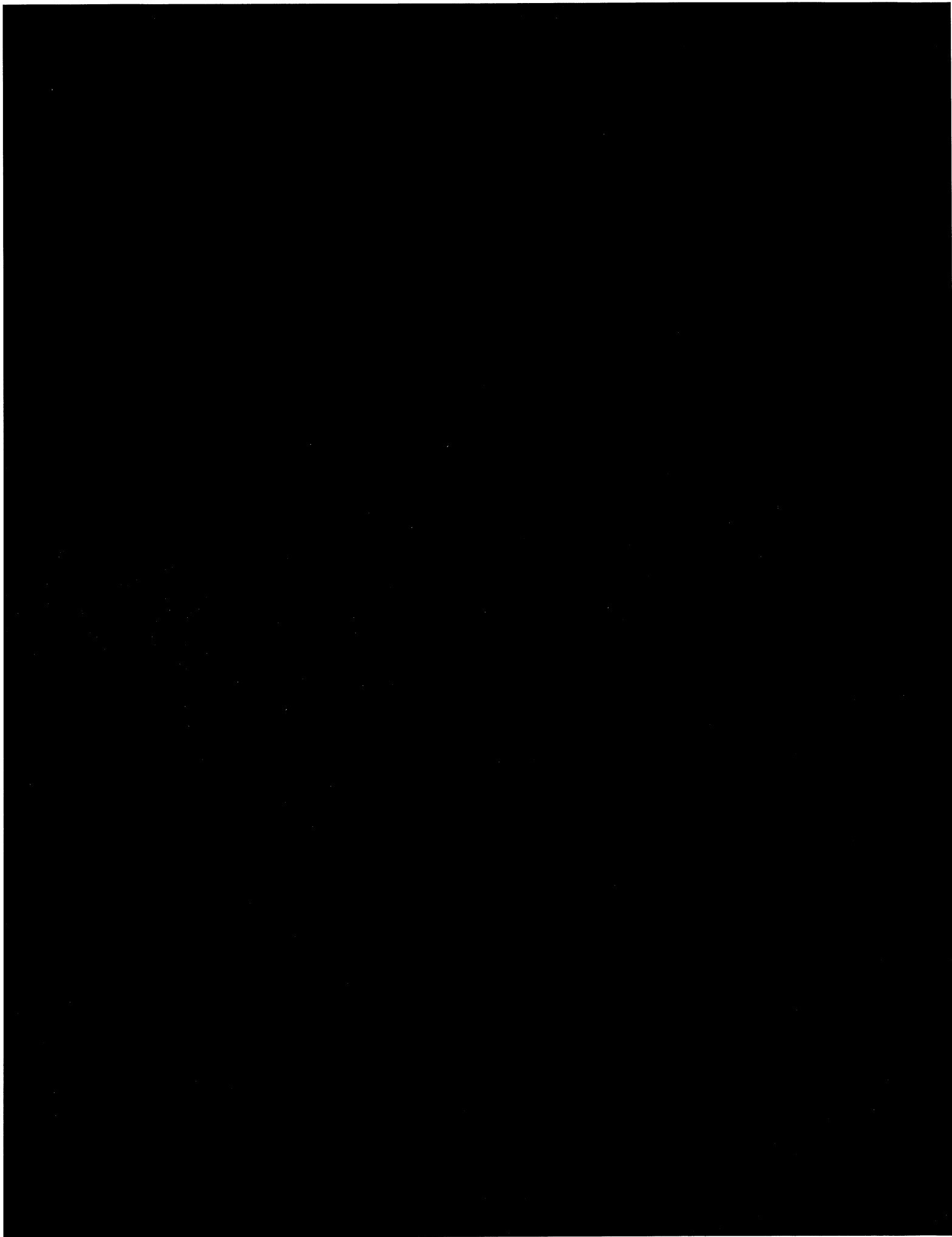
████████ along with the amended NSA minimization procedures, were submitted to the Court on October 31, 2011; and became effective immediately. ~~(S//OC/NF)~~

6. Pursuant to 50 U.S.C. § 1881a(i)(1)(B), this Court has 30 days from the date of submission of a certification to review, and issue an order concerning, the certification and the targeting and minimization procedures submitted therewith. Because the amended certifications, with amended NSA minimization procedures, were submitted to the Court on October 31, 2011, the Court will have until November 30, 2011, to complete its review, and issue an order, concerning the amendments to DNI/AG 702(g) Certifications ██████████ and the amended NSA minimization procedures. This time period extends beyond November 2, 2011, the date specified in the Court's October 5, 2011, secondary orders to the electronic communications service providers assisting NSA in conducting upstream collections. Accordingly, the Government respectfully requests that the Court issue the notices attached hereto, which inform such providers that the Government may continue to acquire Internet communications with the assistance of such providers until the Court issues an order

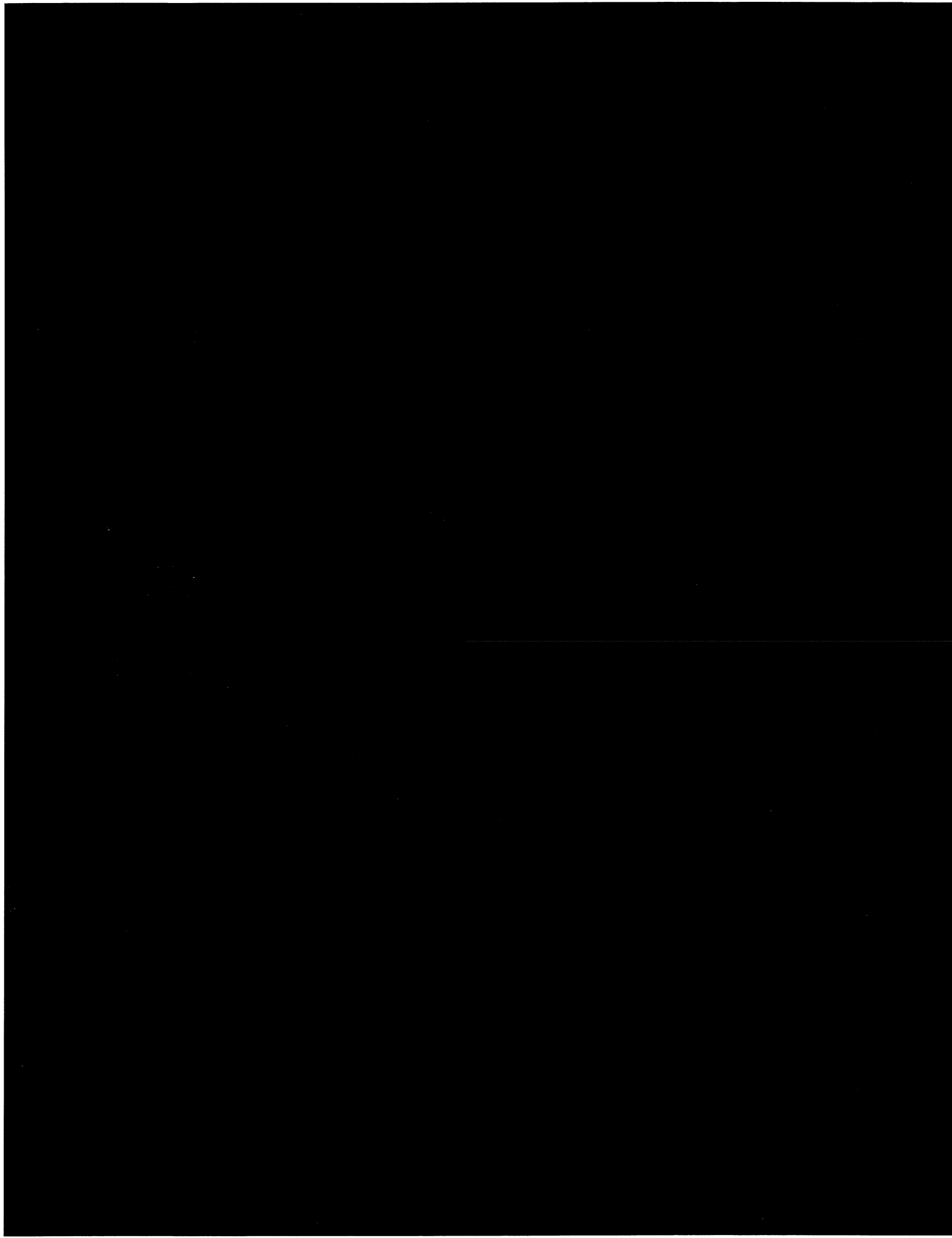
~~TOP SECRET//COMINT//ORCON//NOFORN~~

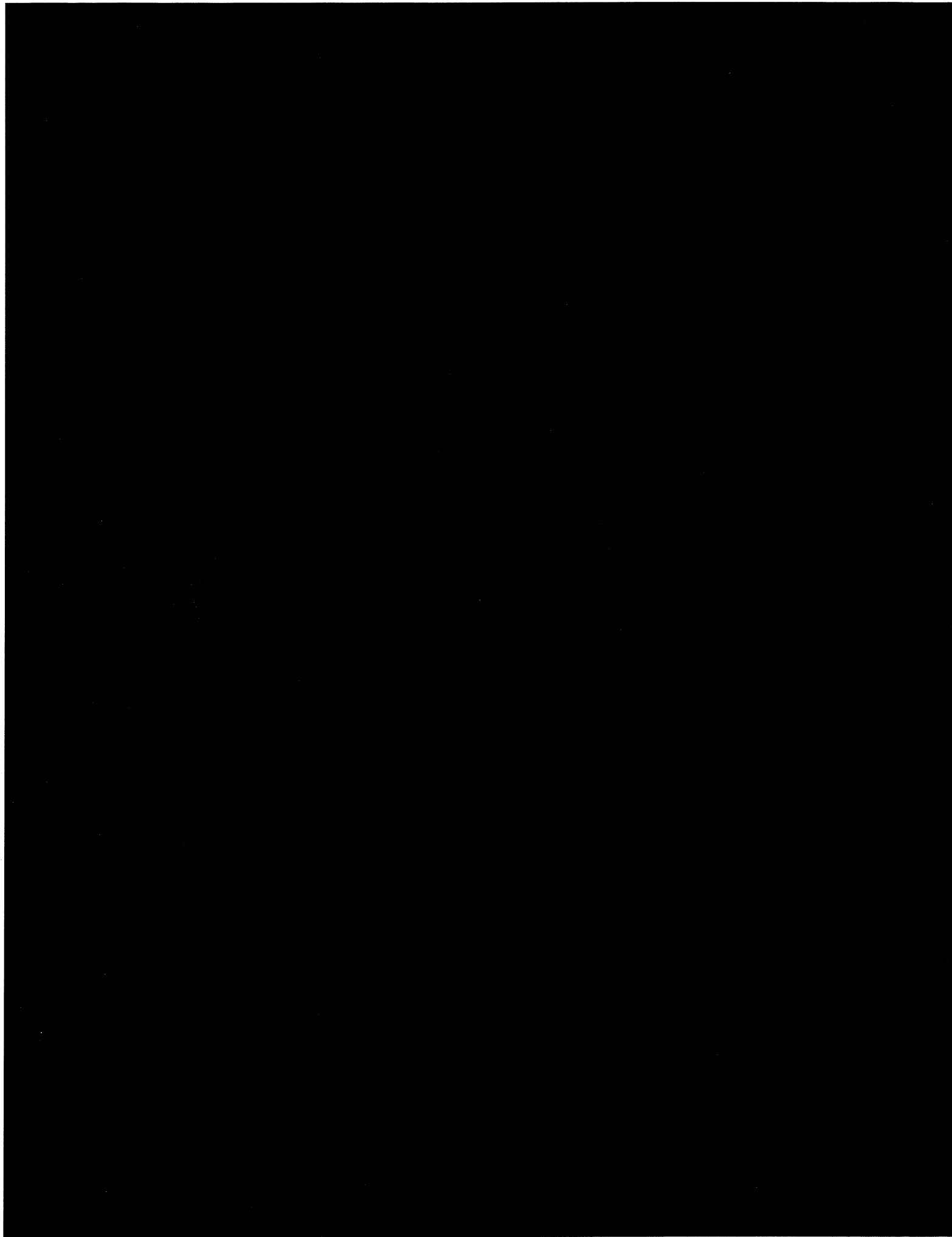


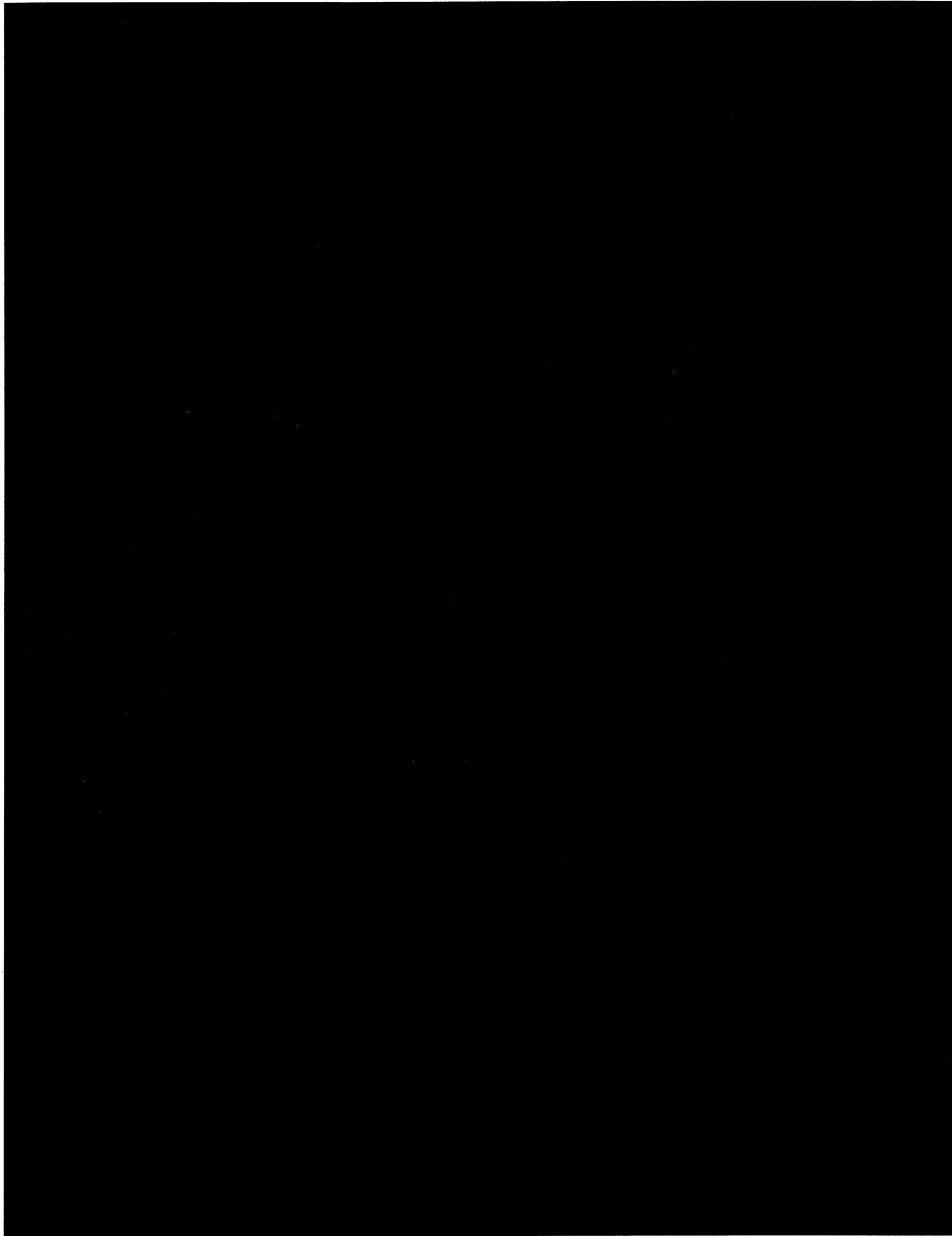




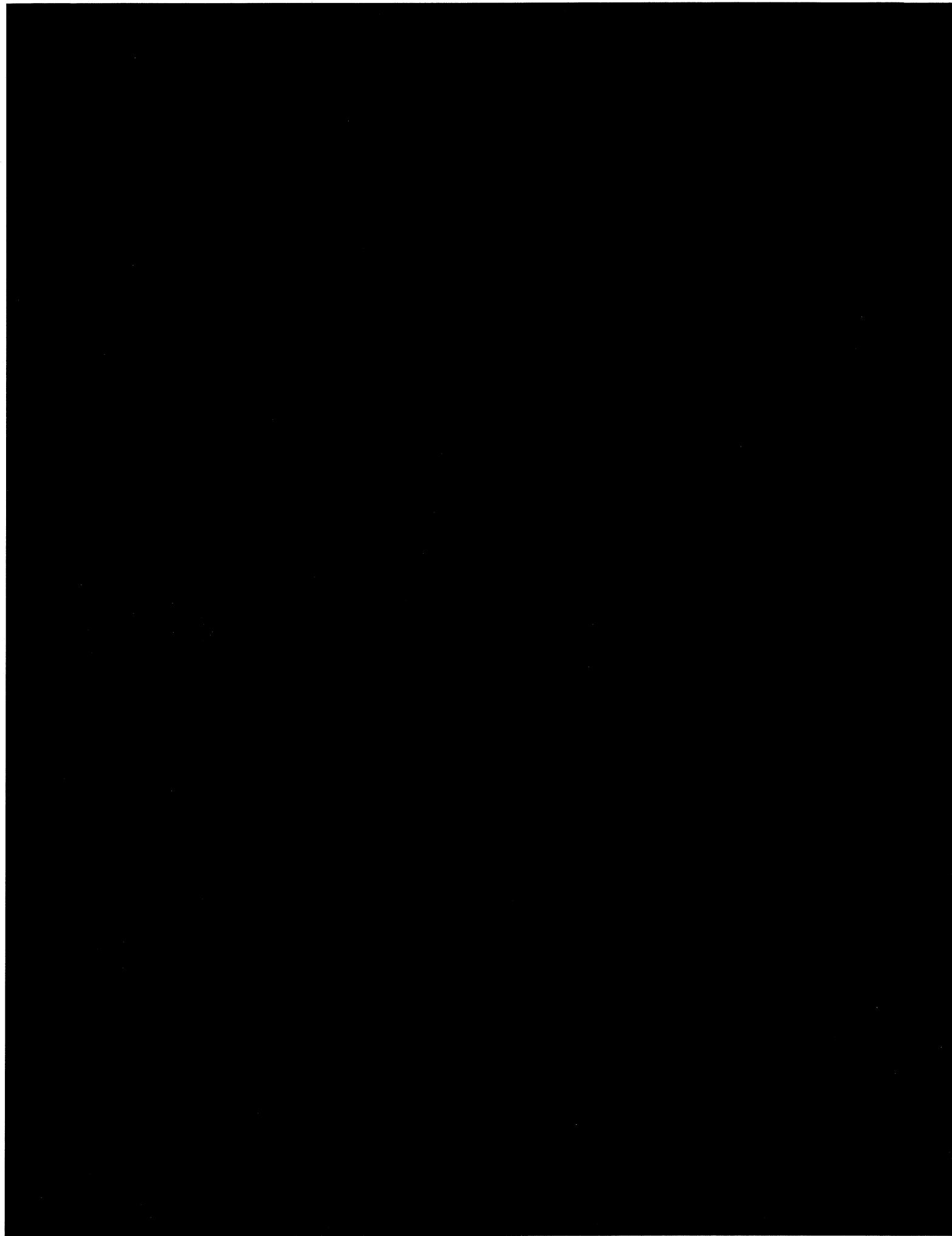


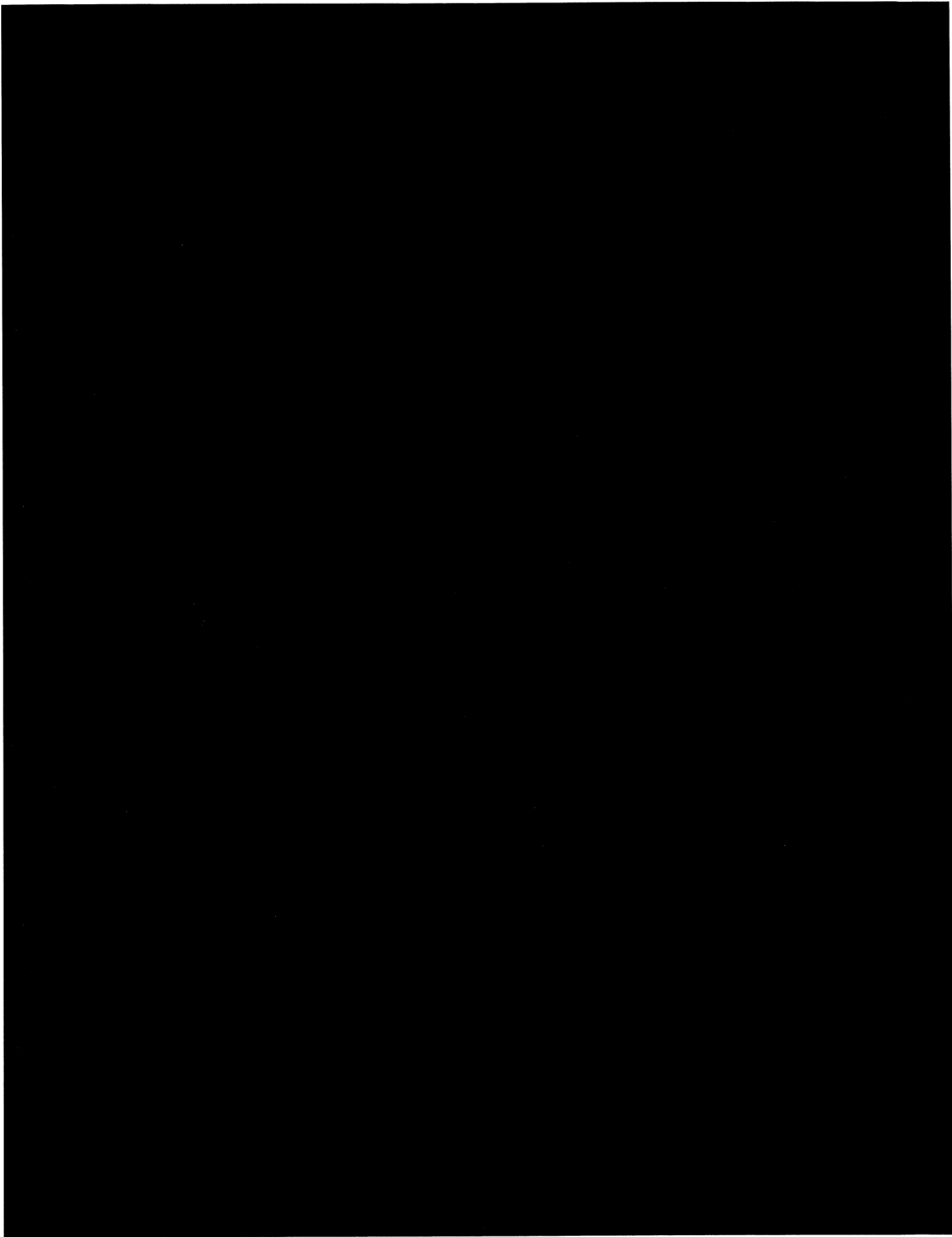


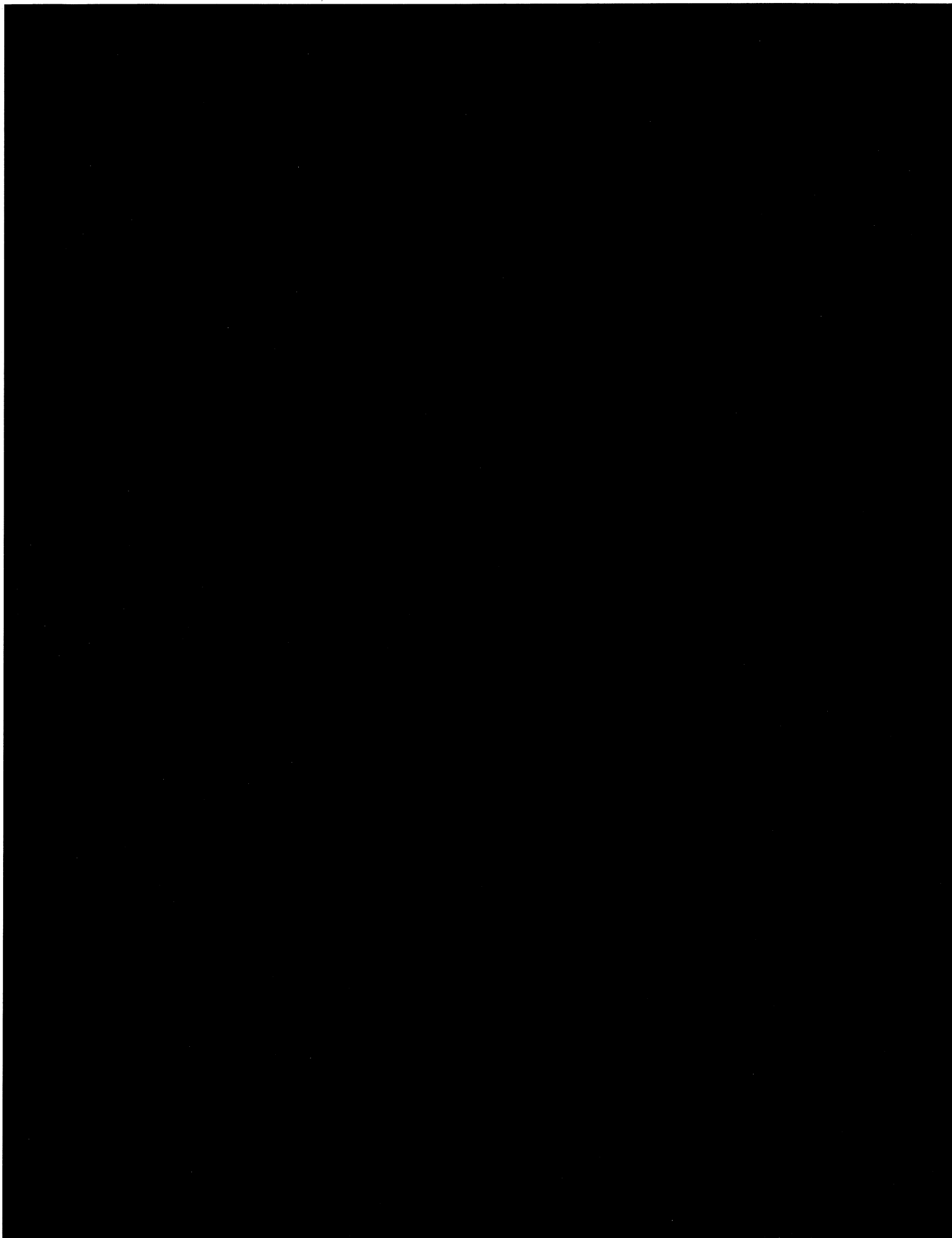


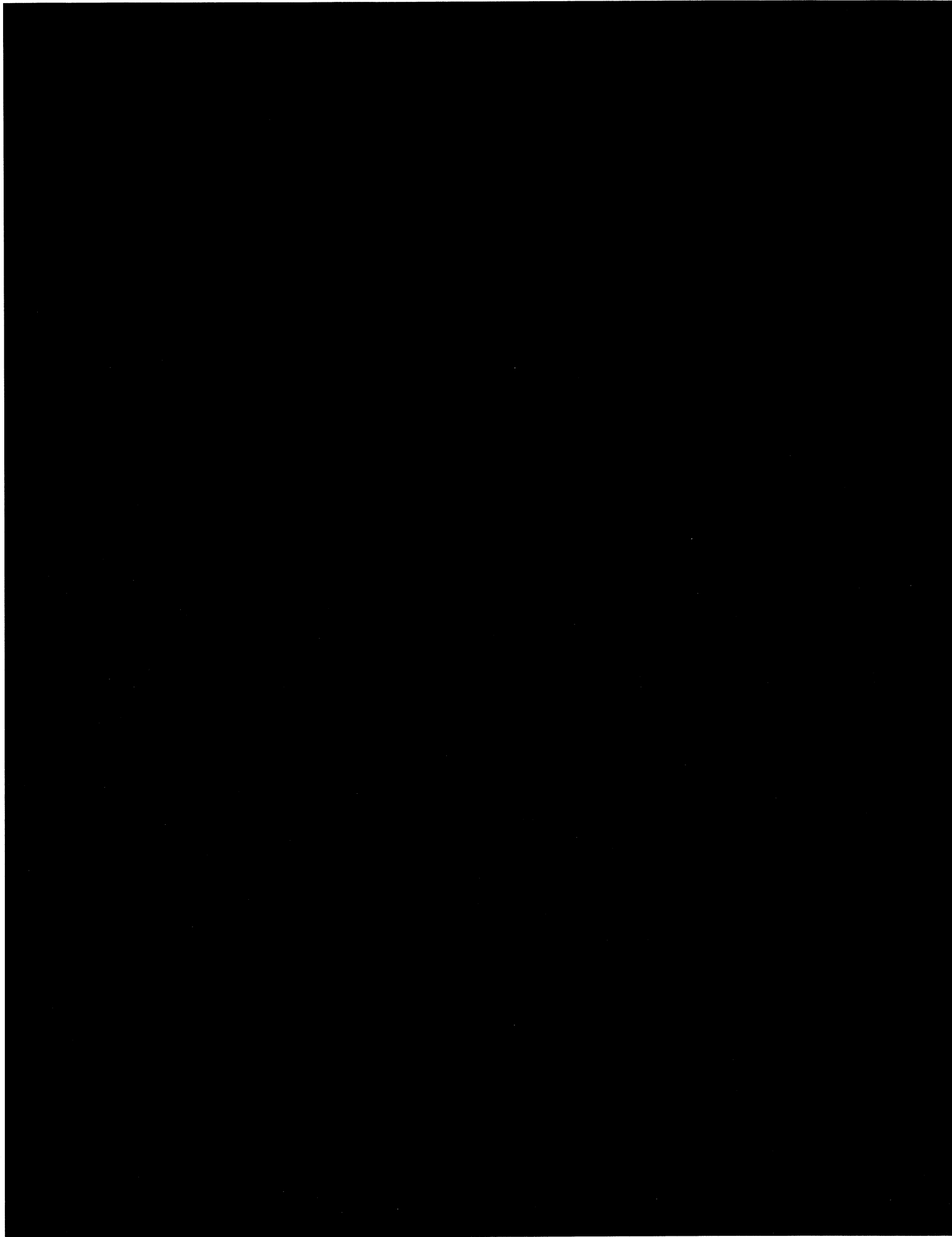






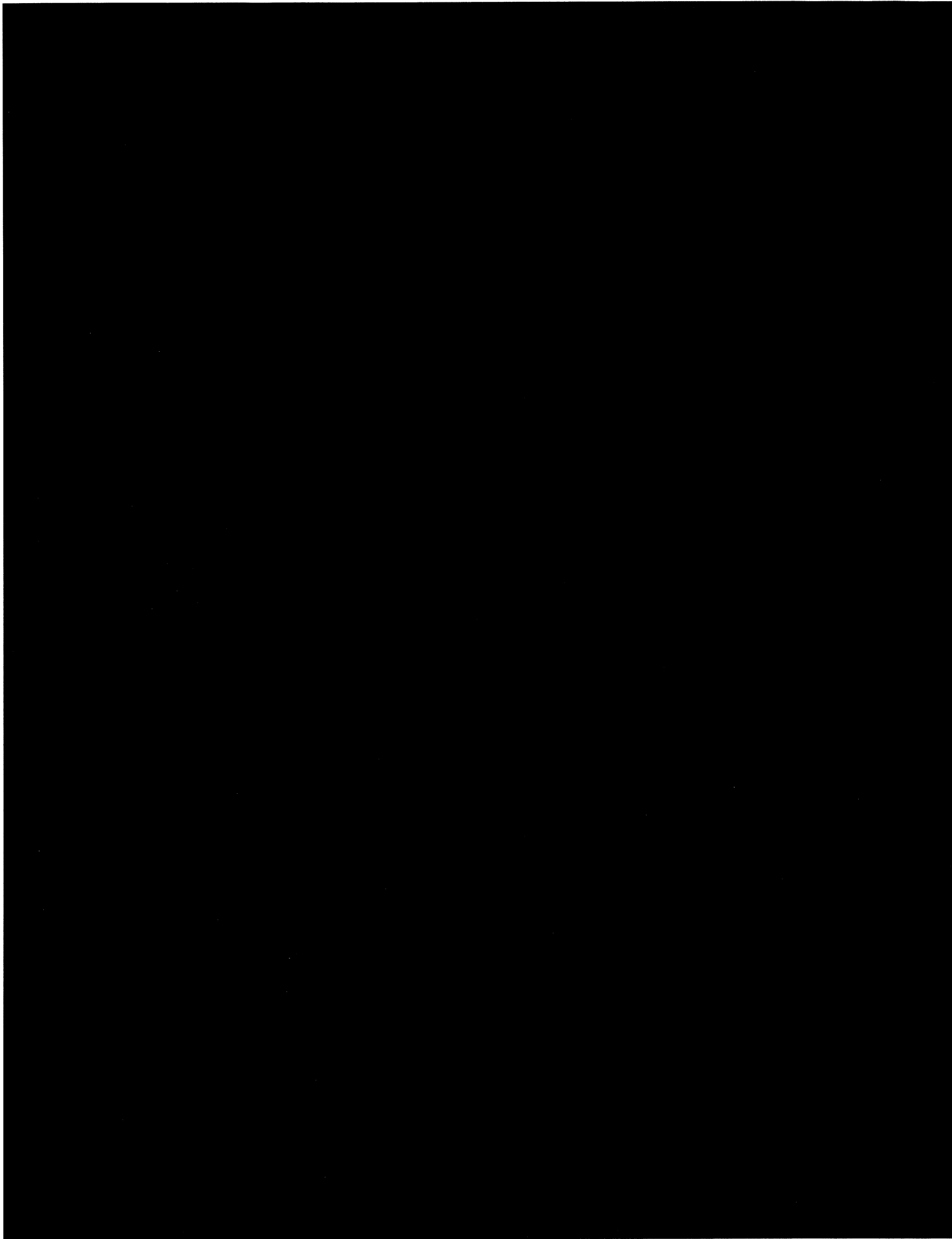


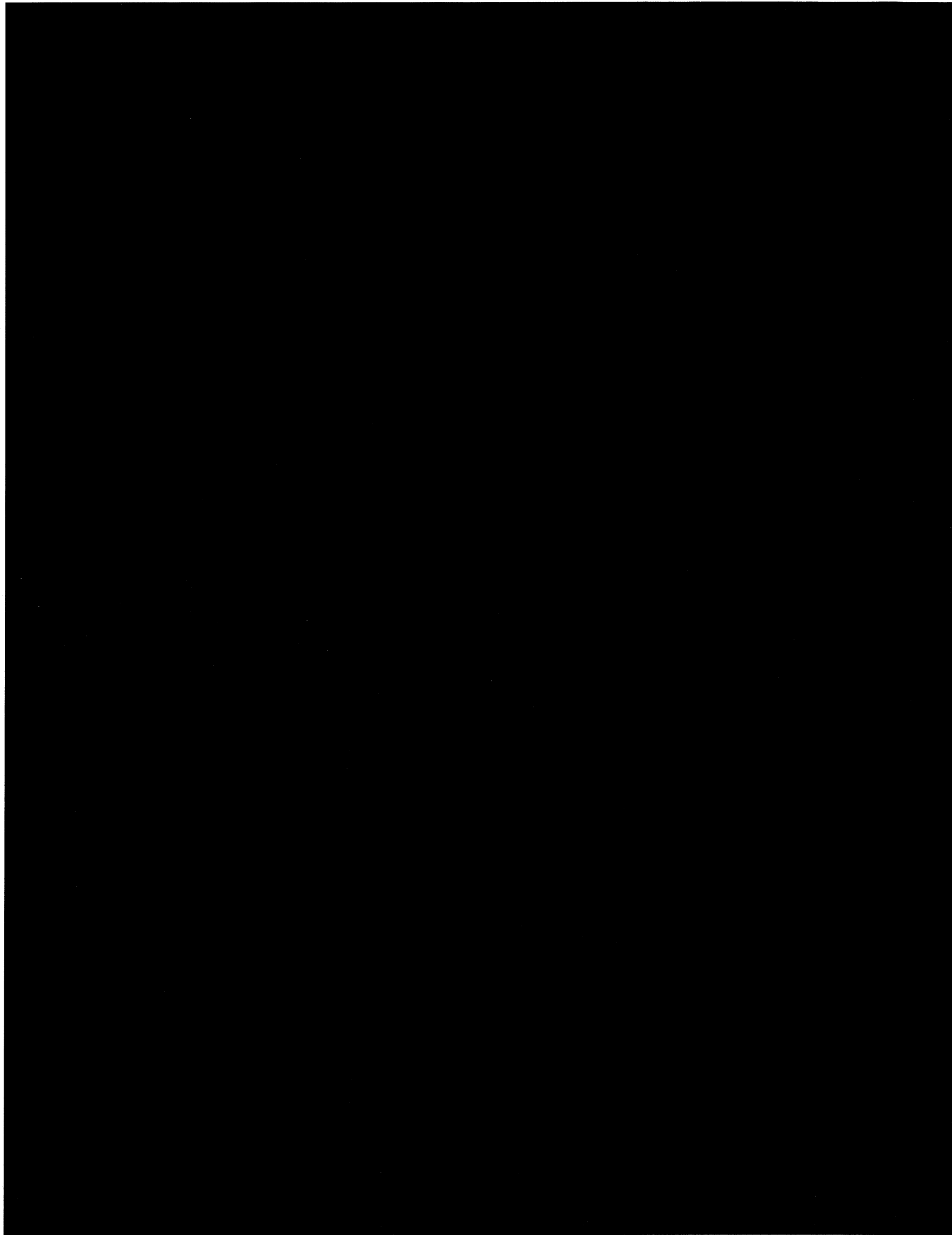


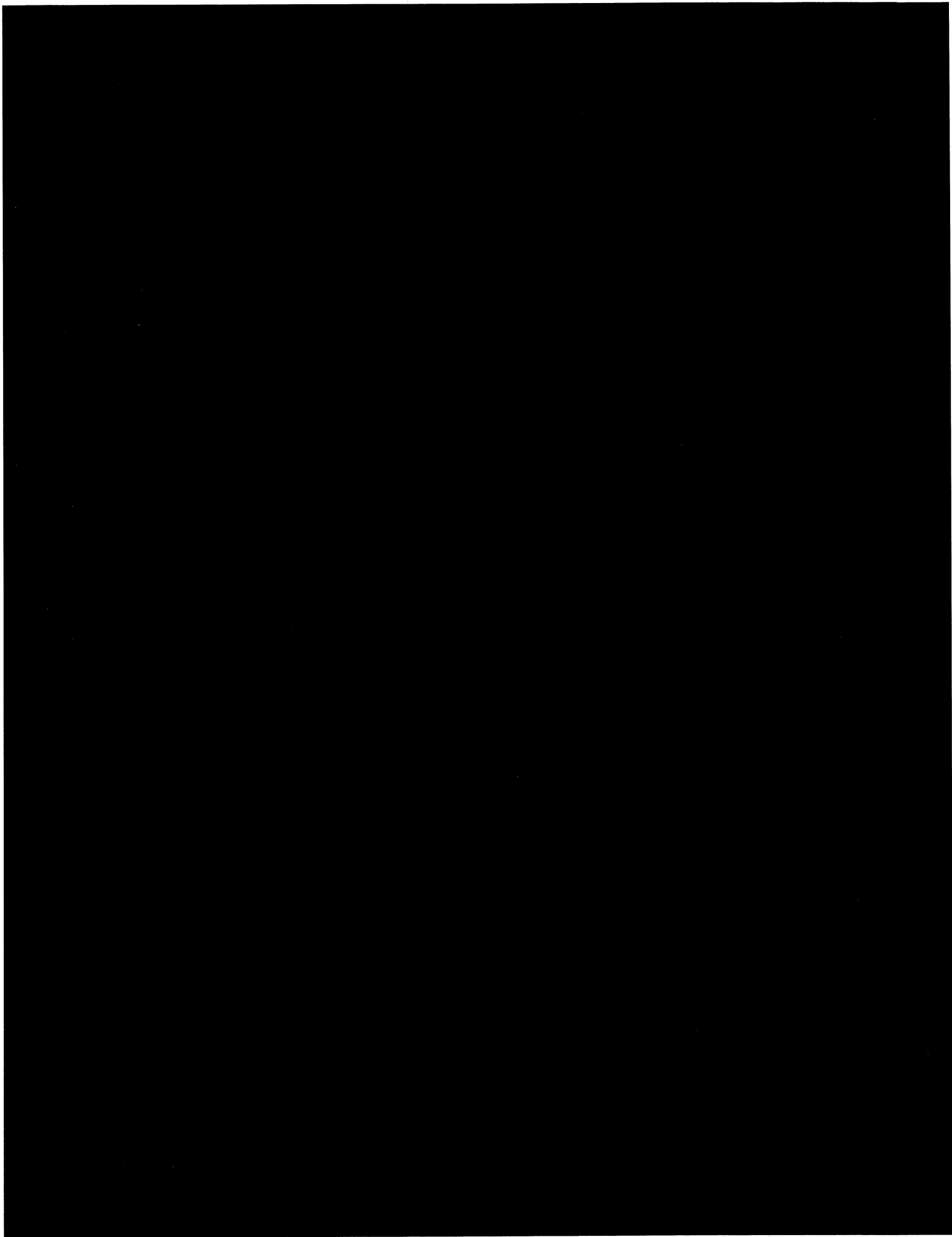


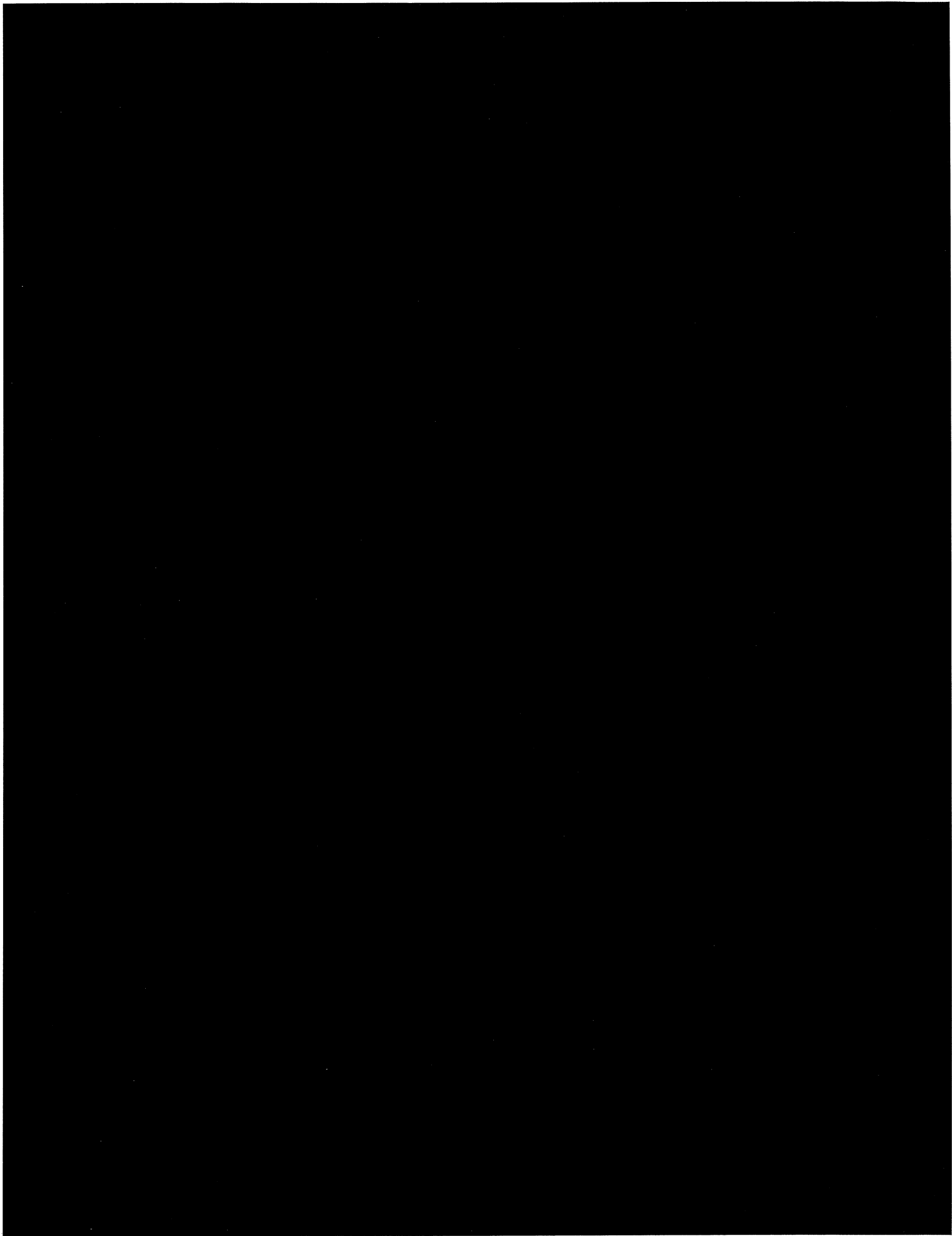
\_\_\_\_\_











~~SECRET//ORCON/NOFORN~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

U.S. DISTRICT COURT  
SURVEILLANCE COURT  
2011 OCT 31 PM 5:10  
LEEANN FLYNN HALL  
CLERK OF COURT

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED] (S)

UNDER SEAL

Docket No. [REDACTED]

GOVERNMENT'S EX PARTE SUBMISSION OF AMENDMENT  
TO DNI/AG 702(g) CERTIFICATION [REDACTED] AND EX PARTE SUBMISSION OF  
AMENDED MINIMIZATION PROCEDURES (S)

In accordance with subsection 702(i)(1)(C) of the Foreign Intelligence  
Surveillance Act of 1978, as amended ("the Act"), the United States of America, by and  
through the undersigned Department of Justice attorney, hereby submits ex parte the  
attached Amendment to DNI/AG 702(g) Certification [REDACTED]. Attached as Exhibit B to  
this Amendment to DNI/AG 702(g) Certification [REDACTED] are the amended minimization  
procedures to be used under the certification. (S//OC/NF)

DNI/AG 702(g) Certification [REDACTED] as amended, contains all of the elements  
required by the Act, and the minimization procedures to be used under the certification,  
as amended, are consistent with the requirements of the Act and the Fourth  
Amendment to the Constitution of the United States. Accordingly, the Government

~~SECRET//ORCON/NOFORN~~

Classified by: Lisa O. Monaco, Assistant Attorney  
General, NSD, DOJ  
Reason: 1.4 (c)  
Declassify on: 31 October 2036



~~SECRET//ORCON/NOFORN~~

respectfully requests that this Court enter an order pursuant to subsection 702(i)(3)(A) of the Act approving DNI/AG 702(g) Certification [REDACTED] as amended, and the use of the minimization procedures attached as Exhibit B to the Amendment to DNI/AG Certification [REDACTED] (S//OC/NF) —

Respectfully submitted,

[REDACTED]

National Security Division  
United States Department of Justice

~~SECRET//ORCON/NOFORN~~

~~SECRET~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED]

Docket No. [REDACTED]

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, "contains all the required elements" and that the revised minimization procedures submitted with the amendment "are consistent with the requirements of [Section 1881a(e)] and with the fourth amendment to Constitution of the United States."

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such amendment and the use of such procedures are approved.

Entered this \_\_\_\_ day of November 2011, at \_\_\_\_\_ Eastern Time.

\_\_\_\_\_  
JOHN D. BATES  
Judge, United States Foreign  
Intelligence Surveillance Court

~~SECRET~~

Derived From: ~~Submission to the USFISC  
in Docket Number captioned above~~

~~SECRET//ORCON/NOFORN~~

**CERTIFICATION OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND THE  
ATTORNEY GENERAL PURSUANT TO SUBSECTION 702(g) OF THE FOREIGN  
INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED**

NOV 31 PM 5:10

**Amendment to DNI/AG 702(g) Certification**

On April 13, 2011, based on supporting affidavits, the Director of National Intelligence and the Attorney General executed in writing and under oath DNI/AG 702(g) Certification pursuant to subsection 702(g) of the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA" or "the Act"), thereby authorizing the targeting of non-United States persons reasonably believed to be outside the United States to acquire foreign intelligence information. Specifically, the Director of National Intelligence and the Attorney General certified that:

- (1) there are procedures in place that had been approved or would be submitted with the certification for approval by the Foreign Intelligence Surveillance Court ("FISC")<sup>1</sup> that are reasonably designed to --
  - a. ensure that an acquisition authorized pursuant to subsection 702(a) of the Act is limited to targeting persons reasonably believed to be located outside the United States; and
  - b. prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States;

<sup>1</sup> Specifically, the targeting procedures to be used by the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) were submitted as Exhibits A and C, respectively, to the certification. ~~(S//OC/NF)~~

~~SECRET//ORCON/NOFORN~~

Classified by: The Attorney General  
Reason: 1.4(c)  
Declassify on: 31 October 2035

~~SECRET//ORCON/NOFORN~~

- (2) the minimization procedures with respect to such acquisition --
  - a. meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act; and
  - b. had been approved or would be submitted with the certification for approval by the FISC;<sup>2</sup>
- (3) guidelines have been adopted in accordance with subsection 702(f) of the Act to ensure compliance with the limitations in subsection 702(b) of the Act and to ensure that an application for a court order is filed as required by the Act;
- (4) the procedures and guidelines referred to in sub-paragraphs (1), (2), and (3) above are consistent with the requirements of the Fourth Amendment to the Constitution of the United States;
- (5) a significant purpose of the acquisition is to obtain foreign intelligence information;
- (6) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
- (7) the acquisition complies with the limitations in subsection 702(b) of the Act.

DNI/AG 702(g) Certification [REDACTED] including supporting affidavits and targeting and minimization procedures, was submitted to the FISC for review on April 22, 2011. ~~(S//OC/NF)~~

In accordance with subsection 702(i)(1)(C) of the Act, DNI/AG 702(g) Certification

[REDACTED] is hereby amended. Specifically, the use of the NSA minimization procedures attached

<sup>2</sup> Specifically, the minimization procedures to be used by the NSA, FBI, and Central Intelligence Agency (CIA) were submitted as Exhibits B, D, and E, respectively, to the certification. ~~(S//OC/NF)~~

~~SECRET//ORCON/NOFORN~~

~~SECRET//ORCON/NOFORN~~

hereto as Exhibit B under DNI/AG 702(g) Certification [REDACTED] is authorized. These minimization procedures --

- a. meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act; and
- b. will be submitted with this certification for approval by the FISC.

~~(S//OC/NF)~~

These minimization procedures are consistent with the requirements of the Fourth Amendment to the Constitution of the United States. ~~(S//OC/NF)~~

This authorization, as amended, shall be effective immediately. All other aspects of DNI/AG 702(g) Certification [REDACTED] remain unaltered and are incorporated herein. ~~(S//OC/NF)~~

*---- The remainder of this page intentionally left blank ----*

~~SECRET//ORCON/NOFORN~~



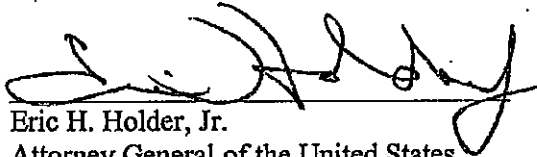
~~SECRET//ORCON/NOFORN~~

VERIFICATION (U)

I declare under penalty of perjury that the facts set forth in the foregoing amendment [REDACTED]

[REDACTED]

[REDACTED] DNI/AG 702(g) Certification [REDACTED] are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746 on October 31, 2011. ~~(S)~~

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

~~SECRET//ORCON/NOFORN~~


~~SECRET//ORCON,NOFORN~~

**VERIFICATION (U)**

I declare under penalty of perjury that the facts set forth in the foregoing amendment [REDACTED]

[REDACTED]

[REDACTED] DNI/AG 702(g) Certification [REDACTED] are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746 on October 31, 2011. ~~(S)~~

  
James R. Clapper  
Director of National Intelligence

~~SECRET//ORCON,NOFORN~~

~~TOP SECRET//COMINT//NOFORN//20320108~~**EXHIBIT B**U.S. FEDERAL  
INTELLIGENCE  
SURVEILLANCE COURT**MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN  
CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE  
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE  
SURVEILLANCE ACT OF 1978, AS AMENDED**2011 OCT 31 PM 5:10  
FEDERAL JUDICIAL  
CLERK OF COURT**Section 1 - Applicability and Scope (U)**

These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). (U)

If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity. (U)

For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). (U)

**Section 2 - Definitions (U)**

In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

- (a) Acquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party. (U)
- (b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. (U)
- (c) Communications of a United States person include all communications to which a United States person is a party. (U)

~~Derived From: NSA/CSSM 1-52~~~~Dated: 20070108~~~~Declassify On: 20320108~~~~TOP SECRET//COMINT//NOFORN//20310108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)
- (e) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications. ~~(S//SI)~~
- (f) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S//SI)~~
- (g) Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [REDACTED] or multiple discrete communications [REDACTED] ~~(TS//SI)~~
- (h) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)
- (i) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)
- (j) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S//SI)~~
- (k) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)
- (1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person. (U)
- (2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

- (3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with 8 U.S.C. § 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)
- (4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

### Section 3 - Acquisition and Processing - General (U)

#### (a) Acquisition (U)

The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition. ~~(S//SI)~~

#### (b) Monitoring, Recording, and Processing (U)

- (1) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Except as provided for in subsection 3(c)(2) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. ~~(S//SI)~~
- (2) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, 6, and 8 of these procedures. (C)

~~TOP SECRET//COMINT//NOFORN//20320108~~



~~TOP SECRET//COMINT//NOFORN//20310108~~

(3) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S)~~

(4) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5, 6, and 8 of these procedures.

~~(S//SI)~~

(5) Processing of Internet Transactions Acquired Through NSA Upstream Collection Techniques ~~(TS//SI)~~

a. Notwithstanding any processing [REDACTED] that may be required to render an Internet transaction intelligible to analysts, NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown. ~~(TS//SI)~~

1. Internet transactions that are identified and segregated pursuant to subsection 3(b)(5)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States. ~~(TS//SI)~~

(a) Any information contained in a segregated Internet transaction (including metadata) may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection 3(b)(5)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be destroyed upon recognition. ~~(TS//SI)~~

(b) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be processed in accordance with subsection 3(b)(5)b. below and handled in accordance the other applicable provisions of these procedures. ~~(TS//SI)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (c) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(5)a.
- 2. Internet transactions that are not identified and segregated pursuant to subsection 3(b)(5)a. will be processed in accordance with subsection 3(b)(5)b. below and handled in accordance with the other applicable provisions of these procedures.
- b. NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information. ~~(TS//SI)~~
  - 1. If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. ~~(TS//SI)~~
  - 2. If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information. ~~(TS//SI)~~
    - (a) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures. ~~(TS//SI)~~
    - (b) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be treated in accordance with the applicable provisions of these procedures. ~~(TS//SI)~~
    - (c) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use.

~~(TS//SI)~~

3. An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(5)b.1. and 2. above.

~~(TS//SI)~~

4. Notwithstanding subsection 3(b)(5)b. above, NSA may use metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(5)a. without first assessing whether the metadata was extracted from: a) a discrete communication as to which the sender and all intended recipients are located in the United States; or b) a discrete communication to, from, or about a tasked selector. Any metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(5)a. will be handled in accordance with the applicable provisions of these procedures. Any metadata extracted from an Internet transaction subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located inside the United States shall be destroyed upon recognition. ~~(TS//SI)~~

- (6) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph. ~~(S//SI)~~

- (7) Further processing, retention and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below. ~~(S//SI)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

(c) Destruction of Raw Data ~~(C)~~

- (1) Telephony communications, Internet communications acquired [REDACTED] from Internet Service Providers, and other discrete forms of information (including that reduced to graphic or "hard copy" form such as [REDACTED] that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition, and may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. ~~(S//SI)~~
- (2) Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. All Internet transactions may be retained no longer than two years from the expiration date of the certification authorizing the collection in any event. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and processed only in accordance with the standards set forth in subsection 3(b)(5) of these procedures. ~~(TS//SI)~~

(d) Change in Target's Location or Status ~~(S//SI)~~

- (1) In the event that NSA determines that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person is in fact a United States person, the acquisition from that person will be terminated without delay. ~~(S//SI)~~
- (2) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person, will be treated as domestic communications under these procedures. ~~(S//SI)~~

Section 4 - Acquisition and Processing - Attorney-Client Communications ~~(C)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed disseminations of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination. ~~(S//SI)~~

#### Section 5 - Domestic Communications (U)

A communication identified as a domestic communication will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that: ~~(S)~~

- (1) the communication is reasonably believed to contain significant foreign intelligence information. Such communication may be provided to the FBI (including United States person identities) for possible dissemination by the FBI in accordance with its minimization procedures; ~~(S)~~
- (2) the communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such communications may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes; ~~(S)~~
- (3) the communication is reasonably believed to contain technical data base information, as defined in Section 2(i), or information necessary to understand or assess a communications security vulnerability. Such communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such communications may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. ~~(S//SI)~~
  - a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S//SI)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signal Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or ~~(S//SI)~~

- (4) the communication contains information pertaining to a threat of serious harm to life or property. ~~(S)~~

Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may advise the FBI of that fact. Moreover, technical data regarding domestic communications may be retained and provided to the FBI and CIA for collection avoidance purposes. ~~(S//SI)~~

#### Section 6 - Foreign Communications of or Concerning United States Persons (U)

##### (a) Retention (U)

Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

- (1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

- a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

- b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signals Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

- (2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

- (3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. ~~(S//SI)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~



~~TOP SECRET//COMINT//NOFORN//20310108~~

## (b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 or 8 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

- (1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;
- (2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;
- (3) the communication or information indicates that the United States person may be:
  - a. an agent of a foreign power;
  - b. a foreign power as defined in Section 101(a) of the Act;
  - c. residing outside the United States and holding an official position in the government or military forces of a foreign power;
  - d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
  - e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;
- (4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;
- (5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications security vulnerability, but only after the agency that originated the information certifies that it is properly classified;
- (6) the communication or information indicates that the United States person may be engaging in international terrorist activities;

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or
  - (8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. (U)
- (c) Provision of Unminimized Communications to CIA and FBI ~~(S//NF)~~
- (1) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI//NF)~~
  - (2) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will process any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI)~~

#### Section 7 - Other Foreign Communications (U)

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy. (U)

#### Section 8 - Collaboration with Foreign Governments ~~(S//SI)~~

- (a) Procedures for the dissemination of evaluated and minimized information. Pursuant to Section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with subsections 6(b) and 7 of these NSA minimization procedures. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

(b) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated: ~~(S)~~

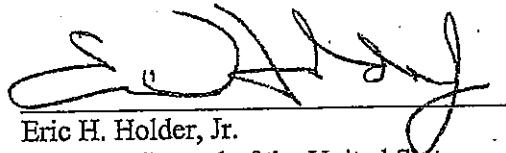
- (1) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA. ~~(S)~~
- (2) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data. ~~(S)~~
- (3) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA. ~~(S)~~
- (4) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (5) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures. ~~(S)~~

10-31-11  
Date

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

~~TOP SECRET//COMINT//NOFORN//20320108~~

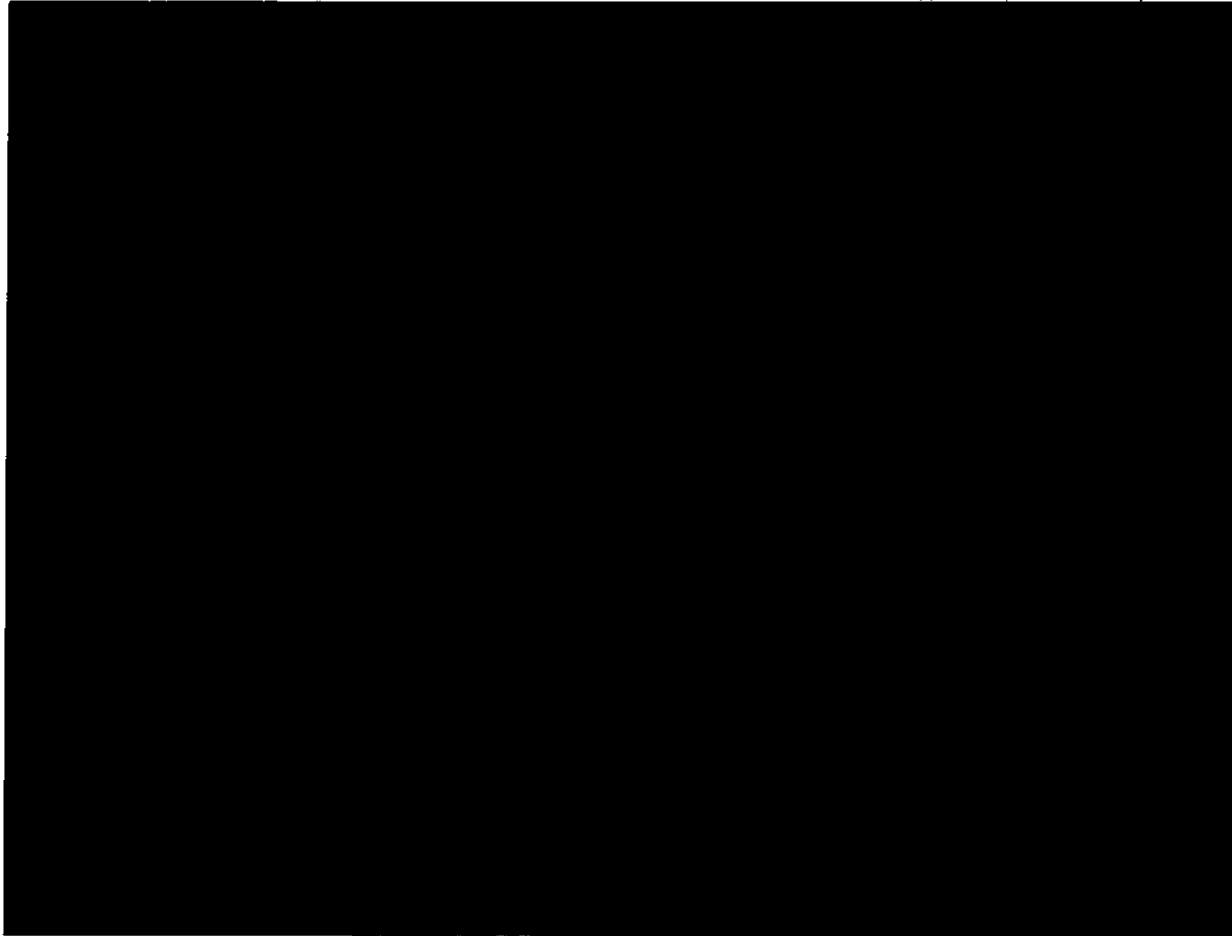
~~TOP SECRET//COMINT//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

2011 NOV 22 PM 5:28  
LEAHY FLYNN HALL



GOVERNMENT'S RESPONSE TO THE COURT'S  
BRIEFING ORDER OF OCTOBER 13, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of  
Justice attorney, respectfully submits the following response to the Court's Briefing

Order of October 13, 2011. ~~(S//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: 22 November 2036

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The Court's Briefing Order of October 13, 2011, in the above-captioned matters (hereinafter "October 13 Briefing Order") enumerated six issues to be addressed by the Government. Items 1. and 2. in the October 13 Briefing Order are addressed together starting on page 3 below; responses for items 3. through 6. begin on page 39. (S)

As an initial matter, as this Court is aware, amended section 702 minimization procedures for the National Security Agency (NSA) were adopted by the Attorney General and approved by the Attorney General and Director of National Intelligence for immediate use on October 31, 2011; that same day the procedures were submitted to the Court for review. NSA's amended section 702 minimization procedures provide, *inter alia*, that "[a]ll Internet transactions may be retained no longer than two years from the expiration date of the certification authorizing the collection in any event." *See, e.g.,* Amendment to DNI/AG 702(g) Certification [REDACTED] Ex. B, filed Oct. 31, 2011, § 3(c)(2) (hereinafter "2011 Amended NSA Minimization Procedures"). In the past, NSA has tried to maintain consistency of its minimization procedures across acquisitions pursuant to multiple certifications. NSA is unable to apply in full the 2011 Amended NSA Minimization Procedures to information acquired prior to October 31, 2011, for technical reasons primarily related to its inability to segregate certain previously collected categories of information in accordance with section 3(b)(5)a, of the amended

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

procedures.<sup>1</sup> Nevertheless, in furtherance of maintaining consistency across data acquired through its upstream collections, and as described in greater detail below, NSA is taking steps to age off of its systems Internet transactions that were collected through its upstream collection platforms pursuant to Docket Nos. [REDACTED] the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007) (hereinafter PAA), and certifications issued under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801, *et seq.* (hereinafter FISA or "the Act") where such authorizations expired more than two years ago. NSA anticipates that it will complete this age-off process no earlier than March 2012. ~~(TS//SI//NF)~~

1. An analysis of the application of Section 1809(a) to each of the three different statutory schemes under which Internet transactions were acquired without the Court's knowledge. ~~(TS//SI//NF)~~
2. The extent to which information acquired under Section 1881a, the PAA, and Docket Nos. [REDACTED] falls within the criminal prohibitions set forth in Section 1809(a). ~~(S)~~

The Government responds to these two items as follows: ~~(S)~~

---

<sup>1</sup> It is for this reason that NSA has not sought to amend prior certifications to permit the use of the 2011 Amended NSA Minimization Procedures to information acquired under those certifications. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

I. The Application of Section 1809 to the Government's Acquisitions Pursuant to Section 1881a, the PAA, and Docket Nos. [REDACTED] (S)

A. Section 1809 is a Criminal Statute Designed to Address Intentional Violations of the Law (S)

As acknowledged earlier this year, the Government concluded that its prior representations to the Court regarding the steps NSA must take in order to acquire single, discrete communications to, from, or about a tasked selector did not fully explain all of the means by which such communications are acquired through NSA's upstream collection techniques. The Government submits that that oversight, although regrettable, does not support a finding that the Government intentionally engaged in unauthorized electronic surveillance, thus implicating a criminal statute. Section 1809 by its terms imposes criminal sanctions (including imprisonment and a substantial fine) on an individual who intentionally engages in unauthorized electronic surveillance or uses or discloses the fruits of unauthorized electronic surveillance.<sup>2</sup> Congress did not intend these stringent penalties to apply to intelligence professionals who, in good faith, reasonably believed that they were acquiring foreign intelligence information in conformity with authorizations by this Court or by the Attorney General and Director of National Intelligence. ~~(TS//SI//NF)~~

Section 1809(a) criminalizes "intentionally (1) engag[ing] in electronic surveillance under color of law, except as authorized by [statute] . . . ; or (2) disclos[ing]

---

<sup>2</sup> Section 1810 of FISA exposes an individual who violates section 1809 to substantial civil penalties. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

or us[ing] information obtained under of color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by [statute]." 50 U.S.C. § 1809(a). Section 1809 provides a complete defense for law enforcement and investigative officers engaged in official surveillance "authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction." *Id.* § 1809(b). Accordingly, by its terms section 1809(a) is violated only where there is intentional conduct and unauthorized electronic surveillance is involved. ~~(S)~~

FISA's inclusion of criminal sanctions reflects a balance between competing priorities. On the one hand, the threat of criminal sanctions reinforces FISA's central edict: before engaging in electronic surveillance, Government agents must obtain the necessary statutory authorization -- typically (though not always) by securing advance judicial approval. On the other, those agents who in good faith obtain and effectuate authorization under the FISA framework are thereby shielded from civil and criminal liability. FISA's proponents stressed that far from chilling lawful intelligence collection, the bill's clear delineation of the scope of criminal liability actually serves to *protect* law-abiding Government agents:

[I]ndividual intelligence agents will know to the letter what is required of them. They will know that what they do pursuant to a warrant is lawful. And they will be protected in the future against criminal prosecutions and civil suits arising from the surveillance as long as they do not exceed their lawful authority.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

*Foreign Intelligence Surveillance Act: Hearing on H.R. 7308 Before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice, House Committee on the Judiciary, 95th Cong. 111 (1978) (statement of Rep. Mazzoli).* To that end, "[t]he word 'intentionally' was carefully chosen. It [was] intended to reflect the most strict standard for criminal culpability. . . . The Government would have to prove beyond a reasonable doubt that the . . . [conduct] was engaged in with a conscious objective or desire to commit a violation." H.R. Rep. No. 95-1283, pt. 1, at 97 (1978) (quotation omitted). In other words, "intentionally" in the context of section 1809 means not only that an individual intentionally undertook electronic surveillance, but undertook electronic surveillance with the knowledge and intention to violate the requirements of FISA. As noted in the Government's Response to the Court's Briefing Order of May 9, 2011, "[b]ased upon discussions between responsible NSA officials and the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) and DOJ and ODNI's review of documents related to this matter, DOJ and ODNI have not found any indication that there was a conscious objective or desire to violate the authorizations here." Government's Response to the Court's Briefing Order of May 9, 2011, Docket Nos. [REDACTED], filed June 1, 2011, at 32 n.27 (hereinafter "June 1 Submission"). In addition, DOJ and ODNI have not found any indication of a conscious objective or desire to violate the authorizations under the PAA or Docket Nos. [REDACTED] (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The enacted version of section 1809 contrasts markedly with a criminal-sanctions provision in a draft bill that would have swept more broadly. The earlier proposal would, among other things, have criminalized intentionally "violat[ing] ... any court order pursuant to this title." H.R. Rep. No. 95-1283, pt. 1, at 96-97 (discussing predecessor bill). Criminalizing all manner of FISA violations "generated considerable debate" and was suggested to have a "deleterious effect on the morale of intelligence personnel." *Id.* at 96. The "any order" language was ultimately stricken from the final bill enacted by Congress. In limiting FISA's criminal penalties to instances in which the Government had failed to obtain prior authorization or intentionally exceeded the boundaries of the authorization obtained, Congress made clear that it envisioned section 1809 as a narrowly tailored sanction, not a comprehensive framework for remedying all manner of Government errors in the course of obtaining or effectuating FISA authorities. ~~(S)~~

Given its underlying purpose, the Government respectfully suggests that section 1809 does not provide the appropriate framework for cases in which the "surveillance, though based on an erroneous factual premise, was authorized by and conducted pursuant to an order issued by the FISC." Note, *The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability under FISA*, 61 U. Miami L. Rev. 393, 427 (2007) (arguing that although this limitation of section 1809 was "appropriate for criminal liability," FISA should be amended to provide civil liability in such circumstances). So

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

understood, section 1809 accords with other criminal offenses that hinge on the absence of valid authorization. For example, in *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004), the Ninth Circuit construed "the meaning of the word 'authorized' in section 2701" of the Stored Communications Act (SCA), 18 U.S.C. § 2702. The defendant in *Theofel* had obtained access to communications by serving a "patently unlawful" subpoena on a third party. *Id.* At issue was whether compliance with that flawed subpoena constituted valid consent -- i.e., qualified as an "authorized" disclosure under the SCA. (S)

Holding that the answer depended on whether the authorization was procured in "bad faith," the Court of Appeals explained:

Because the Stored Communications Act defines a criminal offense and includes an explicit *mens rea* requirement, see 18 U.S.C. § 2701(a)(1), we do not think a defendant can be charged with constructive knowledge [of the authorization's invalidity] on a showing of mere negligence. Rather, the defendant must have consciously procured consent [i.e., "authorization"] through improper means. In this case, the magistrate found that defendants had acted in bad faith. That is enough to charge them with knowledge of [the third party's] mistake. See Black's Law Dictionary 139 (6th ed. 1990) (defining "bad faith" as "not simply bad judgment or negligence, but . . . conscious doing of a wrong because of dishonest purpose or moral obliquity").

*Id.* at 1074 n.2. In addition to recounting the defendant's "bad faith" and "constructive knowledge" of the subpoena's invalidity, the decision stressed that "[a]llowing consent procured by a known mistake to qualify as a defense would seriously impair the statute's operation." *Id.* at 1074. However, for the reasons discussed herein, the

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Government submits that the orders of the Court in the four authorities at issue here were not "procured by a known mistake." ~~(S)~~

The Government submits that the same considerations exclude from criminal liability under section 1809 instances in which judicial approval and authorization of the Director of National Intelligence and the Attorney General were obtained in good faith, premised on incomplete descriptions of how the acquisitions were to be conducted. ~~(TS//SI//NF)~~

B. The Authorizations Remain Valid Despite the Government's Incomplete Description of the Technical Means of Acquisition ~~(S)~~

Congress intended that the "criminal penalties for intelligence agents under [FISA] should be essentially the same as for law enforcement officers under title 18." H.R. Conf. Rep. No. 95-1720, at 33 (1978). Therefore, the law-enforcement context provides instructive guidance with respect to the scope of what should qualify as intentional unauthorized surveillance for purposes of section 1809(a)(1). Provided it was obtained in good faith, a valid authorization to conduct law-enforcement surveillance is not rendered "void" or "invalid" because it was premised on a factual error or misstatement. ~~(S)~~

Under case law developed in the suppression context, it has long been settled that the Government's "[i]nnocent mistakes or negligence alone are insufficient to void a warrant." *United States v. Palega*, 556 F.3d 709, 714 (8th Cir. 2009) (citing *Franks v.*

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

*Delaware*, 438 U.S. 154, 171) (1978)).<sup>3</sup> Recognizing that everyone -- including the agents who serve the Government -- will at times commit errors, the Supreme Court has emphasized, in a variety of circumstances, "the need to allow some latitude for honest mistakes." *Maryland v. Garrison*, 480 U.S. 79, 87 (1987); *see also Brinegar v. United States*, 338 U.S. 160, 176 (1949) (emphasizing that "room must be allowed for some mistakes on [the Government's] part"). ~~(S)~~

In the three decades since *Franks*, it has become hornbook law that a discovery of a good faith misstatement or omission<sup>4</sup> in the application for a warrant -- even one that is material -- does not transform an authorized search into an unauthorized one. *See e.g., Chism v. Washington State*, No. 10-35085, \_\_\_ F.3d \_\_\_, 2011 WL 5304125, at \*16 (9th Cir. Nov. 7, 2011) ("It is well established that omissions and misstatements resulting from negligence or good faith mistakes will not invalidate an affidavit which on its face

---

<sup>3</sup> The decision in *Franks* came down in June 1978, just prior to FISA's enactment. But the core holding of *Franks* was anticipated by many courts. *See, e.g., United States v. Marihart*, 492 F.2d 897, 900 n.4 (8th Cir. 1974) ("We agree with the Seventh Circuit that completely innocent misrepresentation should not support suppression even if material."). The Second Circuit has suggested that "FISA orders should be governed by the principles set forth in *Franks v. Delaware*." *United States v. Duggan*, 743 F.2d 59, 77 n.6 (2d Cir. 1984). Under the Second Circuit's standard, the fact of a negligent misstatement in a FISA application is not grounds for suppression -- or even an evidentiary hearing -- on the issue of whether the surveillance was properly authorized. To warrant a hearing, the court explained, a suppression motion asserting that the Government's surveillance was not authorized by FISA "would be required to make 'a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA judge's approval of the application." *Id.* (quoting *Franks*, 438 U.S., at 155-156). ~~(S)~~

<sup>4</sup> Although *Franks* itself was concerned with the issue of Government misstatements, it is widely accepted that its "reasoning . . . logically extends . . . to material omissions." *United States v. Johnson*, 696 F.2d 115, 118 n.21 (D.C. Cir. 1982) (quoting 2 W. LaFare, Search and Seizure, § 4.4 (Supp. 1982)). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

establishes probable cause.") (quotation omitted); *United States v. Andrews*, 577 F.3d 231, 238-39 (4th Cir. 2009) ("In challenging a search warrant on the theory that the officer's affidavit omitted material facts with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading, the defendant must show (1) that the officer deliberately or recklessly omitted the information at issue and (2) that the inclusion of this information would have defeated probable cause.") (quotation and citation omitted). The appropriate inquiry looks to the Government's good faith in submitting the application, and the fact that an error may be attributable to an internal miscommunication within the Government, or to gaps in the Government's understanding, is not itself an indication of bad faith. See, e.g., *United States v. Yusuf*, 461 F.3d 374, 378 (3d Cir. 2006) (in performing the *Franks* analysis, lower court "erred by failing to recognize that government agents should generally be able to presume that information received from a sister governmental agency is accurate"); *United States v. Radtke*, 799 F.2d 298, 310 (7th Cir. 1986) (finding no "deliberate falsehood" where a police officer of one department compiled erroneous information derived from another department's investigation).<sup>5</sup> ~~(S)~~

---

<sup>5</sup> The case law "hold[s] the government accountable for statements made . . . by the affiant [and] statements made by other government employees which were deliberately or recklessly false or misleading insofar as such statements were relied upon by the affiant in making the affidavit." *United States v. Kennedy*, 131 F.3d 1371, 1376 (10th Cir. 1997). See also *United States v. Hammett*, 236 F.3d 1054, 1058-1059 (9th Cir. 2001) ("In informing Detective Bolos of the information necessary to procure the warrant, it is highly probable that there was a miscommunication between Officer Correia and Detective Bolos that led to the misstatement in the affidavit. We therefore reject the position that the warrant is invalid . . ."); *United States v. Wapnick*, 60 F.3d 948, 956 (2d Cir. 1995) (invalidation turns on whether

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The *Franks* framework has been extended to mistakes in Title III applications. As Judge Posner has explained:

[I]f government agents execute a valid wiretap order and in the course of executing it discover it was procured by a mistake . . . the record of the conversations is admissible in evidence . . . . The discovery of the mistake does not make the search unlawful from its inception.

*United States v. Ramirez*, 112 F.3d 849, 851 (7th Cir. 1997); see also *United States v. Garcia*, 785 F.2d 214, 222 (8th Cir. 1986) (applying *Franks* standard to a Title III wiretap); *United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985) (same); *United States v. Southard*, 700 F.2d 1, 8 (1st Cir. 1983) (same). ~~(S)~~

Although the Government has not located cases applying the *Franks* standard to illegal wiretapping prosecutions (presumably because cases raising that fact pattern are rarely, if ever, prosecuted), *Franks* also delineates the scope of an "illegal search" in civil litigation under 42 U.S.C. § 1983. See, e.g., *Peet v. City of Detroit*, 502 F.3d 557, 570 (6th Cir. 2007) ("In cases involving search warrants . . . the law is clear that an officer may be held liable under 42 U.S.C. § 1983 for an illegal search . . . when the officer 'knowingly and deliberately, or with a reckless disregard for the truth' makes 'false statements or omissions that create a falsehood' and 'such statements or omissions are material, or necessary, to the finding of probable cause.'") (citing *Wilson v. Russo*, 212 F.3d 781, 786-787 (3d Cir. 2000)). When it enacted section 1809, Congress surely did not intend to

---

anyone in the government "*deliberately insulat[ed]* affiants from information material to the determination of probable cause") (emphasis added); *United States v. Calisto*, 838 F.2d 711, 714 (3d Cir. 1988) (same). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

impose a less forgiving standard of *criminal liability* in the national security context than generally exists for *civil liability* in the law-enforcement context. ~~(S)~~

The Government submits that the Court should consider the latitude afforded the Government in the law-enforcement context equally appropriate for surveillance conducted under the aegis of national security investigations, in which the Government's focus will often be "less precise . . . than [surveillance] directed against more conventional types of crime." *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972). All of which is not to suggest that the Government bears diminished responsibility for mistakes in the record. Upon becoming aware of its failure to communicate to the Court certain salient aspects of its collection activities, the Government bore responsibility for correcting its past statements. See FISC Rule 13(a). When mistakes happen notwithstanding the Government's best efforts, they are regrettable. Nevertheless, the Government respectfully submits that the potential exposure to *criminal liability* -- and the resultant civil liability under section 1810 -- is not the appropriate means to respond to such miscommunications within the Government. ~~(S)~~

C. The Authorities at Issue ~~(S)~~

1. Section 1881a ~~(S)~~

Beneath the heading "AUTHORIZATION," section 702 in pertinent part empowers the Attorney General and the Director of National Intelligence, upon the issuance of an

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

order from this Court approving a certification and the use of targeting and minimization procedures, to "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). Acquisitions authorized under section 702 must be conducted in accordance with targeting and minimization procedures adopted by the Attorney General and in conformity with a certification submitted to the FISC. *See* 50 U.S.C. § 1881a(c)(1). Accordingly, section 702 accords the Court a crucial role in ensuring that the Government's targeting and minimization procedures are consistent with the statutory requirements of section 702 and the Fourth Amendment to the Constitution of the United States. *See* 50 U.S.C. § 1881a(i) (providing that the FISC "shall have jurisdiction to review [the] certification . . . and the targeting and minimization procedures"). Nevertheless, while the Government cannot commence or continue acquisition without Court approval, the statute commits responsibility for "authorization" to the Attorney General and the Director of National Intelligence. ~~(TS//SI//NF)~~

Section 702 provides for two potential outcomes of judicial review, neither of which appears to vitiate a past determination of the Attorney General and Director of National Intelligence to authorize acquisitions in good faith. The first is "APPROVAL," in which event the Court "enter[s] an order approving the certification and the use . . . of the procedures for the acquisition." 50 U.S.C. § 1881a(i)(3)(A). The second is a

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

"CORRECTION OF DEFICIENCIES," in which event the Court "shall issue an order directing the Government to, at the Government's election . . . (i) correct any deficiency identified by the Court's order . . . ; or (ii) cease, or not begin, the implementation of the authorization for which such certification was submitted." 50 U.S.C. § 1881a(i)(3)(B). Notably, section 702 makes no provision for an order requiring the Government to purge information acquired under authorizations from the Attorney General and Director of National Intelligence in the event the Government chooses to discontinue its collection after receipt of a deficiency order.<sup>6</sup> ~~(S)~~

In keeping with the above, the operative certifications, and the targeting and minimization procedures adopted by the Attorney General for use with those certifications, were submitted by the Government to the FISC and approved pursuant to 50 U.S.C. § 1881a(i), albeit without provision of certain information relevant to the manner in which NSA acquires Internet transactions to, from, or about a tasked selector through its upstream collection. The Attorney General and Director of National Intelligence at all times acted in good faith in discharging their responsibilities under section 702. As the Court has already found, each prior certification contained all of the required statutory elements. *See In re DNI/AG 702(g) Certifications* [REDACTED]

---

<sup>6</sup> In this respect, section 702 appears to represent a departure from the "traditional" FISA framework, which expressly -- and significantly -- restricts the use of information acquired pursuant to surveillance activities authorized by the Attorney General without a court order and later rejected by the Court. *See, e.g.,* 50 U.S.C. § 1805(e)(5). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED], *et al.*, Docket Nos. [REDACTED] Memorandum Opinion at 12 & n.11 (USFISC Oct. 3, 2011) (hereinafter "Oct. 3 Mem. Op."). Moreover, as the Government noted in its June 1 Submission, the Attorney General and Director of National Intelligence have confirmed that their prior section 702 authorizations continued to be valid and in force, notwithstanding the acquisition of Internet transactions featuring multiple discrete communications (hereinafter "MCTs"). *See* June 1 Submission at 35; *see also* Government's Response to the Court's Supplemental Questions of June 17, 2011, Docket Nos. [REDACTED], filed June 28, 2011, at 26-27. Accordingly, the Government respectfully submits that personnel who relied on those authorizations and followed those procedures in acquiring MCTs did not engage in unauthorized surveillance, and did not *intend* to engage in surveillance that was not authorized under FISA. ~~(TS//SI//NF)~~

2. The PAA ~~(S)~~

Section 105B of the PAA likewise empowered the Director of National Intelligence and the Attorney General to "authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States." § 105B, 121 Stat. at 552-55. Such acquisitions were specifically exempted from FISA's definition of "electronic surveillance." *See id.* § 105A, 121 Stat. 552. As under section 702, the PAA provided for judicial review of the targeting procedures used to implement those authorizations, but the review was limited by statute. Under

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

the PAA, the Attorney General was required to submit to this Court "the procedures by which the Government determines that acquisitions conducted pursuant to [its statutory authority] do not constitute electronic surveillance." *Id.* § 105C(a), 121 Stat. at 555. The Court, in turn, was then required to assess whether the Government's determination was "clearly erroneous." *Id.* § 105C(b), 121 Stat. at 555. As this Court has noted, the deferential "clearly erroneous" standard of review would "not entitle a reviewing court to reverse the [Attorney General's] finding . . . simply because [ . . . ] it would have decided the case differently." *In re DNI/AG 105B Certifications* [REDACTED] [REDACTED] Mem. Op. at 6 (USFISC Jan. 15, 2008) (hereinafter "PAA Mem. Op.") (quoting *Anderson v. City of Bessemer City*, 470 U.S. 564, 573 (1985)). Moreover, judicial review was limited to "certain aspects of the certification process." *Id.* at 4. "Executive branch determinations . . . regarding the purpose of the acquisition and the adequacy of minimization procedures [were] not subject to judicial review" at all. *Id.* at 6.

(TS//SI//NF)

Applying the PAA's "clearly erroneous" standard of review, this Court found the Government's targeting procedures were "reasonably designed to ensure that the users of tasked facilities are reasonably believed to be located outside the United States." *Id.* at 15. As to "abouts" communications, the Court "adopt[ed] the [Government's] interpretation that . . . surveillance [of 'abouts' communications] is 'directed' (i) at the users of tasked e-mail accounts . . . ; (ii) at those parties to acquired communications

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

who . . . are reasonably believed to be outside the United States; or (iii) at both these classes of persons." *Id.* at 21. Just as in the section 702 context, Government personnel who relied on the PAA authorizations to acquire MCTs did not engage in unauthorized surveillance, let alone did so intentionally. ~~(TS//SI//NF)~~

3. FISA Title I-(S)

The issues concerning NSA's upstream collection techniques raised during the Court's consideration of the above-captioned dockets potentially implicate the applications approved by the Court in *In re* [REDACTED]

[REDACTED] Docket Nos. [REDACTED]. ~~(TS//SI//NF)~~

With respect to Docket No. [REDACTED] the Government sought, and the Court approved, "authorization to direct electronic surveillance" at [REDACTED] that the Government believed were being used, or were about to be used, by its targets to communicate. In its order approving the surveillance, the Court stated that it "underst[ood] that, in certain instances, NSA may collect non-target [internet] communications." *In re* [REDACTED]

[REDACTED], Docket No. [REDACTED] Mem. Op. at 9 n.9 (USFISC Apr. 6, 2007) (hereinafter [REDACTED] Mem. Op."), just as the Court understood that "[a]lthough NSA surveillance will be designed to acquire only international [telephone] communications where one communicant is outside the United States, . . .

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

the manner in which [NSA] routes communications do not permit complete assurance that this will be the case," *id.* at 7-8 n.7. The Court approved the collection with the expectation that NSA would "handle these communications in accordance with its standard FISA minimization procedures, as described and modified herein." *Id.* at 9 n.9; see also *id.* at 7-8 n.7. Accordingly, Government personnel who relied on that approval and acted in accordance with those procedures in no way engaged in unauthorized surveillance, and certainly did not do so with "a conscious and objective desire to commit a violation." H.R. Rep. No. 95-1283, pt. 1, at 97 (1978) (quotation omitted).

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

With respect to Docket No. [REDACTED] the Government acknowledges that its application did not fully explain the methodology through which [REDACTED] Internet communications upstream would "ensure that all communications forwarded to NSA . . . are indeed communications that have been sent or received using, and that 'refer to' or are 'about,' e-mail accounts/addresses/identifiers for which there is probable cause to believe are being used, or are about to be used, by [the targets.]" Decl. of Lt. Gen. Keith B. Alexander, Docket No. [REDACTED] filed May 23, 2007, at 21. But for the reasons discussed in greater detail above, this good faith mistake does not render the prior authorization void or the surveillance collected thereunder "unauthorized," thereby exposing Government personnel to potential criminal and civil liability. On the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

contrary, such good faith mistakes can and should be meaningfully redressed without recourse to section 1809. ~~(TS//SI//NF)~~

II. Should the Court Determine that Unauthorized Collection Occurred, Only the Acquisition of Certain Subsets of Communications Acquired Through NSA's Upstream Collections Conducted Pursuant to the Authorities at Issue Would Constitute Electronic Surveillance, as Defined by the Act ~~(S)~~

By its terms section 1809(a) applies only to unauthorized electronic surveillance as that term is defined in FISA. Thus, the extent to which section 1809(a) applies to acquisitions under the authorities at issue herein depends on whether or not those acquisitions constitute "electronic surveillance." ~~(S)~~

NSA's upstream Internet collections under all four authorities have acquired only communications [REDACTED]

[REDACTED] As such, any communication that NSA has acquired through its upstream Internet collections conducted pursuant to the four authorities at issue would be a "wire communication," as defined by the Act -- that is, a "communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." *Id.* § 1801(l). ~~(TS//SI//NF)~~

The Act defines "electronic surveillance" in four different ways. *See id.* § 1801(f).

Two of these four types of electronic surveillance on their face do not apply to NSA's upstream collections conducted pursuant to the authorities discussed in the Court's

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Briefing Order. The first type of electronic surveillance, which requires "intentionally targeting" a "particular, known United States person who is in the United States," *id.* § 1801(f)(1), is not implicated, because none of the authorities at issue here permitted the targeting of United States persons inside the United States.<sup>7</sup> Similarly, the third type of electronic surveillance, which involves the acquisition of the contents of certain radio communications, *see id.* § 1801(f)(3), is not implicated, [REDACTED]

[REDACTED] S)

For the reasons discussed below, the second type of electronic surveillance defined by the Act, which involves the acquisition of certain types of wire communications, *see id.* § 1801(f)(2), is potentially implicated to varying degrees (or not at all) in each of the four acquisition authorities at issue. *See, e.g., In re* [REDACTED]

[REDACTED]

[REDACTED], Docket No. [REDACTED] Application at 18-19, filed Dec. 13, 2006; *In re* [REDACTED]

<sup>7</sup> Specifically, in Docket No. [REDACTED], the authority granted by the Court required that "[a]ll selectors shall be telephone numbers or e-mail addresses that NSA reasonably believes are being used by persons outside the United States," *In re* [REDACTED]

[REDACTED] Docket No. [REDACTED] Primary Order at 12 (USFISC Apr. 6, 2007) (hereinafter "[REDACTED] Primary Order"); in Docket No. [REDACTED], the authority granted by the Court was "limited to the surveillance of telephone numbers and e-mail accounts/addresses/identifiers which the NSA reasonably believes are being used, or about to be used, by persons outside the United States," *In re* [REDACTED]

[REDACTED], Docket No. [REDACTED] Primary Order at 11 (USFISC Aug. 24, 2007) (hereinafter "[REDACTED] Primary Order"); under the PAA, the Government was only authorized to acquire "foreign intelligence information concerning persons reasonably believed to be located outside the United States," § 105B(a), 121 Stat. at 552; and under section 702, the Government may acquire foreign intelligence information through "the targeting of persons reasonably believed to be located outside the United States," 50 U.S.C. § 1881a(a), and is prohibited from "intentionally target[ing] any person known at the time of acquisition to be located in the United States," *id.* § 1881a(b)(1). (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN

[REDACTED]

[REDACTED] Docket No. [REDACTED] Application at 16-17, filed May 24, 2007.<sup>8</sup> As noted above, all communications acquired through NSA's upstream collections under the four authorities are wire communications, as defined by the Act. Because the fourth type of electronic surveillance specifically excludes the acquisition of wire communications, *see id.* § 1801(f)(4), it does not apply to NSA's upstream collections under the authorities at issue. (TS//SI//NF)

Pursuant to the authority granted by this Court in Docket Nos. [REDACTED]

[REDACTED] NSA acquired wire communications through its upstream collections. To the extent that such wire communications (including any discrete communications within an MCT) were to or from a person inside the United States, the acquisition of those communications would have constituted electronic surveillance as defined in subsection 1801(f)(2). Most of that electronic surveillance was specifically contemplated and approved by the Court in these dockets. However, upon closer review of the record and as described below, certain wire communications to or from persons located in the United States acquired through NSA's upstream collections may not have been specifically contemplated by the Court at the time authorization orders were issued in Docket Nos. [REDACTED] (TS//SI//NF)

<sup>8</sup> [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] (TS//SI//NF)

TOP SECRET//COMINT//ORCON,NOFORN

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Section 105A of the PAA "carved out" of the FISA Title I definitions of electronic surveillance, a surveillance directed at a person reasonably believed to be located outside of the United States. § 105A, 121 Stat. at 552 ("Nothing in the definition of electronic surveillance under section 101(f) [i.e., 50 U.S.C. § 1801(f)] shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States."). As explained in detail below, NSA's acquisitions pursuant to the PAA were at all times the product of surveillance directed at persons reasonably believed to be located outside the United States and thus did not constitute electronic surveillance as defined by the Act. Accordingly, section 1809(a) is not implicated by NSA's acquisition of any communications pursuant to PAA -- even those that may not have been specifically contemplated or considered by the Court at the time it reviewed and approved NSA's targeting procedures as required by Section 105C of the PAA.<sup>9</sup>

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

Unlike the PAA, section 702 did not exempt from the Act's definition of electronic surveillance the acquisitions contemplated by section 702. Many, if not most,

---

<sup>9</sup> As noted above, the scope of judicial review under the PAA was narrow. Section 105B(c) required the Attorney General to transmit to the Court a copy of each certification. *See* § 105B(c), 121 Stat. at 553. Section 105C(a) required the Attorney General to submit to the FISC "the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance." *Id.* § 105C(a), 121 Stat. at 555. Following such submission by the Attorney General, the Court was required to assess the Government's determination by applying a clearly erroneous standard. *See id.* § 105C(b), 121 Stat. at 555. Attorney General and Director of National Intelligence determinations regarding the purpose of the acquisitions and adequacy of the minimization procedures were not subject to Court review under Section 105C. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

of the wire communications NSA has acquired through its section 702 upstream collections were specifically contemplated and considered by the Court during its review and approval of NSA's targeting and minimization procedures as required by section 702(i) of the Act.<sup>10</sup> However, NSA has also collected certain other communications to or from persons located in the United States through its upstream collections pursuant to section 702 authorizations that were not specifically contemplated or considered by the Court at the time it reviewed and approved NSA's minimization and targeting procedures. ~~(TS//SI//NF)~~

For the reasons more particularly discussed above, the Government maintains that it did not engage in unauthorized electronic surveillance, let alone did so intentionally in violation of section 1809(a)(1). Should the Court determine that portions of the acquisitions under the four pertinent authorities were not authorized, the following summarizes the extent to which the Government believes section 1809(a)(2), which would govern the further disclosure or use of unauthorized acquisitions, would be implicated. For purposes of clarity and ease of understanding, this discussion categorizes the communications at issue in the same manner this Court

---

<sup>10</sup> Pursuant to section 702, the Court has jurisdiction to review certifications and minimization and targeting procedures and any amendments thereto. *See* 50 U.S.C. § 1881a(i)(1)(A). Certifications are reviewed to ensure that they contain all required elements. *Id.* § 1881a(i)(2)(A). Minimization procedures are reviewed to assess whether they meet the requirements of the Act and are consistent with the Fourth Amendment. *Id.* § 1881a(i)(2)(C). Targeting procedures are reviewed to assess whether they are reasonably designed to ensure that acquisitions are limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of wholly domestic communications. *Id.* § 1881a(i)(2)(B). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

did in its opinion of October 3, 2011. In addition, as used in this discussion, the term "communication" refers to a single discrete communication within an Internet transaction.<sup>11</sup> ~~(S)~~

A. Active User is the Target ~~(S)~~

Under Docket Nos. [REDACTED] the PAA, and section 702, section 1809(a) is not implicated at all with respect to the acquisition of communications where the active user is the target. That is because such acquisitions were clearly authorized under all four authorities. *See, e.g., In re DNI/AG 702(g) Certifications* [REDACTED] *et al.*, Docket Nos. [REDACTED] Order at 3 (USFISC Oct. 3, 2011).<sup>12</sup> ~~(TS//SI//NF)~~

<sup>11</sup> An Internet transaction may consist of one or more single, discrete communications. *See* Oct. 3 Mem. Op. at 15. ~~(TS//SI//NF)~~

<sup>12</sup> The Government also notes that the acquisition of communications where the active user is the target in many cases does not constitute "electronic surveillance." With respect to Docket No. [REDACTED] Docket No. [REDACTED] and section 702, the acquisition of communications where the active user is the target constitutes electronic surveillance only to the extent that such communications are to or from a person in the United States. Under the PAA, the acquisition of all communications where the active user of the transaction is the target -- even communications to or from a person in the United States -- is not "electronic surveillance." As discussed above, the PAA removed from FISA's definition of electronic surveillance "surveillance directed at a person reasonably believed to be located outside of the United States." § 105A, 121 Stat. at 552. Where the active user of the acquired communication was the target, the surveillance resulting in that acquisition was directed at a person reasonably believed to be located outside the United States (i.e., the target). *See* PAA Mem. Op. at 13 ("[I]t is natural to think of the users of the tasked facilities as the persons at whom surveillance is 'directed.'"). Accordingly, such acquisitions are not "electronic surveillance" under the PAA. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

B. Active User is Not the Target and is Located Overseas ~~(S)~~

Under Docket No. [REDACTED] and section 702, the acquisition of communications where the active user of the communication is not the target but is located overseas potentially implicates section 1809(a), but only under very limited circumstances. First, section 1809(a) is not implicated if the communication of the non-target active user located outside the United States is to or from another person located outside the United States (including the user of a tasked selector), because the acquisition of such a communication is not "electronic surveillance."<sup>13</sup> Second, if the communication of the non-target active user located outside the United States is to or from a person located in the United States (and its acquisition is thus "electronic surveillance"), section 1809(a) is not implicated if the communication is one of the [REDACTED] types of "abouts" communications recognized by the Court in Docket No. [REDACTED] *see In re* [REDACTED], Primary Order at 13-14 (USFISC Aug. 24, 2007) (hereinafter "[REDACTED] Primary Order"); under the PAA, *see* PAA Mem. Op. at 17 n.18; and section 702, *see, e.g., In re DNI/AG Certification* [REDACTED], Docket No. 702(i)-08-01, Mem. Op. at 17-18 n.14 (USFISC Sept. 4, 2008) (hereinafter "[REDACTED] Mem. Op.").<sup>14</sup> It is only in cases where a communication of the

<sup>13</sup> Moreover, to the extent that such communications were to or from the user of a tasked selector (i.e., a target), the acquisition of such communications was authorized in any event. ~~(S)~~

<sup>14</sup> For example, as explained by the Court in approving DNI/AG 702(g) Certification [REDACTED] the categories of "abouts" communications include where:

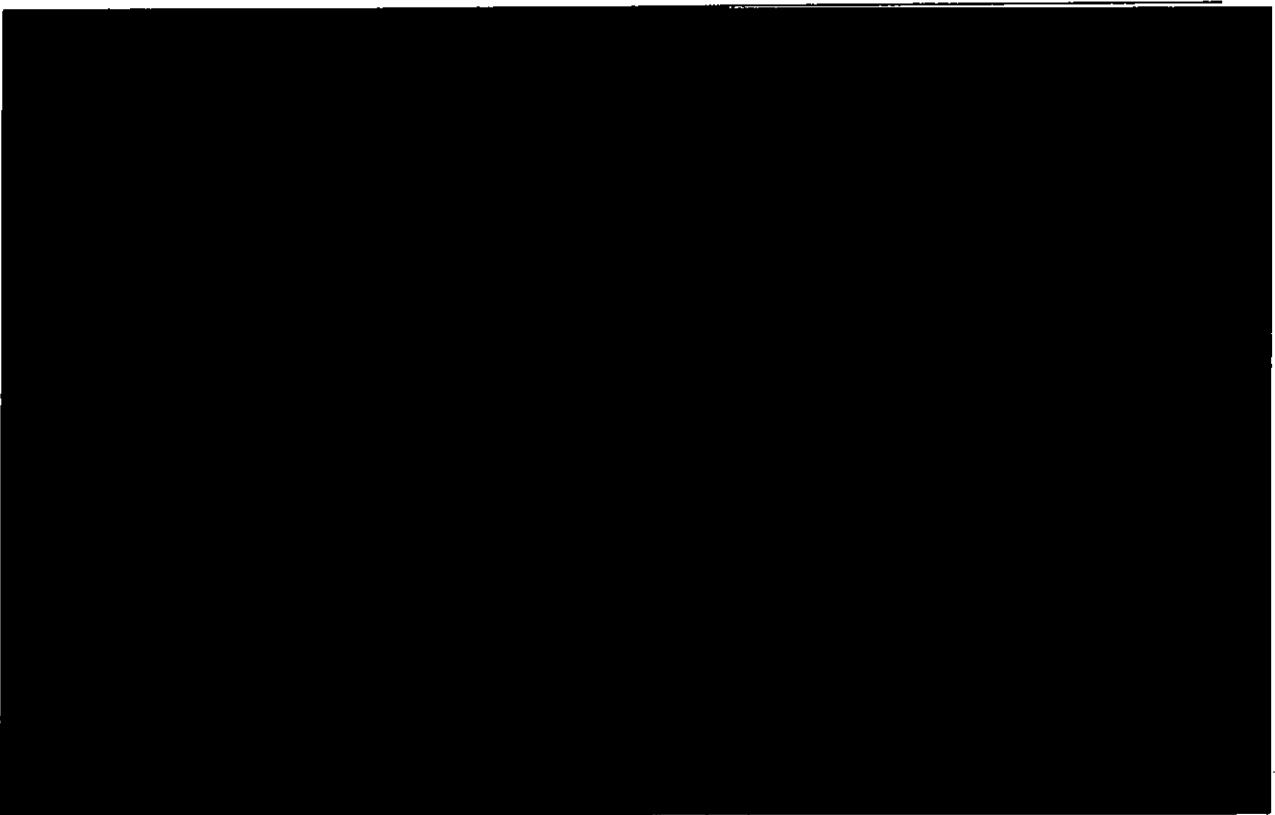
~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

non-target active user outside the United States is (1) to or from a person located in the United States and (2) either is not one of the [REDACTED] types of "abouts" communications described to the Court, or the communication does not contain a tasked selector at all, that section 1809(a) is implicated by the acquisition of communications where the active user of the transaction is a non-targeted person located overseas. ~~(TS//SI//NF)~~

The acquisition of communications under Docket No. [REDACTED] where the active user of the transaction is not the target but is located overseas implicates section 1809(a) to an even lesser extent than similar acquisitions under Docket No. [REDACTED] and section 702. As with Docket No. [REDACTED] and section 702, the acquisition of a foreign-based

~~Id. (TS//SI//NF)~~~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

active user's communication does not implicate section 1809(a) if the communication is to or from another person located outside the United States (including the user of a tasked selector), because the communication is not acquired through "electronic surveillance."<sup>15</sup> Unlike Docket No. [REDACTED] and section 702, however, the scope of the acquisition of "abouts" communications was not defined under Docket No. [REDACTED] See [REDACTED] Primary Order at 8 n.6 ("The Court understands that [REDACTED] will select [REDACTED] not only international Internet communications to and from agents of [the targeted foreign powers], but also Internet communications in which e-mail addresses [REDACTED] or such agents are mentioned in the Internet communication."). Thus, if the communication of the non-target active user located outside the United States is to or from a person in the United States, its acquisition was authorized so long as a tasked selector was present in the communication, regardless of the type of "about" that communication is. It is only in cases where a tasked selector does not appear in a communication between a non-target active user located outside the United States and a person in the United States that section 1809(a) is implicated. ~~(TS//SI//NF)~~

Section 1809(a) is not implicated at all with respect to any communication acquired under the PAA where the active user of the communication is [REDACTED]

[REDACTED]

---

<sup>15</sup> Again, to the extent that such communications were to or from the user of a tasked selector (i.e., a target), the acquisition of such communications was authorized in any event. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] That is because all such acquisitions under the PAA resulted from surveillance directed at a person reasonably believed to be located outside the United States (i.e., the non-target active user). Specifically, if the communication is between [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>16</sup> The surveillance would also be directed at the non-target active user located outside the United States if the acquired communication was a communication sent to or from a person in the United States, even if the communication did not contain a tasked selector. Cf. PAA Mem. Op. at 21 (accepting, *inter alia*, that "abouts" surveillance is directed "at those parties to the acquired communications who, by virtue of the use of Internet Protocol filters or [REDACTED] [REDACTED] are reasonably believed to be located outside the United States."). Accordingly, such acquisitions do not implicate section 1809(a) because they do not constitute "electronic surveillance" as defined by FISA. ~~(TS//SI//NF)~~

C. Active User is Not the Target and Whose Location is Not (and Cannot Be) Known ~~(S)~~

Section 1809(a) is not implicated by acquisition under the PAA of *any* communications where the active user's location is not (and cannot be) known. This is

<sup>16</sup> The Government also notes that the acquisition of such a communication would not be "electronic surveillance" even in the absence of the § 105A carve-out, because the communication is not to or from a person in the United States. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

most evident when such communication is to or from a person located outside the United States (including the user of a tasked selector), at whom it can be said the surveillance resulting in the acquisition is directed. It is equally true, albeit somewhat counter-intuitively, for any communication between an active user whose location is not (and cannot be) known and a person located in the United States. As discussed above, section 105A of the PAA excluded surveillance that is directed at a person "reasonably believed" to be located outside the United States from FISA's definition of "electronic surveillance." The means described in the NSA's PAA targeting procedures -- i.e., the use of IP filters or [REDACTED]

[REDACTED] -- operated to ensure that acquisitions were directed at a person reasonably believed to be located outside the United States. Just because NSA ultimately may be unable to determine the true location of the active user of the communication does not mean NSA did not reasonably believe, at the time of acquisition, that the surveillance was being directed at a person located outside the United States. Cf. *In re DNI/AG 105B Certifications* [REDACTED] Docket Nos. Transcript of Proceedings at 47-48 (USFISC Dec. 12, 2007) (hereinafter "PAA Transcript") (recognizing one possible scenario where [REDACTED])

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

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Section 1809(a)(2) is also not implicated with respect to acquisitions under Docket No. [REDACTED], Docket No. [REDACTED] and section 702 where the communication is between a person outside the United States and an active user whose location is not (and cannot be) known. Section 1809(a)(2), which makes it a crime to intentionally "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act," among other authorities. If the location of the non-target active user cannot be determined, and the other communicant is known to be located outside the United States, then one cannot "know[] or hav[e] reason to know" that the communication was acquired through electronic surveillance at all. Cf. *In re* [REDACTED] *et al.*, Docket No. [REDACTED] Mem. Op. at 114 (USFISC [REDACTED] hereinafter "PR/TT Mem. Op.") (recognizing that "it might not be apparent from available information whether the communication to which a piece of data relates is to or from a person in the United States, such that acquisition constituted electronic surveillance as defined in Section 1801(f)(2)"). Section 1809(a)(2) can hardly be said to be implicated by the use or disclosure of communications acquired under such circumstances. *See id.* at 115 ("When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance not authorized by the Court's prior orders, the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

information is not subject to the criminal prohibition in Section 1809(a)(2).").

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

Under Docket No. [REDACTED] and section 702, it is only in cases where the active user is a non-target whose location is not (and cannot be) known communicates with a person in the United States that section 1809(a)(2) is potentially implicated. Yet if the communication of a non-target active user whose location is not (and cannot be) known is to or from a person in the United States, its acquisition under those two authorities does not implicate Section 1809(a)(2) if the acquired communication is one of the [REDACTED] types of "abouts" communications recognized by the Court. Under Docket No. [REDACTED] and section 702, it is only in cases where the communication is not one of these [REDACTED] types of "abouts" communications, or the communication does not contain a tasked selector at all, that 1809(a)(2) is implicated by the acquisition of a communication to or from a person in the United States where the location of the non-target active user is not (and cannot be) known. ~~(TS//SI//NF)~~

Acquisition under Docket No. [REDACTED] of communications to or from a person in the United States where the location of the non-target active user of the communication is not (and cannot be) known implicates section 1809(a)(2) to an even lesser extent than similar acquisitions under Docket No. [REDACTED] and section 702. That is because, as discussed above, the scope of the acquisition of "abouts" communications was not defined under Docket No. [REDACTED]. Thus, if the communication is between a non-target

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

active user whose location is not (and cannot be) known and a person in the United States, its acquisition was authorized so long as a tasked selector was present in the communication, regardless of the type of "about" that communication is. It is only in cases where a tasked selector does not appear in communication between a non-target active user whose location is not (and cannot be) known and a person in the United States that section 1809(a)(2) is implicated. ~~(TS//SI//NF)~~

D. Active User is Not the Target and is Located in the United States ~~(S)~~

Section 1809(a) is not implicated at all with respect to the acquisition of communications under the PAA where the active user is not the target and is located in the United States. Section 105A of the PAA excluded from the definition of "electronic surveillance" surveillance that is directed at a person reasonably believed to be located outside the United States. See § 105A, 121 Stat. at 552. As discussed in more detail below, communications acquired under the PAA where the active user was located in the United States -- even those that do not contain a tasked selector -- were the product of surveillance directed at a person reasonably believed to be located outside the United States, and thus did not constitute "electronic surveillance" by virtue of section 105A.

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

This conclusion is most obvious where the communication is between a U.S.-based active user and the user of a tasked facility (i.e., the target). In that case, the surveillance is clearly directed at the foreign-based target. See PAA Mem. Op. at 13

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

("[I]t is natural to think of the users of the tasked facilities as the persons at whom surveillance is 'directed.'"). Somewhat less obvious, but no less true, are instances where the communication is between a U.S.-based active user and a non-target reasonably believed to be located outside the United States. Cf. PAA Mem. Op. at 21 (accepting, *inter alia*, that "abouts" surveillance is directed "at those parties to the acquired communications who, by virtue of the use of Internet Protocol filters or [REDACTED] [REDACTED] are reasonably believed to be located outside the United States."); *In re DNI/AG 105B Certification* [REDACTED] Ex. A (NSA Targeting Procedures), filed Aug. 17, 2007, at 1-2 ("In addition, in those cases where NSA seeks to acquire communications about the target that is not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [REDACTED] [REDACTED]. In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.").

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

Under the PAA, even the acquisition of communications that were in fact sent between an active user in the United States and another person in the United States did not constitute "electronic surveillance," so long as at the time of acquisition NSA reasonably believed that one of those communicants was located outside the United States. As discussed above, section 105A of the PAA excluded surveillance that is

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

directed at a person "reasonably believed" to be located outside the United States from FISA's definition of "electronic surveillance." The means described in the NSA's PAA targeting procedures -- i.e., the use of Internet Protocol (IP) filters or [REDACTED] [REDACTED] -- were reasonably designed to ensure that each acquisition was directed at a person reasonably believed to be located outside the United States.<sup>17</sup> That this reasonable belief may ultimately have proven to be mistaken does not mean that the acquisition resulted from "electronic surveillance" because the communication was in fact to or from a person in the United States. Cf. [REDACTED] Mem. Op. at 25 (concluding that "the government is authorized [under section 702] to acquire communications when it has a reasonable, but mistaken, belief that a target is a non-U.S. person located outside the United States"); PAA Transcript at 47-48 (recognizing one possible scenario where [REDACTED]

[REDACTED] [REDACTED]).<sup>18</sup> ~~(TS//SI//NF)~~

<sup>17</sup> As previously explained to the Court, these means are employed with respect to any Internet transaction acquired through NSA upstream collection, not just "abouts." See June 1 Submission, at 5. ~~(TS//SI//NF)~~

<sup>18</sup> The Court also concluded that "abouts" acquisitions were directed at the users of the tasked selectors referred to in those communications, rather than the senders or recipients of the communications. See PAA Mem. Op. at 21. Although this was not a theory advanced by the government, see *id.* at 20, the government notes that the acquisition of wholly domestic "abouts" communications would not be "electronic surveillance" under this theory either, because such surveillance would have been directed at the foreign-based user of the tasked selector. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Of course, section 1809(a) is potentially implicated under Docket No. [REDACTED] Docket No. [REDACTED] and section 702 in cases where the active user is located in the United States. That is because every such communication would be to or from a person in the United States (i.e., the U.S.-based active user) and, therefore, their acquisition would constitute electronic surveillance as defined in section 1801(f)(2). Thus, the relevant inquiry here focuses solely on whether such (f)(2) electronic surveillance was authorized. Most obviously, section 1809(a) is not implicated by the acquisition of communications between an active user in the United States and a user of a tasked selector, because such acquisitions would in all cases be authorized (f)(2) electronic surveillance. At the other end of the spectrum, the acquisition of the communications of a U.S.-based active user that do not contain a tasked selector implicates section 1809(a) if it is ultimately concluded that such acquisitions are not authorized. ~~(TS//SI//NF)~~

Falling between these two extremes is the acquisition of "abouts" communications of a U.S.-based active user. Under Docket No. [REDACTED], the acquisition of all types of "abouts" communications of a U.S.-based active user would be authorized (f)(2) electronic surveillance because, as discussed above, the scope of the acquisition of "abouts" communications was not defined under [REDACTED]. However, only those "abouts" communications of a U.S.-based active user that fall within the [REDACTED] types of "abouts" described to the Court under Docket No. [REDACTED] and section 702 would be authorized (f)(2) surveillance. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

As with the PAA, the acquisition of wholly domestic "abouts" communications under Docket Nos. [REDACTED] and [REDACTED] does not implicate section 1809(a). To acquire a communication under the authority granted in Docket No. [REDACTED] NSA was required to establish probable cause to believe that at least one party to the communication was outside the United States. See [REDACTED] Primary Order at 12. To establish this probable cause, NSA employed IP filters or [REDACTED]

[REDACTED] See *id.* at 8. Use of either of these means would "reasonably ensur[e] that the [acquired] communications originate or terminate in a foreign country." *Id.* That this probable cause determination may ultimately have been proven wrong in a particular case does not mean that the resulting acquisitions did not comport with the Court's order and thus were unauthorized. See, e.g., *Illinois v. Rodriguez*, 497 U.S. 177, 195 (1990) ("[T]he possibility of factual error is built into the probable cause standard."); *Illinois v. Gates*, 462 U.S. 213, 246 n.14 (1983) ("Probable cause . . . simply does not require [] perfection."). Indeed, this Court explicitly recognized that NSA's IP filters would not in all cases prevent the acquisition of all wholly domestic communications. See [REDACTED] Primary Order at 8 n.7 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

[REDACTED]"). ~~(TS//SI//NF)~~

The same holds true for the acquisition of wholly domestic "abouts" communications under Docket No. [REDACTED]. Although the order entered in Docket No. [REDACTED] did not require NSA to establish probable cause to believe that a party to an acquired communication be located outside the United States, the Government's authority to acquire "abouts" communications under that docket was nonetheless limited to communications as to which "NSA reasonably believe[d] that the e-mail account/address/identifier [sending or receiving the 'abouts' communication was] being used, or [was] about to be used, by persons located outside the United States." [REDACTED] Primary Order at 15. The means approved by the Court for NSA to use to formulate that reasonable belief were the same [REDACTED] methods used under Docket No. [REDACTED]. See *id.* at 21 (recognizing that [REDACTED])

[REDACTED]

[REDACTED] IP filters may be used "to increase the chances of collecting foreign communications" and "to minimize acquisition of communications wholly within the United States."). Again, like under the PAA and Docket No. [REDACTED] the fact that these mechanisms did not in all cases prevent the acquisition of wholly domestic communications is not inconsistent with this reasonable belief; nor does it mean that an

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

acquisition conducted under that reasonable belief was unauthorized. *See, e.g.,*

*Rodriguez*, 497 U.S. at 195; *Gates*, 462 U.S. at 246 n.14. ~~(TS//SI//NF)~~

Section 1809(a) is implicated by the acquisition of "abouts" communications between a U.S.-based active user and another person in the United States under section 702. However, the Government notes that this Court recently held that NSA's targeting procedures are reasonably designed to prevent the acquisition of such communications, and that their acquisition does not run afoul of section 702(b)(4). *See* Oct. 3 Mem. Op. at 47-48. ~~(TS//SI//NF)~~

3. Whether the collections under Section 1881a, the PAA, and Docket Nos. [REDACTED] & [REDACTED] include information that was not authorized for acquisition, but is not subject to the criminal prohibitions of Section 1809(a). ~~(S)~~

Should the Court determine that NSA's upstream collection of communications that included "abouts" communications outside of the [REDACTED] categories previously specified to the Court in Docket No. [REDACTED], the PAA, and section 702,<sup>19</sup> as well as those discrete communications collected under all four pertinent authorities that are not to, from, or about a tasked selector, was not authorized, the Government believes that the following categories of information, although unauthorized, would not be subject to the provisions of section 1809(a), because they do not constitute electronic surveillance, as defined by FISA: ~~(TS//SI//NF)~~

---

<sup>19</sup> As noted above, the categories of "abouts" communications that could be acquired were not discussed or specified under the authorities granted in Docket No. [REDACTED] ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

(1) Where the active user is the target: As discussed above, where the active user is the target, all acquisitions were clearly authorized under all four authorities.

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

(2) Where the active user is outside the United States or the active user's location is not (and cannot be) known: In such situations, acquisition would have been unauthorized, but would not have constituted electronic surveillance -- and therefore not subject to section 1809(a) -- in two situations, both of which would require the active user to be communicating [REDACTED]

[REDACTED]. First, under Docket No. [REDACTED], the PAA, and section 702, collection would be unauthorized where the acquired communication was about a tasked selector, but was not one of the [REDACTED] categories of "abouts" communications previously specified to the Court (*see* footnote 14, *supra*). Second, for all four authorities, collection would be unauthorized, but not subject to section 1809(a), where the discrete communication acquired (whether standing alone or within the context of an MCT) was not to, from, or about a tasked selector. ~~(TS//SI//NF)~~

(3) Where the active user is located inside the United States: As described above, due to the user's location in the United States, any unauthorized acquisition under Docket Nos. [REDACTED] and [REDACTED] as well as section 702 would constitute electronic surveillance as defined by 50 U.S.C. § 1801(f)(2), and therefore would be subject to section 1809(a). Acquisitions under the PAA, which as discussed

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

above were exempted from FISA's definition of electronic surveillance, would have been unauthorized, but not subject to section 1809(a), where (i) the acquired communication was about a tasked selector, but was not one of the [REDACTED] previously described categories of "abouts" communications, or (ii) where the acquired discrete communication (whether standing alone or within the context of an MCT) was not to, from, or about a tasked selector. ~~(TS//SI//NF)~~

**4. Whether any of the over-collected material has "aged off" NSA systems such that it is no longer retained by NSA or accessible to its analysts. ~~(S)~~**

As indicated above, NSA is implementing a reduced retention period of two years for upstream Internet collection from Docket Nos. [REDACTED] and [REDACTED], the PAA, and section 702, thus accelerating the scheduled age-off of such collection in NSA systems.<sup>20</sup> Doing so will require NSA to make significant adjustments to the software and handling rules associated with its repositories, and NSA estimates that it may take until at least March 2012 to responsibly complete the accelerated age-off without adversely affecting the data repositories and technical infrastructure NSA relies upon to appropriately handle the information it acquires pursuant to its section 702 authorities. NSA will update the Court on its progress at appropriate intervals and provide final notification once the accelerated age-off process has been completed.<sup>21</sup> The age-off will

---

<sup>20</sup> The two-year retention period will be calculated from the expiration of the relevant authorization. ~~(S)~~

<sup>21</sup> In the course of effecting the actions described herein, NSA may determine that it is necessary to submit amended procedures in response to operational concerns. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

result in a significant reduction in the amount of data that might contain information subject to section 1809(a)(2) should the Court determine that certain aspects of NSA's collection of Internet transactions upstream was not authorized. ~~(TS//SI//NF)~~

The material collected pursuant to Docket Nos. [REDACTED] and [REDACTED] DNI/AG 105B Certifications [REDACTED] under the PAA, and section 702 is subject to a five-year retention period, which is still in effect for all of these authorities. Accordingly, the oldest of the material is not due to begin to age off until 2012. However, as set forth above, NSA is currently in the process of applying an accelerated age-off to the upstream data collected pursuant to these authorities. ~~(TS//SI//NF)~~

As of the time of this filing, NSA has confirmed that unevaluated Internet transactions collected pursuant to PAA DNI/AG 105B Certification [REDACTED] [REDACTED] during the first twelve months it was in effect,<sup>22</sup> all of which featured a one-year retention period, has aged-off in NSA collection stores, corporate stores, [REDACTED] and some of NSA's backup systems. Thus, the data from [REDACTED] remains in certain NSA backup systems, but will eventually be removed.<sup>23</sup> [REDACTED]

<sup>22</sup> DNI/AG 105B Certification 08-01 [REDACTED]

[REDACTED] DNI/AG 105B Certification 08-01. ~~(S)~~

<sup>23</sup> NSA maintains backup and archive systems whose function is to provide data recovery in the event of a system failure or other disaster. The material which has not aged-off in the backup systems is not available for use by intelligence analysts. Because of the varied nature of the individual backup systems, NSA will assure compliance with the retention periods for collected data by requiring each system to

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

[REDACTED] However, as noted

above, the accelerated age-off process will remove the upstream data from DNI/AG 105B Certification 08-01 that is subject to the four-year extension, as well as Internet transactions collected pursuant to the PAA to the extent that those transactions had been evaluated, in whole or in part, and determined to be suitable for retention in accordance with the applicable minimization procedures. ~~(TS//SI//NF)~~

5. If the government has determined that it has acquired information that is subject to Section 1809(a) or was otherwise unauthorized: ~~(S)~~

- a. Describe how the government proposes to treat any portions of the prior unauthorized collection that are subject to the criminal prohibitions of Section 1809(a). ~~(S)~~

As noted above, for technical reasons, NSA will not be able to apply retroactively the segregation process described in section 3(b)(5)a. of the 2011 Amended NSA Minimization Procedures to Internet transactions acquired via its upstream collection techniques prior to October 31, 2011. That data has already been distributed into NSA repositories. It would not be technically feasible for NSA to reach into those repositories and retroactively apply the segregation process described in section 3(b)(5)a. of the 2011 Amended NSA Minimization Procedures to data that is already within them. For that reason, and to further maintain consistency of its minimization

---

maintain the integrity of the age-off function through system requirements which will ensure that aged-off data is not reintroduced into collection, corporate, and/or analytic stores. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

procedures across acquisitions pursuant to multiple DNI/AG 702(g) certifications, NSA will train its analysts to conduct the analysis set out in section 3(b)(5)b. of the 2011 Amended NSA Minimization Procedures to all MCTs encountered by an analyst and make use of only those portions of an MCT authorized by section 3(b)(5)b. (TS//SI//NF)

Irrespective of the Court's final determination regarding the application of section 1809(a)(2), NSA fully intends to apply the requirements of sections 3(b)(5)(b) and 3(c)(2) of the 2011 Amended NSA Minimization Procedures to any use of Internet transactions previously collected through NSA's upstream collection techniques. Thus, NSA analysts will apply the applicable portions of the 2011 Amended NSA Minimization Procedures to all MCTs collected through NSA's upstream collection techniques prior to the Attorney General's adoption of the amended minimization procedures on October 31, 2011, and like all other upstream collection, information that does not meet the retention standards set forth in the amended procedures will only be retained for two years in any event. (TS//SI//NF)

**b. What steps is NSA taking to ensure that such information subject to 1809(a) is not used in proceedings before the Court?-(S)**

As reflected in the Government's Notice of Clarifications filed on August 30, 2011, NSA has implemented a process to review information from upstream Internet transactions prior to use in FISA applications or other submissions to this Court consistent with section 3(b)(5)b. in the 2011 Amended NSA Minimization Procedures.

See Notice of Clarifications, Docket Nos. [REDACTED] filed

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

August 30, 2011, at 9-10; *see also* 2011 Amended NSA Minimization Procedures, § 3(b)(5)b. NSA will work with the Department of Justice to implement the same process for any communications acquired pursuant to the four pertinent authorities when those communications are relied upon in a submission to this Court made by the Central Intelligence Agency (CIA) or Federal Bureau of Investigation (FBI). *See* 2011 Amended NSA Minimization Procedures, § 3(b)(5)b.<sup>24</sup> ~~(TS//SI//NF)~~

**c. What steps is the government taking to remediate any prior use of such information in proceedings before this Court. ~~(S)~~**

For all new applications to the Court that rely upon NSA information contained in a previous FISA application, the Government will ensure that information is subjected to the same process described above that is required by section 3(b)(5)b. of the 2011 Amended NSA Minimization Procedures. In particular, as noted above, NSA will work with the Department of Justice to implement that process for any communications acquired pursuant to the four pertinent authorities when those communications are relied upon in a submission to this Court made by CIA, FBI, or NSA. ~~(TS//SI//NF)~~

---

<sup>24</sup> As discussed in the 2011 Amended NSA Minimization Procedures, NSA analysts may not use communications that are not to, from, or about a tasked selector, but are to or from U.S. persons or persons located in the United States, except to "protect against an immediate threat to human life." *See* 2011 Amended NSA Minimization Procedures, § 3(b)(5)b.2.(c). Moreover, "if technically possible or reasonably feasible," NSA analysts will document their determination that a discrete communication not to, from, or about a tasked selector is to or from an identifiable U.S. person or person reasonably believed to be located in the United States. *See id.* To the extent that the minimization procedures allow for the use of discrete communications in an MCT, those discrete communications (including any U.S. person information contained therein) must be handled in accordance with the applicable provisions of the minimization procedures. *See id.* § 3(b)(5)b.2.(a) and (b). ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

- d. How does the government propose to treat any portions of the collection that are unauthorized but not subject to Section 1809(a), and explain why such treatment is appropriate. ~~(S)~~

This question necessarily encompasses two separate categories of information. Because section 1809(a)(2) only reaches the disclosure or use of information a person knows or has reason to know was obtained under color of law via unauthorized electronic surveillance as defined in section 1801(f) of FISA, the first category of information would include single, discrete communications within an MCT where NSA does not know, and has no reason to know, that such communication was acquired under color of law through electronic surveillance which was not authorized.<sup>25</sup> For example, and as described above, under certain circumstances when the communication is between a person outside the United States and an active user whose location is not (and cannot be) known, NSA may have no way to determine based on available information whether a single, discrete communication (or metadata extracted from that communication) was sent to or from a non-targeted person actually located in the United States such that the acquisition constituted electronic surveillance as defined

---

<sup>25</sup> This Court has previously concluded that section 1809(a)(2) does not criminalize all disclosures or uses of unauthorized electronic surveillance. Section 1809(a)(2) reaches disclosures or use only by a person "knowing or having reason to know that the information was obtained through" unauthorized electronic surveillance. 50 U.S.C. § 1809(a)(2). "When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2)." See PR/TT Mem. Op. at 115. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

by section 1801(f)(2).<sup>26</sup> The second category of information obviously would include single, discrete communications within an MCT which NSA knows or has reason to know were not acquired through unauthorized electronic surveillance. Such communications would include, for example, single, discrete communications within an MCT as to which the active user is a non-target who is reasonably believed to be located outside the United States [REDACTED]

[REDACTED] The Government does not believe that there should be any restriction on its ability to retain, access, or use these two categories of information consistent with the applicable portions of NSA's minimization procedures. ~~(TS//SI//NF)~~

Single, discrete communications within an MCT which do not contain the presence of a tasked selector (and which fall into one of the two categories set out above) may nevertheless contain foreign intelligence information which is relevant to the authorized purpose of the acquisitions conducted pursuant to the four relevant authorities, and NSA is required to limit its queries to those which are reasonably designed to return foreign intelligence information. *See, e.g.,* 2011 Amended NSA Minimization Procedures, § 3(b)(6). Moreover, as described above, NSA has committed to applying section 3(b)(5)b. of its amended section 702 minimization procedures to its

---

<sup>26</sup> While pointing out that the Government may not be willfully blind in assessing whether a piece of information was obtained through unauthorized electronic surveillance, the Court has previously found that "neither Section 1809(a)(2) nor any other provision of law precludes it from authorizing the government to access and use this category of information." PR/TT Mem. Op. at 115. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

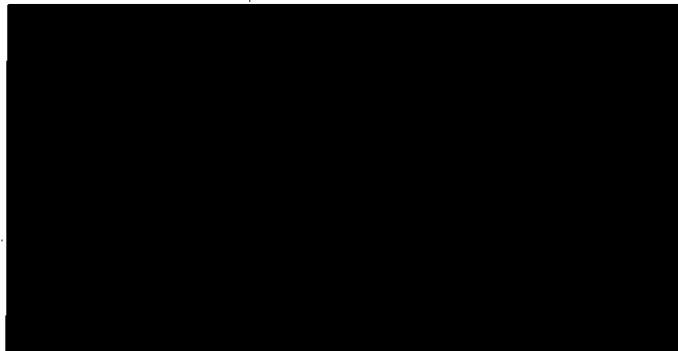
historical holdings, including transactions acquired pursuant to all four authorities at issue. Accordingly, even if the Court were to conclude that NSA's acquisition of certain information historically was not authorized, application of section 3(b)(5)b. of NSA's amended minimization procedures to its historical holdings would reasonably ensure that only information in MCTs which does not constitute electronic surveillance as defined by section 1801(f)(2) of FISA would be used or disseminated. ~~(TS//SI//NF)~~

6. Whether there are any other matters that should be brought to the Court's attention with regard to these collections that implicate Section 1809(a) or that were unauthorized. ~~(S)~~

After a thorough review of these collections, the Government has determined that there are no other matters that need to be brought to the Court's attention at this time that implicate section 1809(a) or that were unauthorized. ~~(S)~~

Respectfully submitted,

Tashina Gauhar  
Deputy Assistant Attorney General



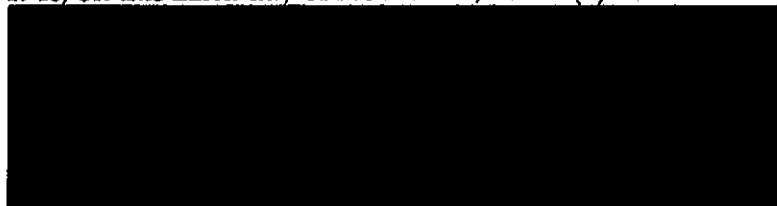
National Security Division  
U.S. Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

VERIFICATION

I declare under penalty of perjury that the facts set forth in the attached Government's Response to the Court's Briefing Order of October 13, 2011, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 22nd day of November, 2011. ~~(S)~~



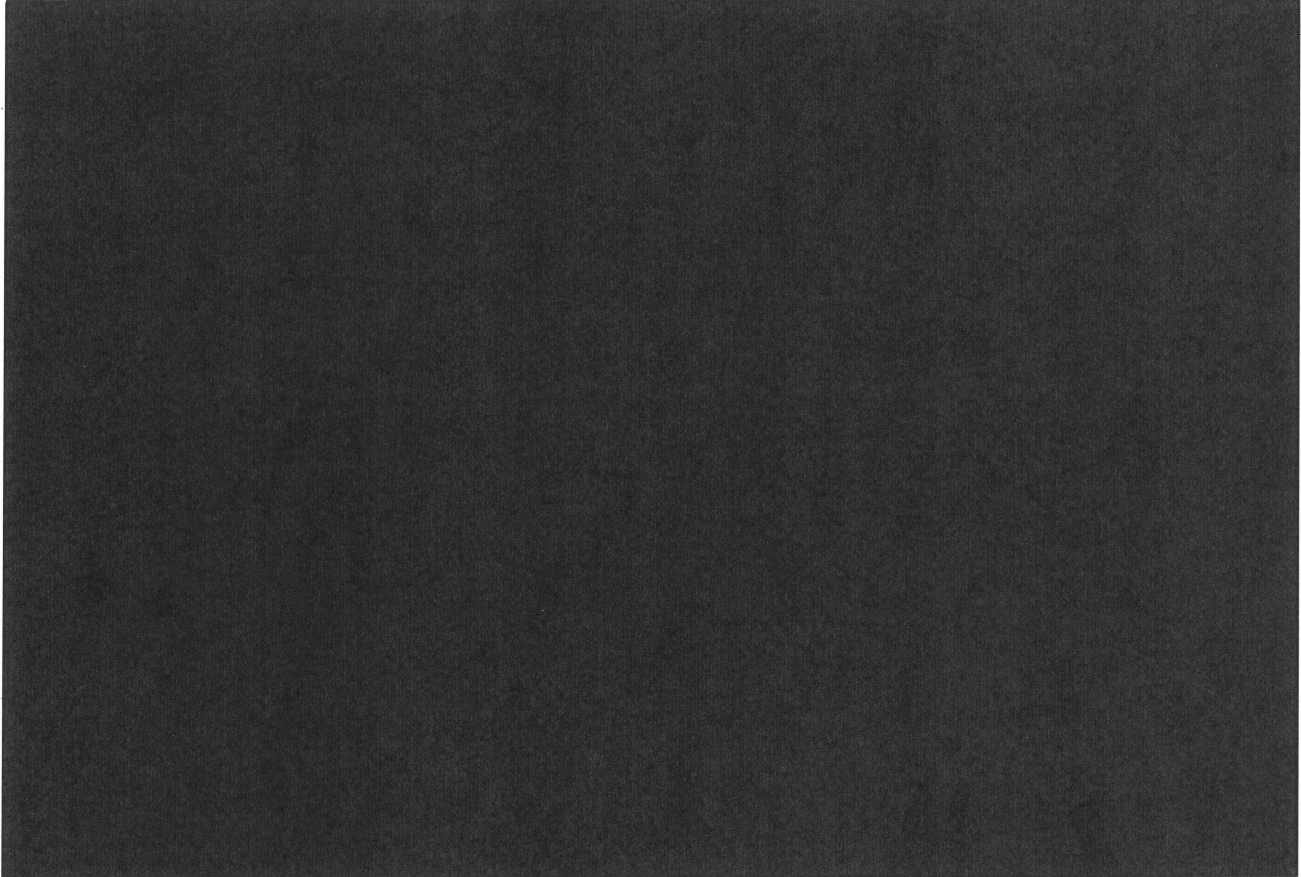
Signals Intelligence Directorate Compliance Architect  
National Security Agency

~~TOP SECRET//COMINT//ORCON,NOFORN~~

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

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT  
2011 NOV 29 PM 4:14  
FRANKLYN HALL  
COURT



NOTICE

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits this notice concerning the above-captioned matters. ~~(S//OC/NF)~~

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

~~Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: 29 November 2036~~



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

On April 13, 2011, the Director of National Intelligence and the Attorney General executed amendments to the above-captioned certifications. Those amendments authorized, *inter alia*, the use of the National Security Agency (NSA) section 702 minimization procedures submitted with DNI/AG 702(g) Certifications [REDACTED] [REDACTED] in connection with foreign intelligence information acquired in accordance with the above-captioned certifications. On October 3, 2011, this Court issued a Memorandum Opinion and Order finding, *inter alia*, those NSA section 702 minimization procedures deficient in certain respects. *See In re DNI/AG 702(g) Certifications* [REDACTED] Docket Nos [REDACTED] [REDACTED] Order at 3 (USFISC Oct. 3, 2011). The Court further ordered the Government to, at its election, correct within thirty days the deficiencies identified in the Memorandum Opinion and Order, or cease the implementation of the certifications to the extent they permit acquisitions implicating the deficiencies. *See id.* at 3-4.

~~(S//OC/NF)~~

On October 31, 2011, the Director of National Intelligence and the Attorney General executed amendments to DNI/AG 702(g) Certifications [REDACTED] [REDACTED] Those amendments authorized the immediate use of amended NSA section 702 minimization procedures containing additional provisions intended to correct the deficiencies identified by the Court in its Memorandum Opinion and Order of October 3, 2011. In particular, the amended NSA section 702 minimization procedures require

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

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

that as certain specific types of Internet transactions are acquired under DNI/AG 702(g) Certifications [REDACTED], those transactions shall be segregated and subjected to special access and handling rules. The amended NSA section 702 minimization procedures also limit NSA's retention of all Internet transactions acquired under DNI/AG 702(g) Certifications [REDACTED] and impose additional requirements that must be met before NSA analysts can use information contained in the transactions. The amended certifications, along with the amended NSA section 702 minimization procedures, were submitted to the Court for its review on October 31, 2011. ~~(TS//SI//OC/NF)~~

As explained to the Court in the Government's Response to the Court's Briefing Order of October 13, 2011, the Government cannot retrospectively apply all of the additional requirements in the amended NSA section 702 minimization procedures to communications that have already been acquired under the above-captioned certifications, all of which have already expired. See Government's Response to the Court's Briefing Order of Oct. 13, 2011, Docket Nos [REDACTED] [REDACTED] filed Nov. 22, 2011, at 2-3 & n.1. In particular, it is technically infeasible for NSA to apply the above-discussed segregation process to communications that have already been acquired under the above-captioned certifications. *Id.* at 2-3. The Government continues to evaluate the most appropriate means of handling communications acquired under the above-captioned certifications, and accordingly

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

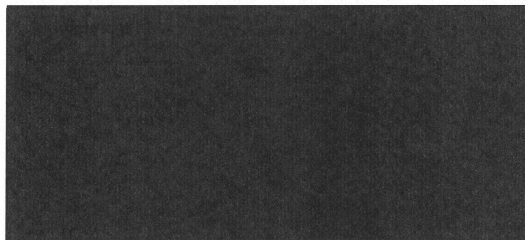
~~TOP SECRET//COMINT//ORCON//NOFORN~~

intends to expeditiously submit to the Court amended NSA minimization procedures.

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

In the interim, and as more specifically described in the Government's Response to the Court's Briefing Order of October 13, 2011, NSA has been applying and will continue to apply the additional requirements in the amended NSA section 702 minimization procedures that can feasibly be applied to Internet transactions that have already been acquired under the above-referenced certifications. ~~(TS//SI//OC/NF)~~

Respectfully submitted,



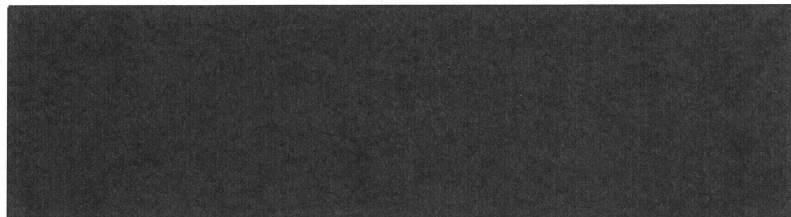
National Security Division  
U.S. Department of Justice

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

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

VERIFICATION

I declare under penalty of perjury that the facts set forth in the attached Notice of Clarification, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 29th day of November, 2011. ~~(S)~~



Signals Intelligence Directorate Compliance Architect  
National Security Agency

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



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

APPROVAL

I hereby approve the filing of this Verified Notice with respect to the above-captioned docket numbers with the United States Foreign Intelligence Surveillance Court. ~~(S)~~



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

11-29-11  
Date

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