

~~TOP SECRET//SI//ORCON//NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

JUL 28 PM 3:56


WASHINGTON, D.C.

LEEANN FLYNN HALL  
CLERK OF COURT



~~UNDER SEAL~~

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

~~(S//OC/NF)~~ In accordance with subsection 702(g)(1)(A) of the Foreign  
Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), the United States  
of America, by and through the undersigned Department of Justice attorney, hereby  
submits ex parte and under seal the attached certifications, 



~~TOP SECRET//SI//ORCON//NOFORN~~

Classified by: John P. Carlin, Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: 28 July 2039

~~TOP SECRET//SI//ORCON//NOFORN~~

These certifications reauthorize [REDACTED]  
[REDACTED] respectively, all of which  
expire on September 10, 2014. Attached as Exhibits A, B, C, D, E, and G to [REDACTED]  
[REDACTED] are the targeting and minimization  
procedures to be used under these certifications.<sup>1</sup>

(S//OC/NF) In addition, [REDACTED]  
[REDACTED] also include amendments to the certifications being reauthorized, [REDACTED]  
[REDACTED] and their predecessors.<sup>2</sup> Specifically,  
these amendments authorize the use of the minimization procedures attached herewith  
as Exhibits B, D, and E to [REDACTED] in  
connection with foreign intelligence information acquired in accordance with [REDACTED]

---

<sup>1</sup> (S//OC/NF) Specifically, the targeting procedures to be used by the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) are attached as Exhibits A and C, respectively. The minimization procedures to be used by NSA, the FBI, the Central Intelligence Agency (CIA), and the National Counterterrorism Center (NCTC) are attached as Exhibits B, D, E, and G, respectively. The NCTC minimization procedures attached as Exhibit G were submitted in connection with [REDACTED] on July 31, 2013, and were approved by the Court on August 30, 2013. The remaining targeting and minimization procedures are being submitted with [REDACTED] for approval by the Court.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



(S//OC/NF) With the exception of the NCTC minimization procedures attached as Exhibit G, the targeting and minimization procedures being submitted with [redacted] [redacted] contain a number of changes from the targeting and minimization procedures approved for use under the predecessor certifications. To aid the Court in its review of the targeting and minimization procedures, below is a discussion of certain of these changes. Also included below is an update to the description of the process that NSA uses to resolve [redacted] indicating that a tasked electronic communications [redacted] may have been accessed from inside the United States.

---

<sup>3</sup>(S//OC/NF) The NCTC minimization procedures attached herewith as Exhibit G are identical to the NCTC minimization procedures that already have been approved for use by this Court in connection with foreign intelligence information acquired in accordance with [redacted] [redacted] Thus, with respect to those procedures, no amendments are necessary.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

~~(S)~~ NSA's Targeting Procedures

~~(S)~~ The NSA targeting procedures submitted as Exhibit A to [REDACTED]

[REDACTED] contain a new provision that clarifies the intended scope of the procedures. Specifically, the NSA targeting procedures state that

[REDACTED]

~~(TS//SI//NF)~~ NSA is required under its current targeting procedures to detask facilities from section 702 acquisition when, *inter alia*, NSA believes that a user of that facility is inside the United States or is a United States person. To date, the Government has been applying this requirement even in circumstances [REDACTED]

[REDACTED]

[REDACTED] and to date the failure to detask the account prior to such access has been considered a compliance incident. Such incidents have involved, for example,

[REDACTED]

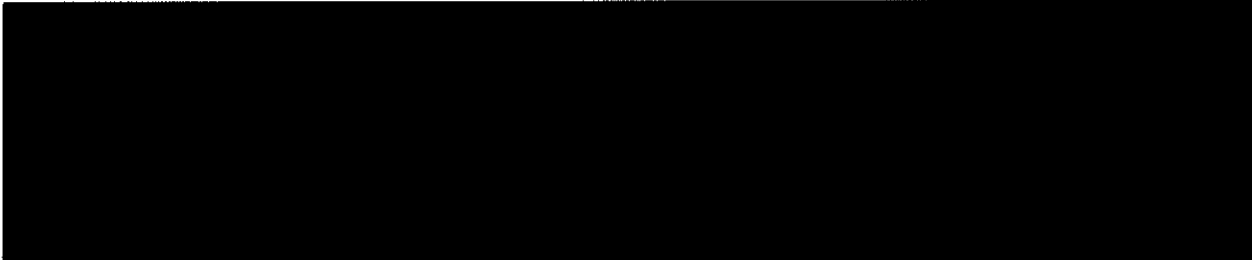
~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



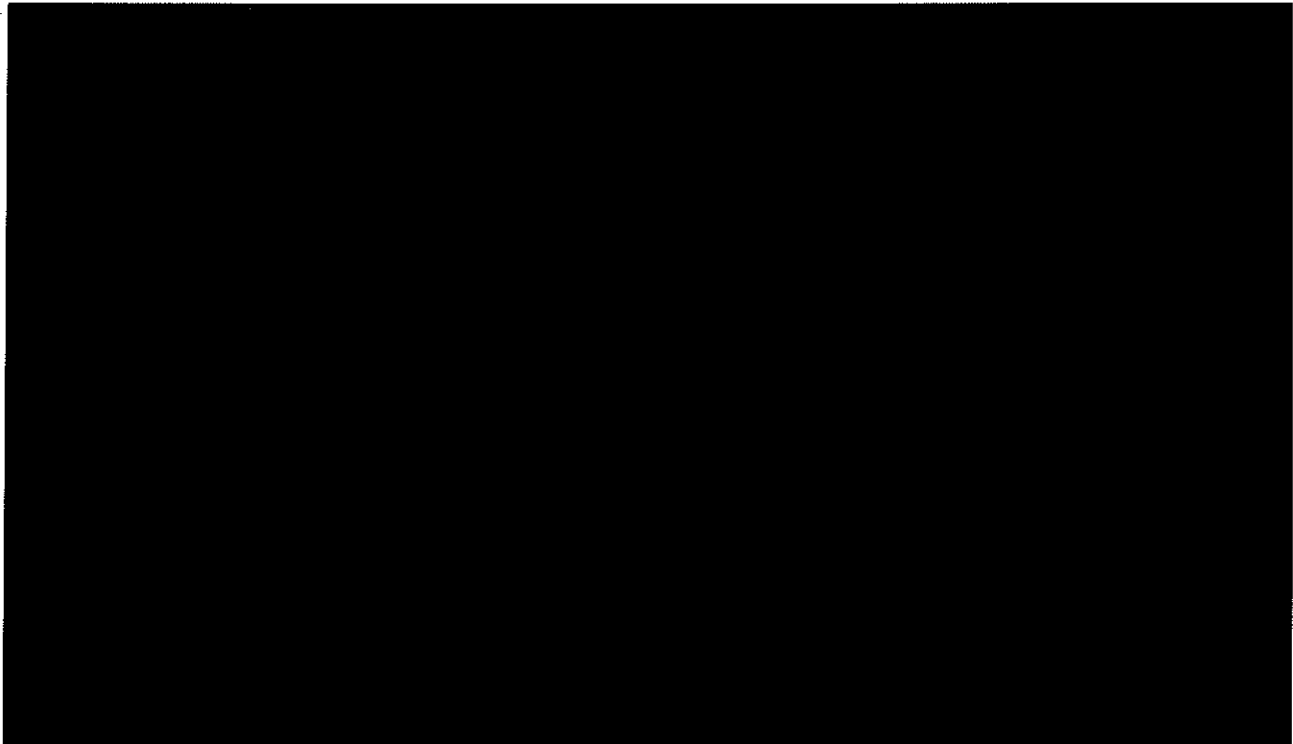
(S//OC/NF) Section 702 permits the Director of National Intelligence (DNI) and the Attorney General (AG) to authorize the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information," 50 U.S.C. § 1881a(a). As previously explained by the Government, the "targeting" of a person to acquire foreign intelligence information under section 702 is accomplished through the tasking of a facility that he/she uses. *See, e.g.,* [REDACTED]

[REDACTED] Government's Preliminary Responses to Certain Questions Posed by the Court (filed Aug. 26, 2008), at 3. Such acquisitions cannot intentionally target U.S. persons. 50 U.S.C. § 1881a(b), (g)(2)(A)(vii). The Government respectfully suggests that when [REDACTED]



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~



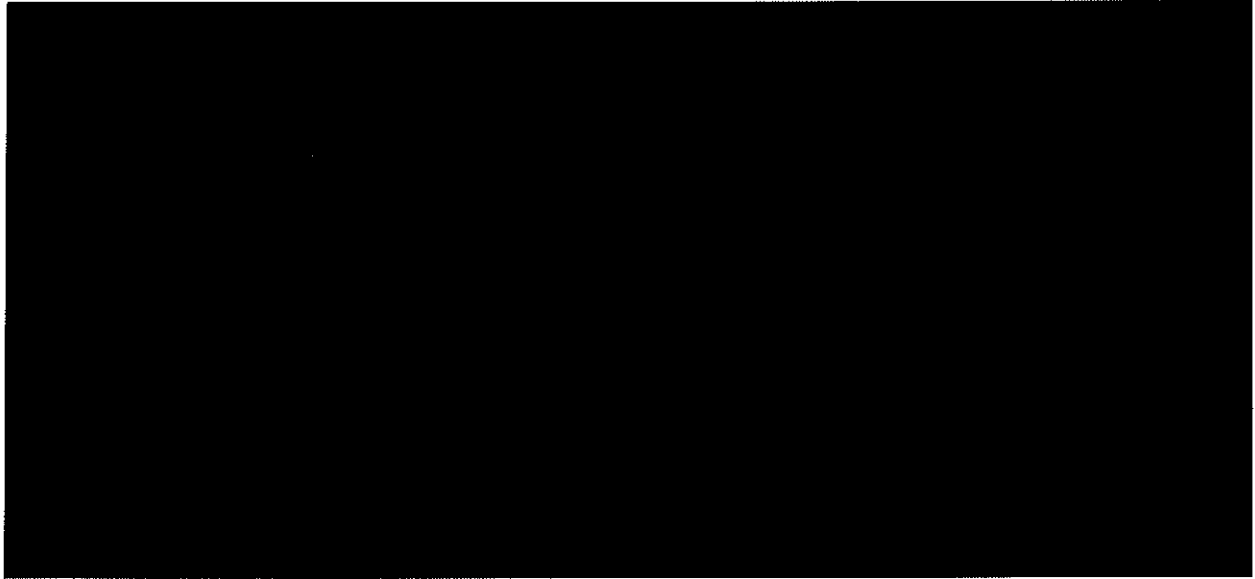
[REDACTED]. The Government therefore respectfully suggests that this change to the NSA targeting procedures is consistent with the requirements of the statute and the Fourth Amendment.

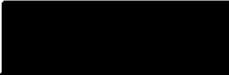
(S) The Government does not believe that this change to NSA's targeting procedures will affect the amount of time NSA takes to resolve [REDACTED] concerning section 702-tasked electronic communications [REDACTED] that may have been accessed from inside the United States. [REDACTED]

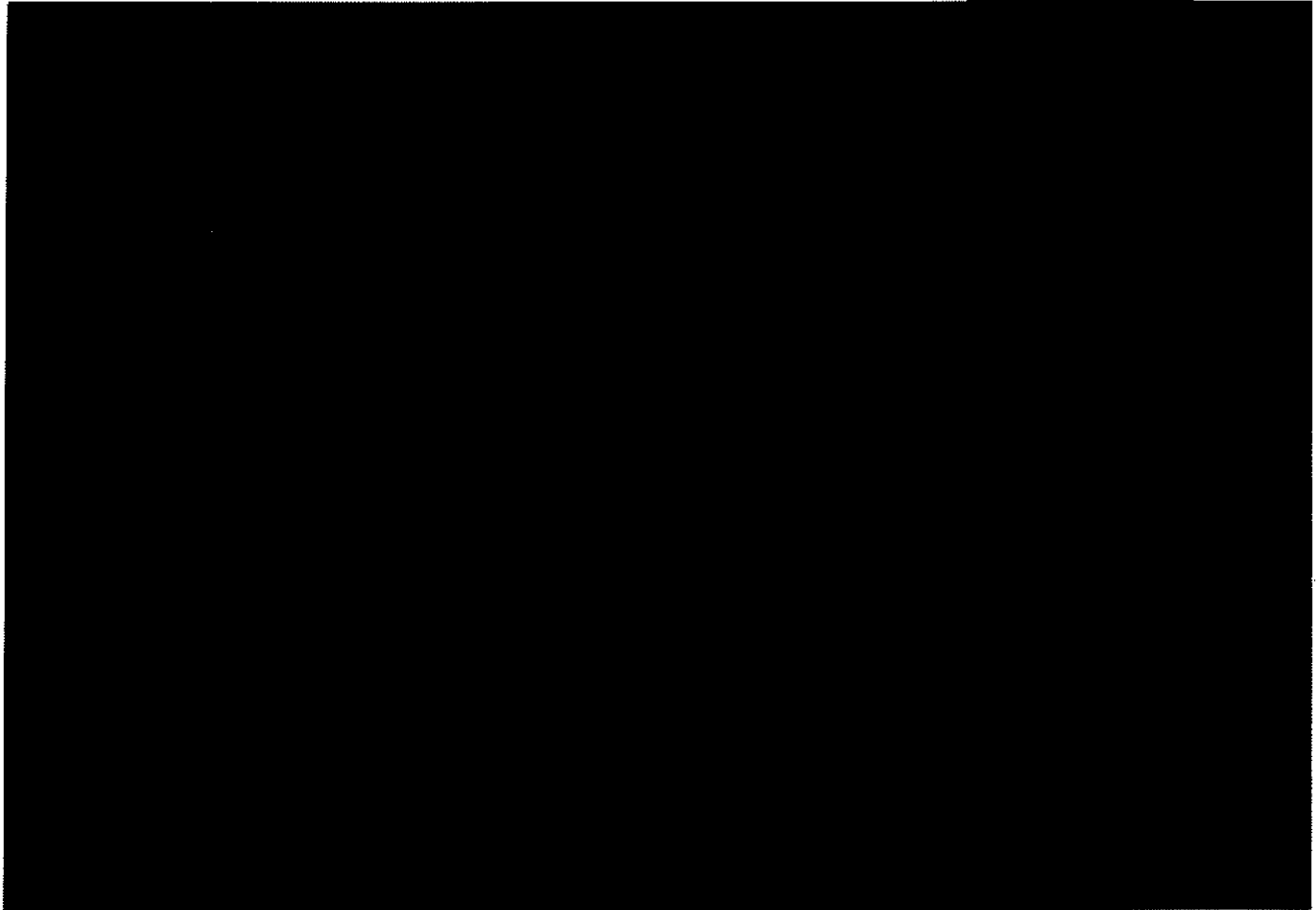


~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

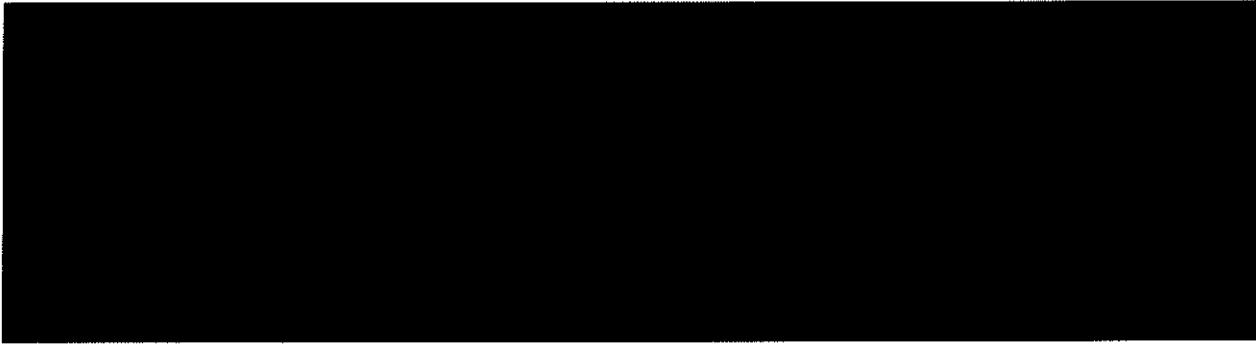


~~(S)~~ The NSA targeting procedures submitted as Exhibit A to 



~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



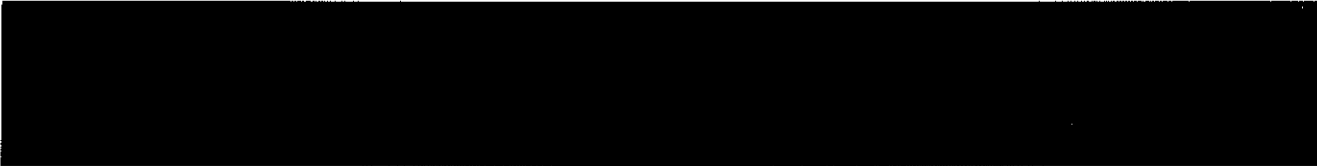
~~(S)~~ FBI's Targeting Procedures



~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~



~~(S)~~ **FBI's Minimization Procedures**

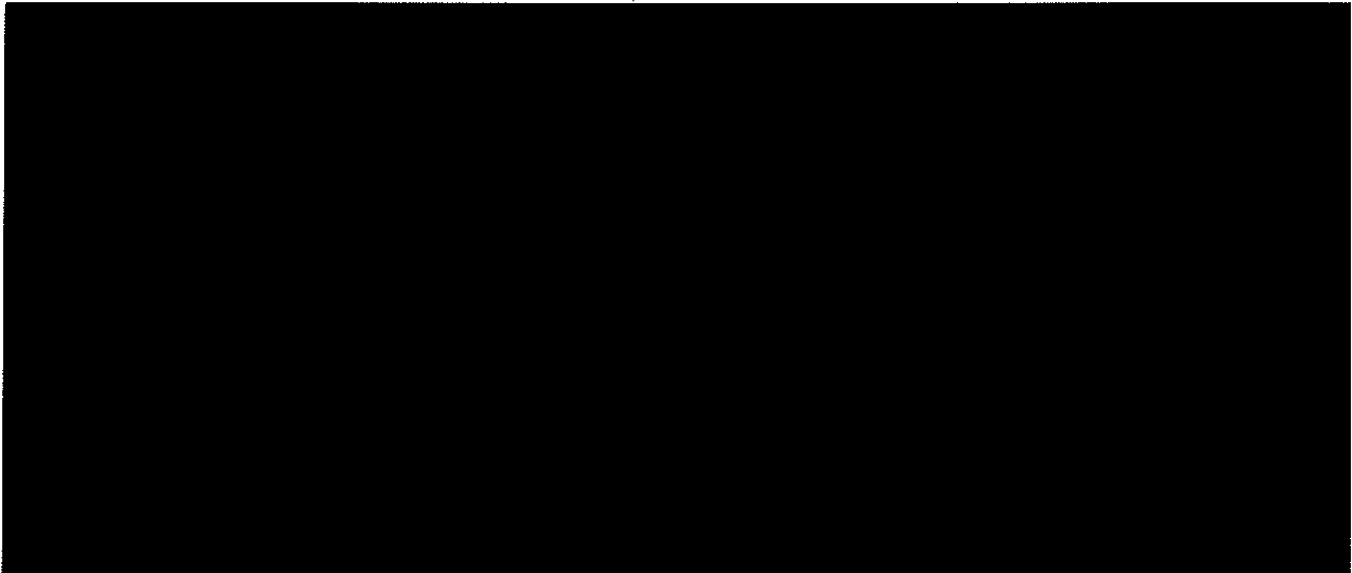
~~(S//NF)~~ The Government has filed with the Court a proposed motion to amend the Standard Minimization Procedures that the FBI applies in matters involving



These proposed amendments contain provisions governing the provision of information to the National Center for Missing and Exploited Children (NCMEC) and the retention of FISA-acquired information associated with litigation matters. The FBI minimization procedures submitted as Exhibit D to



contain substantially similar provisions, described in more



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

detail below.<sup>5</sup>

A. ~~(S//NF)~~ **Dissemination to the National Center for Missing and Exploited Children**

~~(S//NF)~~ The FBI minimization procedures submitted as Exhibit D to Certifications [REDACTED] permit the FBI to disseminate, for law enforcement purposes, section 702-acquired information that reasonably appears to be evidence of a crime related to child exploitation material, including child pornography, to NCMEC. The FBI minimization procedures also permit the FBI to disclose to NCMEC, for the purposes of obtaining technical or linguistic assistance, such FISA-acquired information for further processing and analysis.

~~(S//NF)~~ Through its investigations, the Government has identified and continues to identify section 702-acquired information the Government has determined to be indicative of a crime related to child exploitation material, including child pornography. NCMEC, established by Congressional mandate in 1984, is a private, non-governmental organization that today works in partnership with the Government to "help law enforcement find missing children, eliminate child sexual exploitation, and prevent child victimization." *About Us – Congressional Authorization*, NCMEC, <http://missingkids.com/Authorization> (last visited July 17, 2014). The Government

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

believes it has an obligation to share with NCMEC such section 702-acquired information as part of the Government's Project Safe Childhood initiative, which seeks to combat the proliferation of technology-facilitated crimes involving the sexual exploitation of children, including through the investigation and prosecution of offenders and involvement in prevention and deterrence. *About Project Safe Childhood*, U.S. Dep't of Justice, <http://www.justice.gov/psc/about-project-safe-childhood> (last visited July 17, 2014). The Government also believes it has an obligation to share such section 702-acquired information with NCMEC as part of the Government's National Strategy for Child Exploitation and Interdiction, which was formulated and implemented in response to the Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008 (the "PROTECT Our Children Act"). See U.S. Dep't of Justice, *Nat'l Strategy for Child Exploitation Prevention and Interdiction*, at 8-28, 93-95 (concerning NCMEC in detail); PROTECT Our Children Act of 2008, Pub. L. 110-401, 122 Stat. 4229 (2008).

~~(S//NF)~~ NCMEC has partnered with the Government to prevent and interdict in the sexual exploitation of children. One of the express purposes of the annual grant by Congress supporting NCMEC is for NCMEC to "operate a child victim identification program in order to assist the efforts of law enforcement agencies in identifying victims of child pornography and other sexual crimes." 42 U.S.C. § 5773(b)(1)(R). NCMEC,

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

through its Child Victim Identification Program, serves as the central repository in the United States for information that relates to child victims depicted in images and videos that are sexually exploitative. Child Victim Identification Program, Nat'l Center for Missing and Exploited Children, <http://www.missingkids.com/CVIP> (last visited July 17, 2014). The Child Victim Identification Program has a dual mission to (1) provide information relevant to child pornography investigations; and (2) assist in the identification of child victims depicted in pornographic images. *Id.* Law enforcement officers submit copies of seized child pornography images to law enforcement officers co-located at NCMEC on behalf of their respective agencies. Personnel at NCMEC review the seized images to determine which contain previously identified child victims. *Id.* NCMEC generates a Child Identification Report that includes contact information for the law enforcement agency that originally identified the child. *See generally* Michelle Collins (Vice President, Exploited Children Division and Assistant to the President of NCMEC), "Federal Child Pornography Offenses," Testimony Before the U.S. Sentencing Comm'n. (Feb. 15, 2012), at 3 (describing NCMEC's proprietary software), [http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-hearings-and-meetings/20120215-16/Testimony\\_15\\_Collins.pdf](http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-hearings-and-meetings/20120215-16/Testimony_15_Collins.pdf) (last visited July 17, 2014). NCMEC retains but does not otherwise disseminate or redistribute the images. However, with regard to any possible further disclosure by NCMEC, the FBI will advise

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

NCMEC of the need to comply with the restrictions described in Section IV.D of the FBI minimization procedures.

(S//NF) For the reasons provided, there is criminal investigative and analytic merit to the FBI sharing section 702-acquired information with NCMEC. As FISA's definition of "minimization procedures" makes clear, notwithstanding general protections afforded U.S. persons and U.S. person information, the minimization procedures may "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. § 1801(h); *see also* 50 U.S.C. § 1821(4), 50 U.S.C. § 1881a(e)(1). The Government respectfully submits that the FBI minimization procedures submitted as Exhibit D to [REDACTED]

[REDACTED] are consistent with the needs of the Government to prevent, investigate, and potentially prosecute violations of criminal statutes, find missing children, reduce the incidence of child sexual exploitation, and prevent child victimization.

**B. (S//NF) Retention of FISA-Acquired Information for Litigation-Related Reasons**

(S//NF) The FBI minimization procedures submitted as Exhibit D to Certifications [REDACTED] also address the [REDACTED]

[REDACTED] and the Government's need to

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

retain certain section 702-acquired information for litigation-related reasons. More specifically, the [REDACTED]

[REDACTED] any section 702-acquired information associated with FBI investigative case files that the Government determines must be retained because it may be necessary for, or potentially discoverable in, pending administrative, civil, or criminal litigation. [REDACTED]

[REDACTED]  
(S//NF) The FBI places FBI investigative case files on a "litigation hold" list—thus exempting them from destruction—if those case files relate to active litigation matters. In some instances, these investigative case files also contain information acquired pursuant to FISA. [REDACTED]

[REDACTED] notwithstanding its association with investigative case files subject to a "litigation hold." [REDACTED]

[REDACTED] To permanently address this issue, the [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]

[REDACTED] The Department of Justice and the FBI have developed a collaborative process to identify FISA information that should be retained for litigation-related reasons. In addition, the Government will report to the Court once per year about any FISA information retained pursuant to this provision. [REDACTED]

[REDACTED]

[REDACTED]

(S//NF) Similar to the [REDACTED] the FBI minimization procedures submitted as Exhibit D to Certifications [REDACTED] allow for the retention of section 702-acquired information associated with FBI investigative case files that there is a litigation-related reason to retain. The FBI section 702 minimization procedures exempt from [REDACTED] any section 702-acquired information that may be relevant to active litigation matters, and obviate the need for individual motions to the Court seeking exemption from the destruction requirements in individual cases. Any section 702-acquired information retained pursuant to the "litigation hold" provision will be identified through a collaborative process involving the Department of Justice and FBI, will be subject to access restrictions, and will be reported to the Court once per year.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

**C. ~~(S//NF)~~ Dissemination to Private Entities and Individuals of Foreign Intelligence Information or Evidence of a Crime Involving a Matter of Serious Harm**

~~(S//NF)~~ Finally, the FBI minimization procedures submitted as Exhibit D to Certifications [REDACTED] include a new provision that would allow the FBI to disseminate information to a private entity or individual in those cases in which that entity or individual "is capable of providing assistance in mitigating serious economic harm or serious physical harm to life or property." See Exhibit D, attached herewith, section V.I., at p. 33. This provision closely mirrors section V.H. of FBI's section 702 minimization procedures, which allows for similar disseminations to private entities and individuals who are capable of assisting in mitigating or preventing computer intrusions or attacks. The new provision addressing serious economic harm or serious harm to life or property has been added to allow the FBI to disseminate information to private entities or individuals in cases other than those involving computer intrusions or attacks, such as if the FBI discovered evidence in section 702-acquired data of credit card theft or a plot to destroy a building or monument. The Government submits that this dissemination provision is consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information and comports with the definition of minimization procedures set forth in 50 U.S.C. § 1881a(e)(1). This amendment is consistent with the legislative history of FISA, which

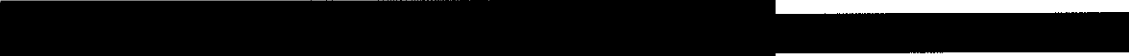
~~TOP SECRET//SI//ORCON/NOFORN~~

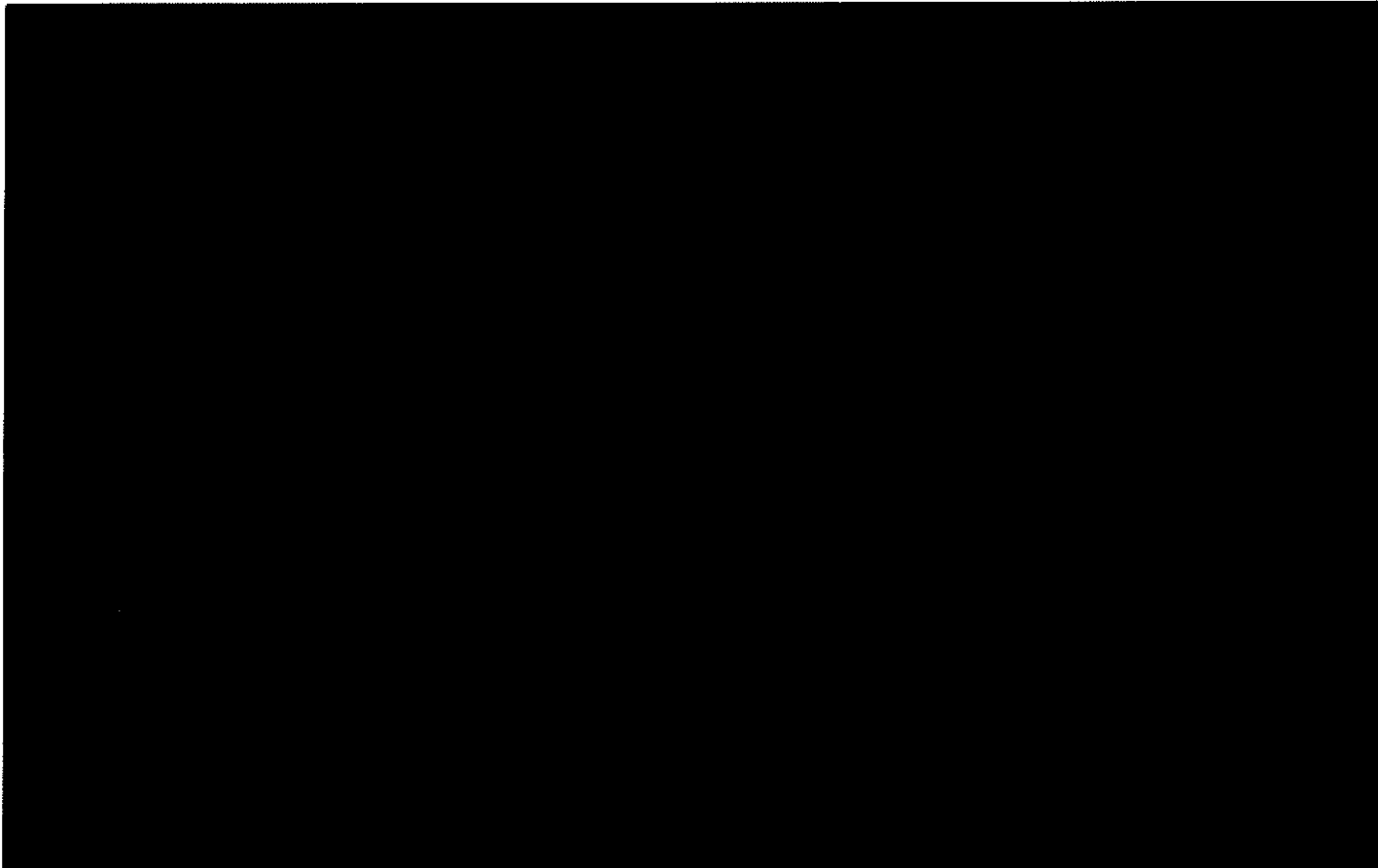


~~TOP SECRET//SI//ORCON//NOFORN~~

recognizes that some situations may require disclosure of FISA-acquired information outside of government channels. See H.R. Rep. 95-1283, at 88 (1978); S. Rep. 95-604, at 54 (1978).

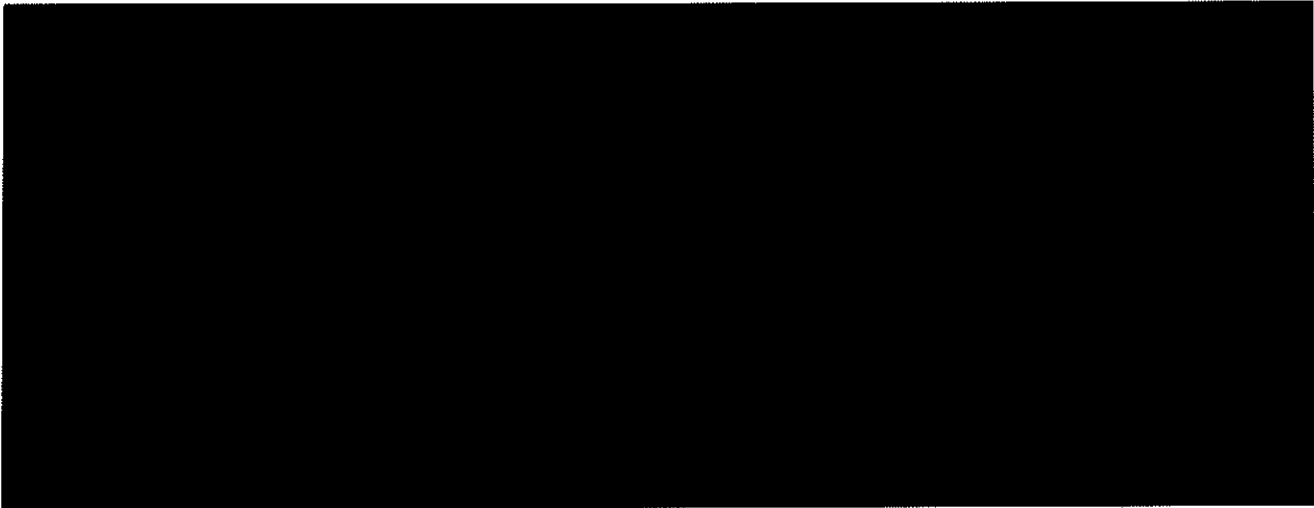
**(S) NSA and CIA's Minimization Procedures**

~~(S//NF)~~ As with the minimization procedures used by the FBI and discussed in further detail above, the Government has added language to the minimization procedures used by the NSA and CIA and submitted as Exhibits B and E, respectively, to 



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~



(S) The Resolution of [REDACTED] Indicating that a User May Be in the United States

(S//NF) Pursuant to Section II of NSA's section 702 targeting procedures, NSA conducts post-targeting analysis that includes routine checks of all section 702-tasked electronic communications [REDACTED] against available [REDACTED] [REDACTED] to determine which, if any, of such [REDACTED] may have been accessed from inside the United States. As previously described to the Court in a letter filed May 21, 2010 (noted above, and attached as Attachment C) and various subsequent compliance notices, NSA uses [REDACTED] as part of its process to implement and prioritize routine checks of all such tasked facilities for information indicative of potential access originating from the United States. Specifically, [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED] a significant volume

[REDACTED] are resolved as not indicative of [REDACTED]

[REDACTED] The volume of [REDACTED] varies, but NSA reports that, [REDACTED]

[REDACTED] on average more than [REDACTED] are typically generated each day (including from [REDACTED]), approximately [REDACTED] of which on average are further prioritized [REDACTED] as potentially indicative of access originating from the United States.<sup>6</sup> It is important to note that a single facility may generate [REDACTED] and not all [REDACTED] are indicative of compliance incidents.<sup>7</sup>

(S//NF) NSA has also implemented controls to ensure the timely and effective resolution of the [REDACTED] generated through the [REDACTED] post-tasking checks. First, [REDACTED]

[REDACTED]

<sup>6</sup> (S) Although the number fluctuates, NSA reports that for 2014 more than 90% of the [REDACTED] generated were false positives, i.e., not indicative of access of the facility by a user inside the United States.

<sup>7</sup> (S) For example, during the first week of June 2014, a total of approximately [REDACTED] that were subject to further analysis corresponded to approximately [REDACTED] facilities, resulting in approximately [REDACTED] reports of potential incidents being forwarded to the Department of Justice and the Office of the Director of National Intelligence.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

that are assessed to be

[REDACTED]

of a user inside the United States are immediately detasked. Second,

[REDACTED]

[REDACTED] Third,

[REDACTED]

[REDACTED]

[REDACTED]

\_\_\_\_\_

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

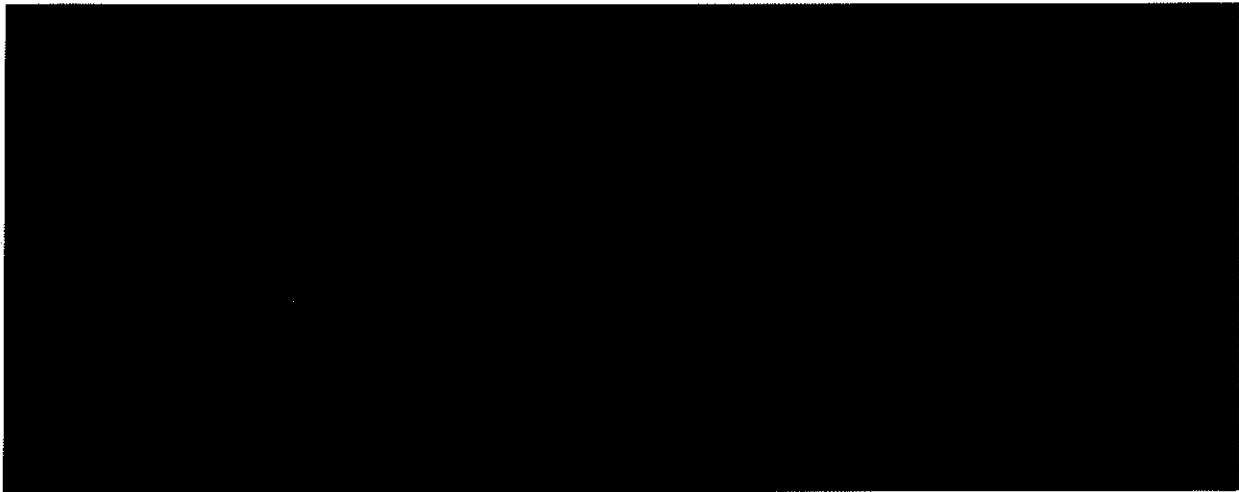
~~TOP SECRET//SI//ORCON//NOFORN~~

(S//NF) More specifically, depending on the circumstances of any given [REDACTED] and the totality of circumstances supporting NSA's reasonable belief that the target remains located outside the United States, further analysis may include:



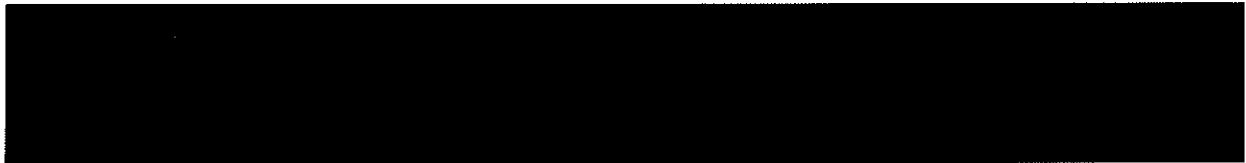
~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



(U) Conclusion

(S//OC/NF) [redacted] contain all of the elements required by the Act, and the targeting and minimization procedures submitted with these certifications are consistent with the requirements of the Act and the Fourth Amendment to the Constitution of the United States. Likewise, the amended minimization procedures to be used in connection with foreign intelligence information acquired in accordance with [redacted]



[redacted] are consistent with the requirements of the Act and the Fourth Amendment to the Constitution of the United States. Accordingly, the government respectfully requests that this Court enter orders pursuant to subsection 702(i)(3)(A) of the Act approving: [redacted] the use

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

of the targeting and minimization procedures attached thereto as Exhibits A, B, C, D, E, and G in connection with acquisitions of foreign intelligence information in accordance with those certifications; and the use of the minimization procedures attached as Exhibits B, D, and E to [REDACTED] in connection with foreign intelligence information acquired in accordance with [REDACTED]

[REDACTED]

Respectfully submitted,

John P. Carlin  
Assistant Attorney General

Stuart J. Evans  
Acting Deputy Assistant Attorney General

By:

(b)(6)  
[REDACTED]

(b)(6)  
Office of Intelligence  
National Security Division  
U.S. Department of Justice

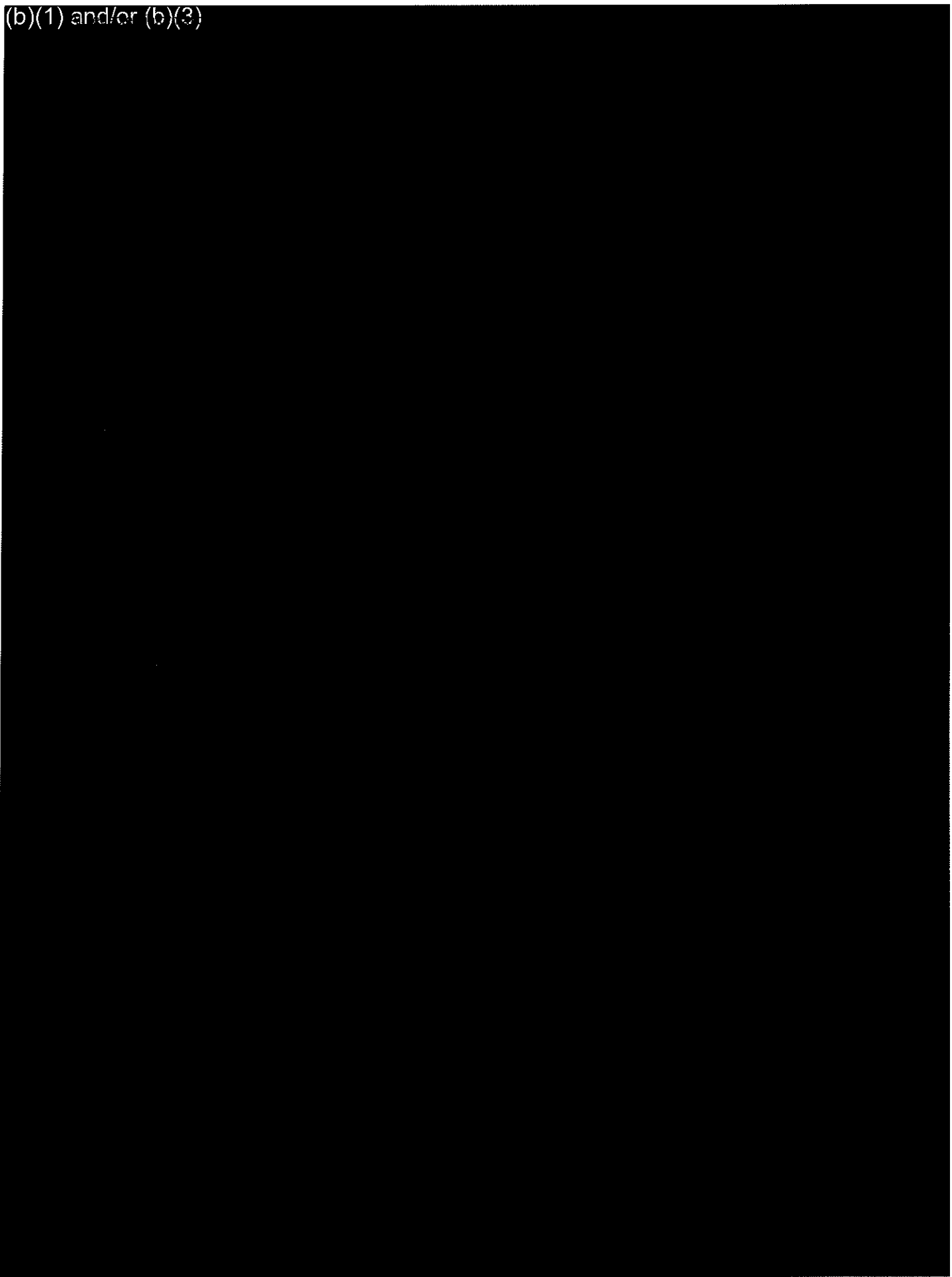
~~TOP SECRET//SI//ORCON//NOFORN~~

(b)(1) and/or (b)(3)





(b)(1) and/or (b)(3)



(b)(1) and/or (b)(3)



(b)(1) and/or (b)(3)



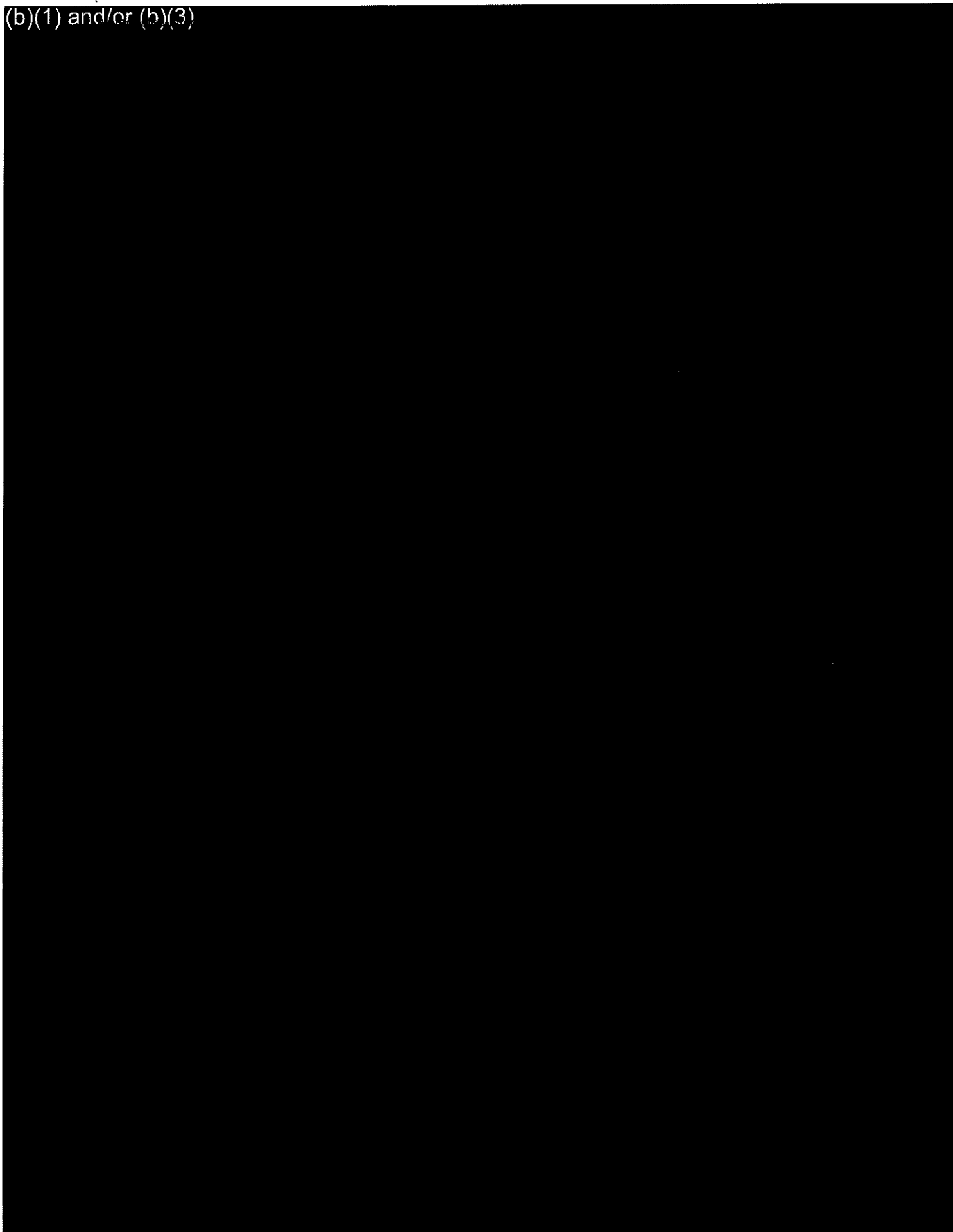
(b)(1) and/or (b)(3)



(b)(1) and/or (b)(3)



(b)(1) and/or (b)(3)



(b)(1) and/or (b)(3)



(b)(1) and/or (b)(3)





(b)(1) and/or (b)(3)



(b)(1) and/or (b)(3)



(b)(1) and/or (b)(3)



# ATTACHMENT A



U.S. Department of Justice

National Security Division

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

2012 JAN 11 PM 4:54

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

Washington, D.C. 20530

LEEANN FLYNN HALL  
CLERK OF COURT

January 11, 2012

The Honorable John D. Bates  
United States Foreign Intelligence Surveillance Court  
333 Constitution Avenue, N.W.  
Washington, D.C. 20001

Re: Supplemental Notice of Compliance Incidents  
Regarding Several Accounts Tasked Pursuant to  
Section 702 of FISA (S)

Dear Judge Bates:

Pursuant to Rule 13(b) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, effective November 1, 2010, this letter provides additional information regarding compliance incidents described in a letter filed on July 29, 2011. The July 29, 2011, letter notified the Court that the National Security Agency (NSA) had continued to direct acquisition under Section 702 at e-mail accounts of non-U.S. persons located outside the United States

[Redacted] (S)

Specifically, on June 27, 2011, NSA reported to the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) that

[Redacted] As detailed in the July 29 letter, [Redacted]

On July 6, 2011, NSA further reported that additional Section 702-tasked facilities had been accessed by [Redacted]. These incidents had not been previously reported to NSD or ODNI. In the July 29 letter, NSD and ODNI preliminarily assessed that NSA's failure to detask at least one of the additional facilities, when it knew the account was [Redacted] resulted in a detasking delay. In the Section 702 Quarterly Compliance Report filed with the Court on September 7, 2011, NSD provided an update, noting that further investigation had revealed that [Redacted] of these additional facilities did not involve compliance

<sup>1</sup> NSA tasked this account pursuant to [Redacted] or [Redacted] and collection continued pursuant to [Redacted] (S)

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

Classified by: Tashina Gauthar, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(e)  
Declassify on: 11 January 2037

[Redacted]

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

incidents because [redacted] all occurred prior to NSA's Section 702 tasking of these facilities. In both the July 29 letter and the Quarterly Report, NSA, NSD, and ODNI committed to conducting further analysis to determine whether other facilities [redacted]

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

NSA reports that it has examined all [redacted] of possible [redacted] received since NSA began acquiring communications pursuant to Section 702

[redacted]

The tasking of, or continued acquisition against, a selector used by a United States person under the circumstances discussed above is not specifically addressed nor permitted under NSA's Section 702 targeting procedures. While purging obligations would attach pursuant to Sections 3(d) and 5 of NSA's minimization procedures for [redacted] discussed above, a compliance incident would have occurred only in cases where Section 702 acquisition of a facility occurred either [redacted]

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

As a result of these incidents, NSA's Office of General Counsel has clarified that NSA will treat [redacted] as [redacted] of a Section 702 tasked facility by a United States person. Additionally, when NSA Oversight and Compliance personnel receive notices [redacted]

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

[redacted]

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

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

NSA is currently in the process of purging Section 702-acquired data [REDACTED] the above-described facilities. The Department of Justice will advise the Court of the status of all required purges in its next quarterly report to the Court regarding Section 702 compliance occurrences. (S)

Respectfully submitted,

(b)(6)

/ Kevin J. O'Connor  
Chief, Oversight Section  
Office of Intelligence, NSD  
U.S. Department of Justice

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

## **ATTACHMENT B**





U.S. Department of Justice

National Security Division

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

2014 JAN 29 PM 12: 04

~~TOP SECRET//SI//NOFORN~~

Washington, D.C. 20530

LEEANN FLYNN HALL  
CLERK OF COURT

January 29, 2014

The Honorable Reggie B. Walton  
United States Foreign Intelligence Surveillance Court  
333 Constitution Avenue, N.W.  
Washington, D.C. 20001

Re: ~~(S)~~ Notice of Compliance Incident Regarding  
Section 702 Targeting

Dear Judge Walton:

~~(TS//SI//NF)~~ Pursuant to Rule 13(b) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, effective November 1, 2010, this letter provides notice of a compliance incident. Specifically, on January 14, 2014, the National Security Agency (NSA) reported to the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ

Reason: 1.4(c)

Declassify on: 29 January 2039

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~(TS//SI//NF)~~ NSA is required under its current targeting procedures to detask facilities from Section 702 acquisition for points in time when, *inter alia*, NSA is aware that the targeted person is inside the United States or is a United States person. The Government understands this to include points in time when the facilities will be [REDACTED]. See, e.g., Supplemental Notice of Compliance Incidents Regarding Several Accounts Tasked Pursuant to Section 702 of FISA, filed on January 11, 2012. [REDACTED]

~~(TS//SI//NF)~~ In [REDACTED] NSA identified training issues related to such [REDACTED] Section 702-tasks facilities. While certain NSA personnel who task facilities to Section 702 acquisition were aware of the need to detask accounts tasked for Section 702 acquisition when they were aware that [REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~



(S) NSA, NSD, and ODNI are continuing to investigate this issue. The Department of Justice will include this issue in its quarterly report to the Court regarding Section 702 compliance occurrences.

(U) NSA has reviewed this letter and confirmed its factual accuracy.

Respectfully submitted,

Kevin J. O'Connor  
Chief, Oversight Section  
Office of Intelligence, NSD  
U.S. Department of Justice

~~TOP SECRET//SI//NOFORN~~

## ATTACHMENT C

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



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

May 21, 2010

The Honorable Mary A. McLaughlin  
Judge  
United States Foreign Intelligence Surveillance Court  
Washington, D.C.

Dear Judge McLaughlin:

I am pleased to provide certain additional information related to certain issues raised and discussed during our meeting on May 17, 2010, concerning the matters currently pending before the Court in [REDACTED]

(S)

Identification of [REDACTED] Information within NSA Systems (S)

As the Court is aware from the testimony provided by the government on April 22, 2010, and from supplemental information provided to the Court on May 10, 2010, the National Security Agency (NSA) stores unminimized and unevaluated signals intelligence (SIGINT) data in its [REDACTED]

[REDACTED] For the reasons more fully explained in our May 10, 2010 submission, the government has proposed separate and distinct purge requirements for each class of information. (TS//SI//NF)

According to NSA, certain of its systems contain multiple classes of information, For example, [REDACTED]

(TS//SI//NF)

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

**Classified by:** David S. Kris, Assistant Attorney General, NSD, DOJ  
**Reason:** 1.4(c)  
**Declassify on:** 21 May, 2035

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

The Resolution of [redacted] (S) —

On Friday, May 7, 2010, the government submitted to the Court its Supplemental Report Regarding NSA's Post-Targeting Analysis. Following its review of the report, the Court expressed concern that allowing [redacted] to go unresolved for an extended period of time may not be consistent with NSA's targeting procedures, which specifically provide that [redacted]

[redacted]

(TS//SI//NF) —

As noted in the government's May 7, 2010 Supplemental Report, [redacted] NSA conducts [redacted]

[redacted] allows NSA to quickly identify [redacted] of a target's presence in the U.S. Those [redacted]

NSA recently established new deadlines in the [redacted] process to ensure consistency in the management of this process given the diversity of targets and reasons for [redacted]. To ensure that [redacted] do not go unresolved for an unreasonable period of time, NSA has imposed a new deadline requiring that [redacted]

[redacted] (TS//SI//NF) —

NSA reports that on average it receives [redacted] through [redacted]. For example, during [redacted] selectors generated a total of [redacted] resulting in [redacted] incident (roaming) reports being forwarded to the Department of Justice and the Office of the Director of National Intelligence. [redacted] continue to be researched. Given the procedures in place as outlined in the government's May 7, 2010 Supplemental Report which are designed to identify, prioritize and resolve those [redacted] having a [redacted] a target's presence in the United States, the government believes that [redacted] is reasonable.

(TS//SI//NF)

NSA intends to provide the Court with further updates regarding [redacted] as well as its efforts to remediate the purge compliance issue on or before Wednesday, May 26, 2010.

(TS//SI//NF)

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

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

The government would like to thank both you and your staff for your consideration of the government's Certification. Should the Court have any additional questions, comments or concerns, please do not hesitate to contact me. (U)

Sincerely,



(b)(6)

Office of Intelligence

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



U.S. Department of Justice

National Security Division

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

2014 MAR 18 PM 4:41

~~SECRET~~

Washington, D.C. 20530

LEEANN FLYNN HALL  
CLERK OF COURT

March 18, 2014

The Honorable Reggie B. Walton  
United States Foreign Intelligence Surveillance Court  
333 Constitution Avenue, N.W.  
Washington, D.C. 20001

Re: (S) Notice of NSA's Assessment of Purge Practices  
and Discovery of Incomplete Purges

Dear Judge Walton:

(S) In describing its remedial efforts regarding most compliance incidents, the Government reports to the Court regarding when data has been purged from Government systems. On January 16, 2014, the National Security Agency (NSA) reported to the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) that two studies of NSA's purge practices (in 2011 and 2012, respectively) had identified incompletely purged data.<sup>1</sup> The purge studies were conducted to verify and improve NSA's purge protocol, which was extensively briefed to the Court in 2010. The purge studies identified a small percentage of communications that had been added to NSA's Master Purge List (MPL), but had not been purged from all relevant NSA systems. The incomplete purges appear to have resulted from mistakes in [redacted] aspects of the purge process.

(S) In 2011, NSA's Office of the Director of Compliance led a purge verification study by taking a sample of [redacted] identifiers that had been added to the MPL [redacted] to identify whether the underlying objects had in fact been purged from NSA's [redacted] storage systems. NSA identified [redacted] objects from that sample that had not been initially purged [redacted]. The [redacted] objects were associated with a total of [redacted] different incidents where a purge was required. [redacted]

[redacted] NSA advises that it cannot confirm when it completed its reexecution of the purges to remove these [redacted] objects from its systems, but can confirm that as of [redacted] all objects have been removed from NSA systems.

<sup>1</sup> (S) NSA's report was the result of NSD follow-up questions in reference to a recommendation made in a March 2013 NSA Office of the Inspector General report regarding [redacted] NSA's purge processes.

~~SECRET~~

Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(e)  
Declassify on: March 18, 2039





~~SECRET~~

(S) In 2012, NSA's Oversight and Compliance section led a similar purge verification study using a sample of [redacted] unique identifiers added to the MPL between [redacted] NSA identified [redacted] records related to one event that had not been purged [redacted]

The communications were purged from the [redacted] in [redacted]

(S) Although the communications described above were not initially purged from certain NSA systems as intended, the unique identifiers of these objects were on NSA's MPL to prevent use in NSA reporting, in FISA applications, or to target pursuant to Section 702.

(S) NSA has made efforts and continues to make efforts to improve its purge processes. Furthermore, as discussed in the Quarterly Report, in addition to its standard purge discovery process, NSA has implemented several supplemental processes to [redacted] any data that is identified is removed from NSA systems upon discovery. See Quarterly Report to the Foreign Intelligence Surveillance Court Concerning Compliance Matters Under Section 702 of the Foreign Intelligence Surveillance Act, December 2013, n. 8; see also Semiannual Report of the Attorney General Concerning Acquisitions Under Section 702 of the Foreign Intelligence Surveillance Act, September 2012, n. 12.

(S) The Department of Justice will include this issue in its quarterly report to the Court regarding Section 702 compliance occurrences.

Respectfully submitted,

(b)(6)

Kevin J. O'Connor  
Chief, Oversight Section  
Office of Intelligence, NSD  
U.S. Department of Justice

~~SECRET~~



U.S. Department of Justice

National Security Division

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

2014 MAY 29 PM 4:44

~~SECRET//REL TO USA, FVEY~~

Washington, D.C. 20530

LEARN FLYNN HALL  
CLERK OF COURT

May 29, 2014

The Honorable Thomas F. Hogan  
United States Foreign Intelligence Surveillance Court  
333 Constitution Avenue, N.W.  
Washington, D.C. 20001

Re: (U//~~FOUO~~) Supplemental Notice of NSA's Assessment of Purge Practices and Discovery of Incomplete Purges

Dear Judge Hogan:

(U//~~FOUO~~) As part of its overall compliance program, the National Security Agency (NSA) conducts periodic reviews to verify the efficacy of its compliance activities, to include the process the Agency uses to effect purges undertaken for compliance purposes. On March 18, 2014, the Government filed a notice with the Court describing two NSA purge verification studies conducted in 2011 and 2012. The studies determined that some information that NSA personnel had identified for purge and placed on NSA's Master Purge List (MPL) had not been completely purged when the studies were conducted. As described below, the information was subsequently purged.

(S//~~REL TO USA, FVEY~~) In the March 2014 notice, the Government explained that the purge verification studies conducted in 2011 and 2012 were done by taking a sample of [redacted] unique identifiers that had been added to the MPL between certain time periods to identify whether the underlying objects had in fact been purged from [redacted] storage systems. Subsequent to the filing of the March 2014 notice, the Court requested that the Government provide an explanation as to why the studies were conducted in 2011 and 2012, but the notification to the Court regarding the incomplete purges was delayed until March, 2014. This supplemental notice responds to the Court's question, as well as provides additional information regarding the 2011 and 2012 purge verification studies and informs the Court of the results of the additional purge verification studies NSA's Signals Intelligence Directorate Office of Oversight and Compliance has conducted.

~~SECRET//REL TO USA, FVEY~~

Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ

Reason: 1.4(e)

Declassify on: May 29, 2039



~~SECRET// REL TO USA, FVEY~~

~~(S//REL TO USA, FVEY)~~ By way of background, NSA created the MPL and its internal purge process to provide reasonable assurance that NSA purges information consistent with its authorities and representations to the Court, as well as to ensure that personnel do not rely on information that was supposed to have been purged when preparing SIGINT reports or applications to the Court. *See, e.g.*, NSA Memorandum to the Assistant Attorney General, National Security Division (NSD), Department of Justice, as filed with the Court on March 16, 2010.<sup>1</sup>

(U//~~FOUO~~) Following NSA's February 2011 continued confidence letter to the Court, the Director of Compliance initiated a [redacted] activity designed to further study the effectiveness of existing internal controls for purge. From a sample size of [redacted] unique identifiers, NSA identified [redacted] objects that had not been purged but which were listed on the MPL. [redacted] NSA advises that the [redacted] was designed and conducted using statistical sampling in accordance with industry standards for internal auditing. The [redacted] did not represent an exhaustive review of the purge process, or of NSA's purge improvement activities, but rather was a study to provide reasonable assurance that NSA is purging data in compliance with governing laws and policies.

(U//~~FOUO~~) The [redacted] study [redacted]

[redacted] the report also noted that additional checks provide a reasonable assurance that incompletely purged objects are prohibited from further use. NSA has advised that each of the [redacted] identified objects were purged as of September 2013.

<sup>1</sup> ~~(S//REL TO USA, FVEY)~~ [redacted]

<sup>2</sup> ~~(S//REL TO USA, FVEY)~~ [redacted]

~~SECRET// REL TO USA, FVEY~~

~~SECRET//REL TO USA, FVEY~~

~~(S//REL TO USA, FVEY)~~ In addition to the [REDACTED] conducted by NSA's Director of Compliance, NSA's O&C section conducts compliance studies to verify the continued efficacy of, and, where appropriate, improve NSA's compliance processes, to include the purge process. NSA conducted purge verification studies in 2012, 2013, and 2014.<sup>3</sup> The 2012 through 2014 purge verification studies concluded that there have been improvements in the purge process.<sup>4</sup>

[REDACTED]

NSA did not identify any incomplete purges during this 2013 study and again concluded that the purge process was working and had improved.

~~(S//REL TO USA, FVEY)~~ In addition, on April 1, 2014, NSA completed a purge verification study of the [REDACTED] previously described to the Court.

[REDACTED]

~~(S//REL TO USA, FVEY)~~ In March 2013, NSA's Office of the Inspector General issued a report that, among other things, identified several instances where NSA's [REDACTED] purge processes could potentially result in incomplete purges [REDACTED] and recommended [REDACTED] NSA's purge processes. In response to that report, in March 2013, NSD requested further information from NSA regarding whether NSA had identified any instances of purge completions that have been reported to the Court where the underlying information was later identified to not have been fully purged from [REDACTED]. Following subsequent inquiries from NSD and ODNI, NSA responded to NSD's question in January 2014, and reported to NSD and ODNI the purge verification study information that was described in the March 18, 2014, notice to the Court.<sup>5</sup> In response to this Court's question asking why NSA had not previously informed

<sup>3</sup> ~~(S//REL TO USA, FVEY)~~ All of the purge studies from 2012, 2013, and 2014 included [REDACTED]

<sup>4</sup> ~~(S//REL TO USA, FVEY)~~ NSA provided the 2011-2014 reports to NSD on May 16, 2014. Therefore, NSD and the Office of the Director of National Intelligence (ODNI) are continuing to review the results of the reports with NSA and will provide additional updates to the Court as appropriate.

<sup>5</sup> ~~(U//FOUO)~~ On January 31, 2014, NSD and ODNI sent a draft notice to NSA regarding the 2011 and 2012 purge verification studies. NSA sent comments to NSD and ODNI regarding that draft notice on March 13, 2014. NSA

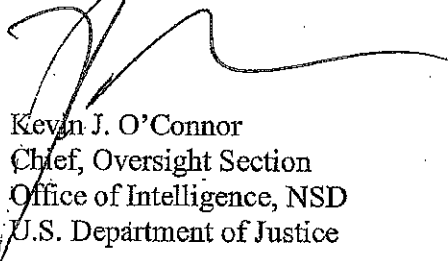
~~SECRET//REL TO USA, FVEY~~

~~SECRET//REL TO USA, FVEY~~

NSD of these incomplete purges, NSA advises that, since it had not identified any instance where items listed on the MPL had been used in a manner contrary to NSA's prior representations, NSA personnel did not think there was a compliance issue that needed to be reported to the Court. Rather, it appeared the safeguards built into the purge process had worked as intended since the studies did not identify any improper use of material that was subject to a purge requirement. NSA has committed to providing NSD and ODNI with details about any instances in which NSA discovers incomplete purges so that NSD can promptly notify the Court.

~~(S//REL TO USA, FVEY)~~ NSA will continue to keep NSD, ODNI, and the Court informed of its efforts to verify and improve the purge process and will more promptly advise NSD and ODNI of such efforts. In addition, NSD and ODNI will continue to review the results of the 2011 through 2014 purge verification studies with NSA. NSA has reviewed this letter and confirmed its accuracy.

Respectfully submitted,



Kevin J. O'Connor  
Chief, Oversight Section  
Office of Intelligence, NSD  
U.S. Department of Justice

---

advised that between January 21, 2014 and March 13, 2014, NSA was confirming the facts of the 2011 and 2012 purge results.

~~SECRET//REL TO USA, FVEY~~



U.S. Department of Justice

National Security Division

~~TOP SECRET//SI//NOFORN~~

Washington, D.C. 20530

July 25, 2014

The Honorable Thomas F. Hogan  
United States Foreign Intelligence Surveillance Court  
333 Constitution Avenue, N.W.  
Washington, D.C. 20001

Re: (U//~~FOUO~~) Notice Regarding NSA Purge Practices

Dear Judge Hogan:

~~(S//REL TO USA, FVEY)~~ This letter provides information regarding gaps in the process by which the National Security Agency (NSA) has effectuated purges. Specifically, in April and May, 2014, NSA reported to the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) inconsistencies in the manner in which NSA purged data from NSA repositories that had been designated as [REDACTED]

~~(TS//SI//NF)~~ As previously described to the Court, any system designated by NSA [REDACTED] must employ a purge protocol to verify that information is purged when the system receives a request to destroy SIGINT information that NSA is not authorized to retain. *See, e.g., In re DNI/AG Certification* [REDACTED] Docket No. [REDACTED] Affidavit of the Director of NSA, filed on May 10, 2010. In the following activities, undertaken as part of NSA's ongoing efforts to identify and resolve issues with its purge process, NSA identified specific objects that were subject to compliance purges but were not purged from [REDACTED]

- ~~(TS//SI//NF)~~ On or before [REDACTED] NSA identified an issue with respect to how information was being purged from [REDACTED]

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ

Reason: 1.4(c)

Declassify on: July 25, 2039

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

NSA corrected this issue

- (TS//SI//NF) On [redacted] as part of a routine activity [redacted]

NSA has confirmed that the approximately [redacted] objects have been removed from [redacted]

- (TS//SI//NF) On [redacted] as a result of [redacted]

The Government will further update the Court on the root causes of the incomplete purges [redacted]

<sup>1</sup> (S//NF) [redacted]

<sup>2</sup> (U//FOUO) NSD notified the Court of this [redacted]

<sup>3</sup> (S//NF) [redacted]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(TS//SI//NF) Separate from the [redacted] purge activities, NSA discovered

[redacted]

[redacted] NSA has corrected the [redacted] error and has purged the above-identified [redacted] objects [redacted]

(TS//SI//NF) NSA is certain that objects [redacted] were not used in NSA reporting, FISA applications, or FAA Section 702 targeting.

[redacted] To the extent that NSA identifies any data subject to purge in any of these ways, NSA will promptly notify NSD and ODNI.

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

[redacted]

~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

(U//~~FOUO~~) NSA has reviewed this letter and confirmed its accuracy. The Department of Justice will continue to provide further information to the Court regarding these matters.

Respectfully submitted,

(b)(6)

Kevin J. O'Connor  
Chief, Oversight Section  
Office of Intelligence, NSD  
U.S. Department of Justice

~~TOP SECRET//SI//NOFORN~~

~~SECRET//NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

**AFFIDAVIT OF JAMES B. COMEY  
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION**

2014 JUL 28 PM 3:57

[REDACTED]

COURT

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

(S//NF) Pursuant to subsection 702(g)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "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//NF) 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] ("Designated Accounts") 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]

[REDACTED]

2. (S//NF) 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] [REDACTED] electronic communication service providers; and a significant purpose of the acquisition is to obtain foreign intelligence information.

3. (S//NF) 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 Designated Account 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 Designated Accounts from the electronic communication service provider to the Central

Derived From: Multiple Sources-  
Declassify On: July 17, 2039

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Intelligence Agency (CIA) in unminimized form without performing any further processes or procedures to ensure that the user of the Designated Account 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.

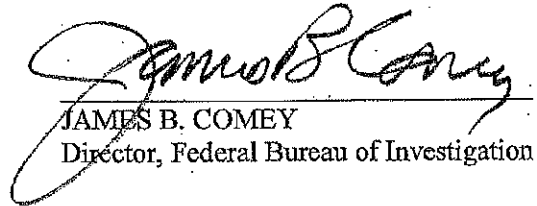
5. ~~(S//NF)~~ The minimization procedures that the FBI will use with respect to any [REDACTED] [REDACTED] it acquires pursuant to the above-referenced certification are attached herewith as Exhibit D.
6. ~~(S//NF)~~ Under the FBI minimization procedures attached herewith as Exhibit D, the FBI may provide the National Counterterrorism Center (NCTC) with access to terrorism-related FISA-acquired information, including minimized information obtained pursuant to section 702 of the Act, through the FBI's general indices (such as the Automated Case Support System (ACS), Sentinel, or successor systems). NCTC does not have a law enforcement function, and therefore the FBI is not permitted to disseminate FISA-acquired information to NCTC that is solely evidence of a crime and not foreign intelligence information. The minimization procedures that NCTC will use with respect to any section 702-derived information that it obtains from FBI that is evidence of a crime, but not foreign intelligence information, which are attached herewith as Exhibit G, were submitted for approval to the Foreign Intelligence Surveillance Court (FISC) in connection with [REDACTED] on July 31, 2013, and were approved by the FISC on August 30, 2013. NCTC will not collect any information pursuant to FISA, and the attached minimization procedures do not permit NCTC to receive unminimized information acquired pursuant to section 702 of the Act.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

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

Signed this 10<sup>th</sup> day of July, 2014.

  
\_\_\_\_\_  
JAMES B. COMEY  
Director, Federal Bureau of Investigation

~~SECRET//NOFORN~~

~~TOP SECRET//SI//NOFORN//20320108~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

**AFFIDAVIT OF RICHARD H. LEDGETT, JR., ACTING DIRECTOR,  
NATIONAL SECURITY AGENCY**

2014 JUL 28 PM 3: 57

[REDACTED]

HALL  
U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

**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 are attached herewith as Exhibit A.
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]

[REDACTED]

**Derived From: NSA/CSSM 1-52**

**Dated: 20070108**

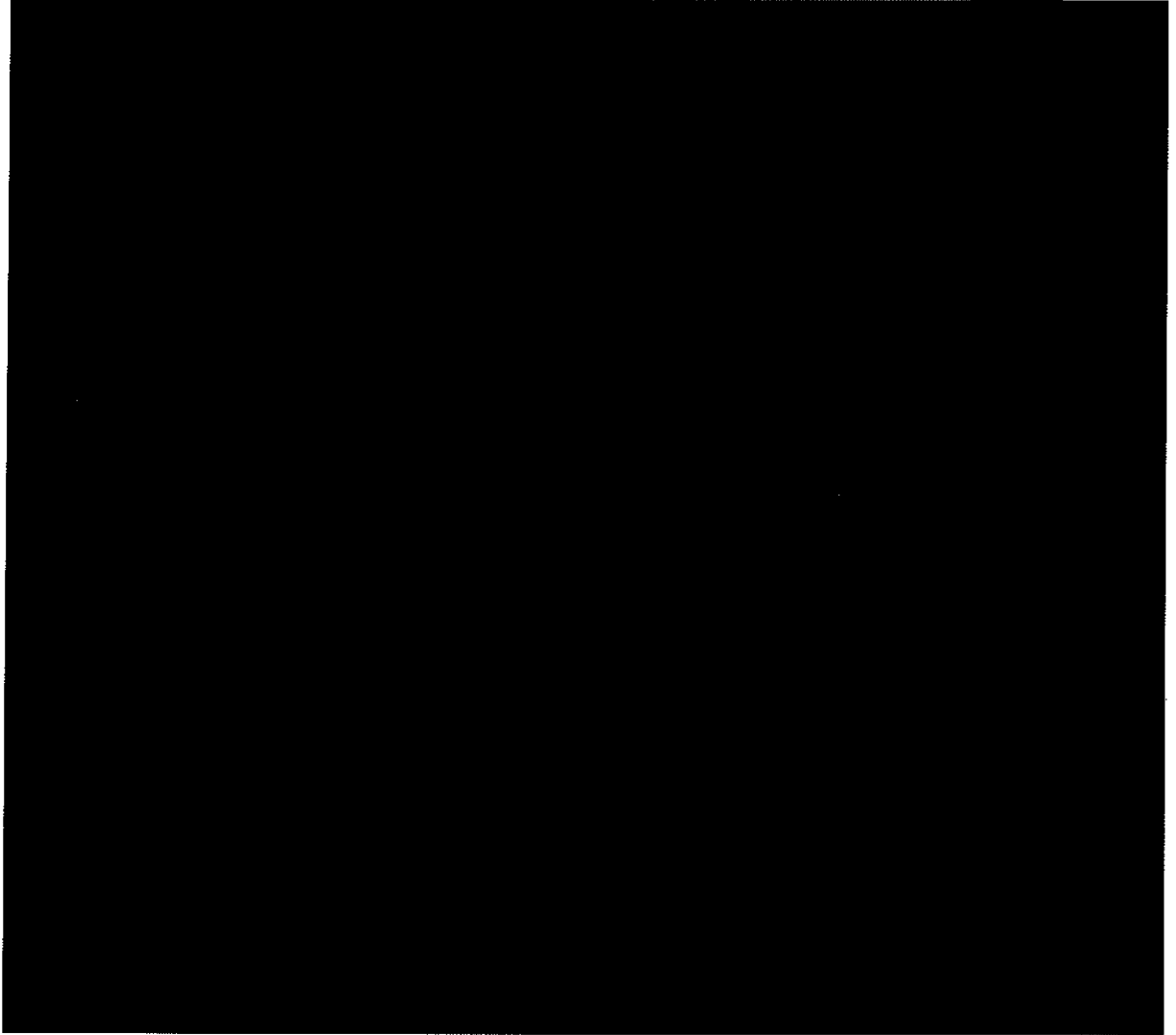
**Declassify On: 20320108**

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~



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



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

 NSA believes that the non-United States persons reasonably believed to be located outside the United States who will be targeted

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

for acquisition under this certification possess, are expected to receive, and/or are likely to communicate foreign intelligence information concerning [REDACTED]. Thus, a significant purpose of this 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 [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.
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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

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//SI//NOFORN//20320108~~



~~TOP SECRET//SI//NOFORN//20320108~~

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

Signed this 23<sup>rd</sup> day of July, 2014.



---

RICHARD H. LEDGETT, JR.  
Acting Director, National Security Agency

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET~~ //NOFORN//20390721

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

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

2014 JUL 28 PM 3:57

[REDACTED]

LEEANN FLYNN HALL  
CLERK OF COURT

[REDACTED]

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

1. (S//NF) 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. CIA's mission 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]

[REDACTED]

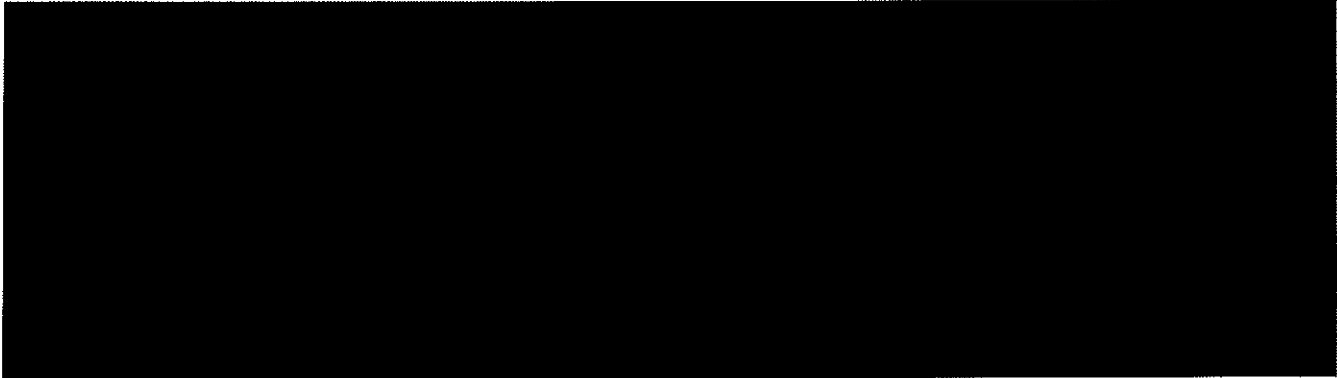
[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET~~ //NOFORN//20390721

~~TOP SECRET// [REDACTED]//NOFORN//20390721~~



5. (U) I have reviewed the minimization procedures attached herewith as Exhibit E. CIA will follow these minimization procedures with respect to any unminimized communications it receives from NSA and FBI acquired pursuant to the above-referenced certification.

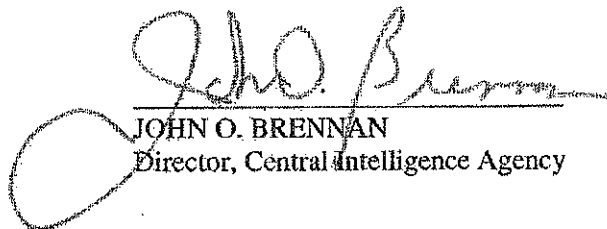
*--- The remainder of this page intentionally left blank ---*

~~TOP SECRET// [REDACTED]//NOFORN//20390721~~

~~TOP SECRET//[REDACTED]//NOFORN//20390721~~

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

Signed this 23<sup>rd</sup> day of July, 2014.



JOHN O. BRENNAN  
Director, Central Intelligence Agency

~~TOP SECRET//[REDACTED]//NOFORN//20390627~~

~~SECRET//ORCON/NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
COURT

**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**

2014 JUL 23 PM 3: 57



LYNN HALL  
OF COURT

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

~~(S//OC/NF)~~ 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 Richard H. Ledgett, Jr., Acting Director of the National Security Agency (NSA), James B. Comey, Director of the Federal Bureau of Investigation (FBI), and John O. Brennan, 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:

- (1) ~~(S)~~ there are procedures in place that will be submitted with this certification for approval by the Foreign Intelligence Surveillance Court<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> ~~(S//OC/NF)~~ Specifically, the NSA and FBI targeting procedures attached herewith as Exhibits A and C, respectively, will be submitted for approval by the Court.

~~SECRET//ORCON/NOFORN~~

Classified by: The Attorney General  
Reason: 1.4(c)  
Declassify on: 24 July 2039

~~SECRET//ORCON/NOFORN~~

- (2) ~~(S)~~ 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>2</sup> or will be submitted with this certification for approval by the Foreign Intelligence Surveillance Court;<sup>3</sup>
- (3) ~~(S)~~ 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) ~~(S)~~ 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) ~~(S)~~ a significant purpose of the acquisition is to obtain foreign intelligence information;
- (6) ~~(S)~~ the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
- (7) ~~(S)~~ the acquisition complies with the limitations in subsection 702(b) of the Act.
- ~~(S//OC/NF)~~ As described in the above-referenced affidavit of Acting Director Ledgett,

the foreign intelligence information to be acquired pursuant to this certification concerns [REDACTED]

[REDACTED]

[REDACTED]

<sup>2</sup> ~~(S//OC/NF)~~ Specifically, the National Counterterrorism Center (NCTC) minimization procedures attached herewith as Exhibit G were submitted for approval by the Court in connection with [REDACTED] on July 31, 2013, and were approved by the Court on August 30, 2013.

<sup>3</sup> ~~(S//OC/NF)~~ Specifically, the NSA, FBI, and CIA minimization procedures attached herewith as Exhibits B, D, and E, respectively, will be submitted for approval by the Court.

~~SECRET//ORCON/NOFORN~~

~~SECRET//ORCON/NOFORN~~

[REDACTED] If NSA seeks to acquire foreign intelligence information concerning additional [REDACTED]  
 [REDACTED] NSA may target  
 consistent with 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 shall include a description of the factual basis for  
 NSA's determination that [REDACTED]

~~(S//OC/NF)~~ 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 described above, is authorized, and such authorization shall be effective on  
 August 28, 2014, 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 September 10, 2013.

**Amendments to DNI/AG 702(g) Certifications** [REDACTED]

~~(S//OC/NF)~~ 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, FBI, and CIA minimization procedures attached  
 herewith as Exhibits B, D, and E, respectively, in connection with foreign intelligence

~~SECRET//ORCON/NOFORN~~

~~SECRET//ORCON/NOFORN~~

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

[REDACTED] is authorized.<sup>4</sup> Such authorization, as amended, shall be effective on August 28, 2014, or on the date upon which the Foreign Intelligence Surveillance Court issues an order concerning these amendments pursuant to subsection 702(i)(3) of the Act, whichever is later. All other aspects of DNI/AG 702(g) Certifications [REDACTED] [REDACTED] as amended, remain unaltered and are incorporated herein.

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

---

<sup>4</sup> ~~(S//OC/NF)~~ 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 Foreign Intelligence Surveillance Court, and are consistent with the requirements of the fourth amendment to the Constitution of the United States.

~~SECRET//ORCON/NOFORN~~



~~SECRET//ORCON/NOFORN~~

(U) VERIFICATION

~~(S)~~ I declare under penalty of perjury that the facts set forth in the foregoing certification

[REDACTED]

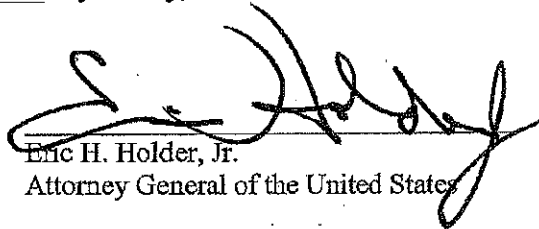
DNI/AG 702(g) Certification [REDACTED] are true and correct to the best of my knowledge and

belief. I further declare under penalty of perjury that the facts set forth in the foregoing

amendments to DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] are true and correct to the best of my knowledge and belief. Executed pursuant to

28 U.S.C. § 1746 on this 29<sup>th</sup> day of July, 2014.



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

~~SECRET//ORCON/NOFORN~~

~~SECRET//ORCON//NOFORN~~

(U) VERIFICATION

~~(S)~~ I declare under penalty of perjury that the facts set forth in the foregoing certification

[REDACTED]

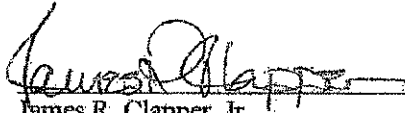
DNI/AG 702(g) Certification [REDACTED] are true and correct to the best of my knowledge and

belief. I further declare under penalty of perjury that the facts set forth in the foregoing

amendments to DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] are true and correct to the best of my knowledge and belief. Executed pursuant to

28 U.S.C. § 1746 on this 25<sup>th</sup> day of July, 2014.

  
James R. Clapper, Jr.  
Director of National Intelligence

~~SECRET//ORCON//NOFORN~~

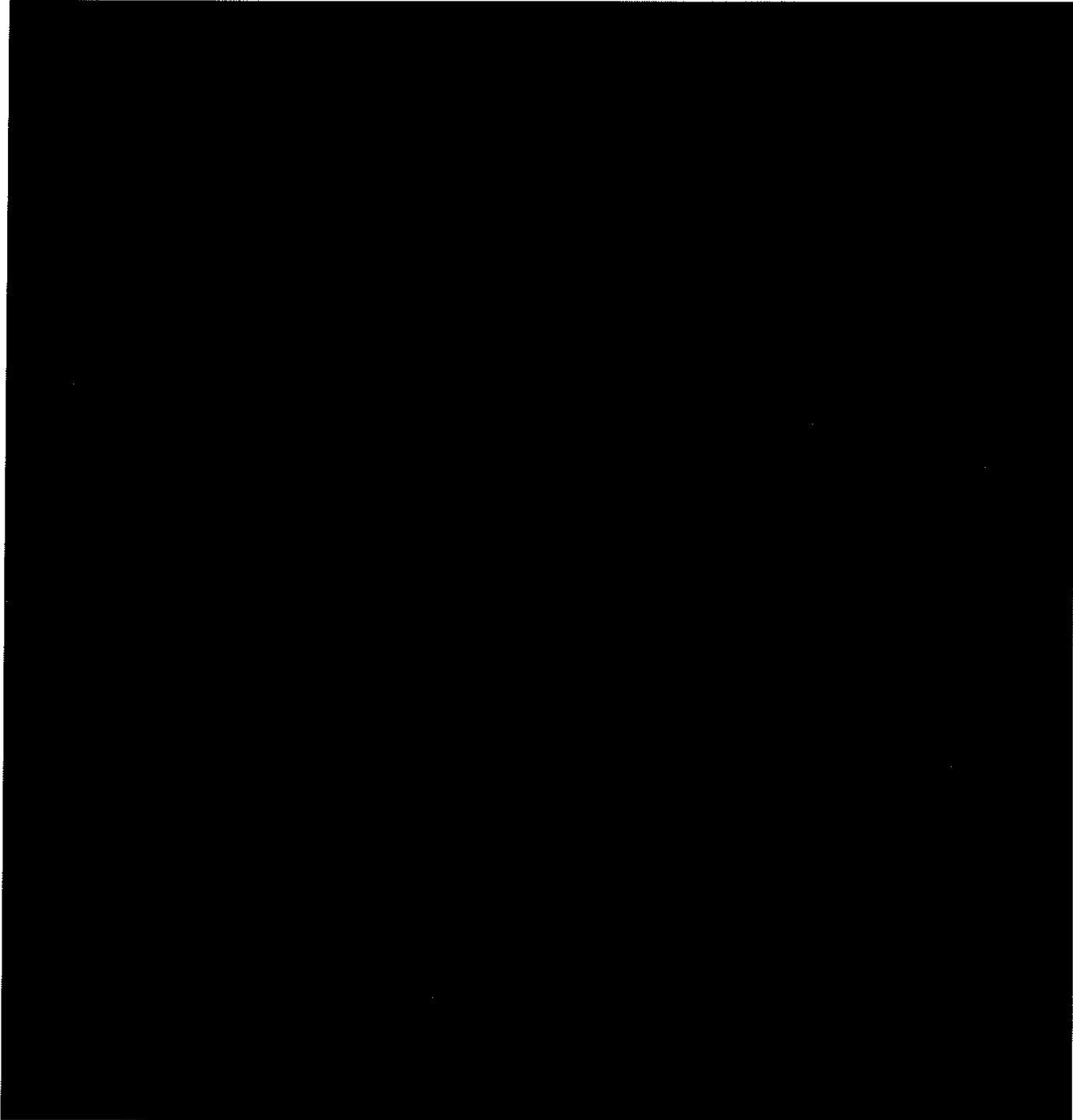
~~TOP SECRET//SI//NOFORN//20320108~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

**EXHIBIT A**

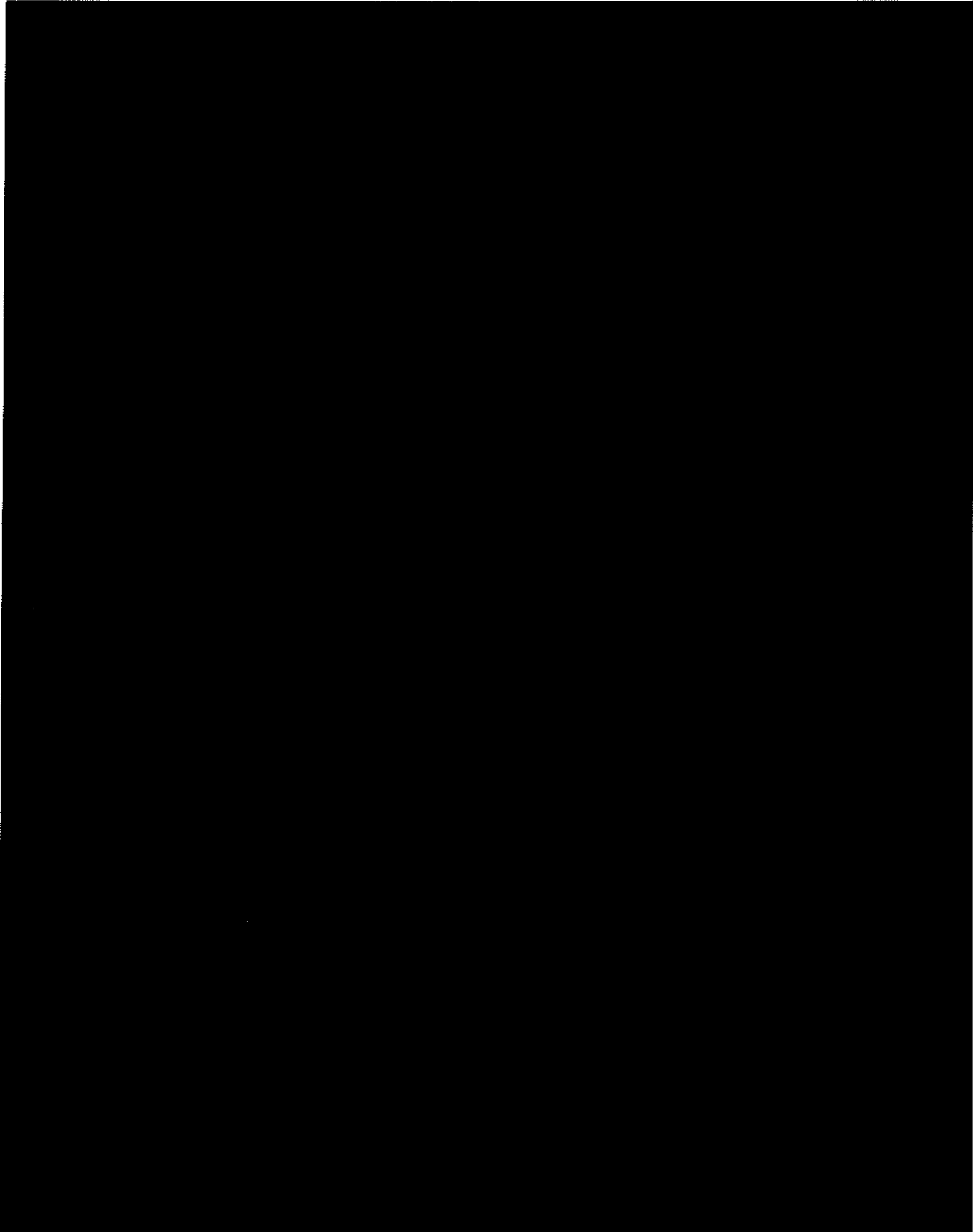
**PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING  
NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED  
OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE  
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE  
SURVEILLANCE ACT OF 1978, AS AMENDED**

2011 JUL 28 PM 3:57  
FANNING HALL  
U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT



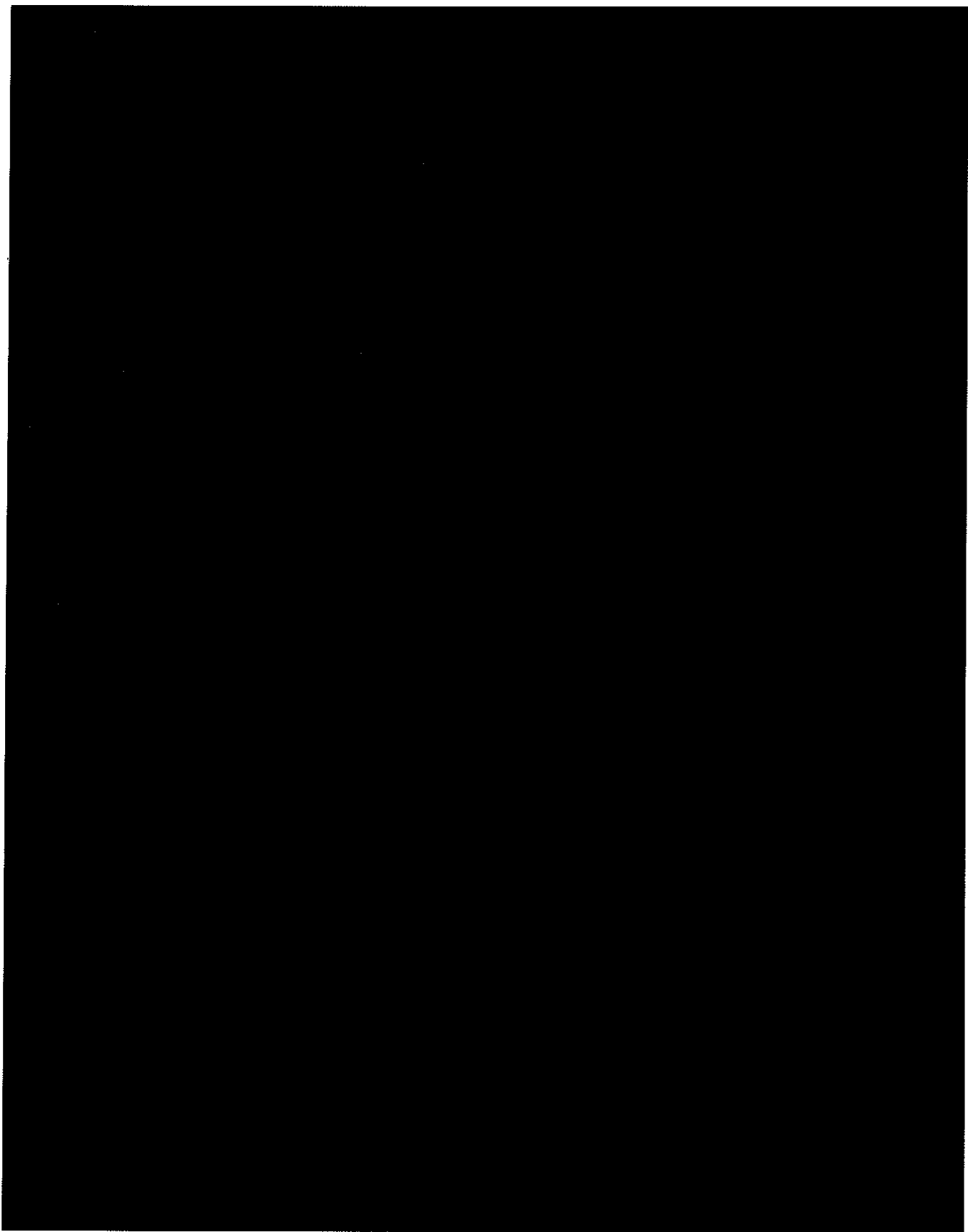
~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~



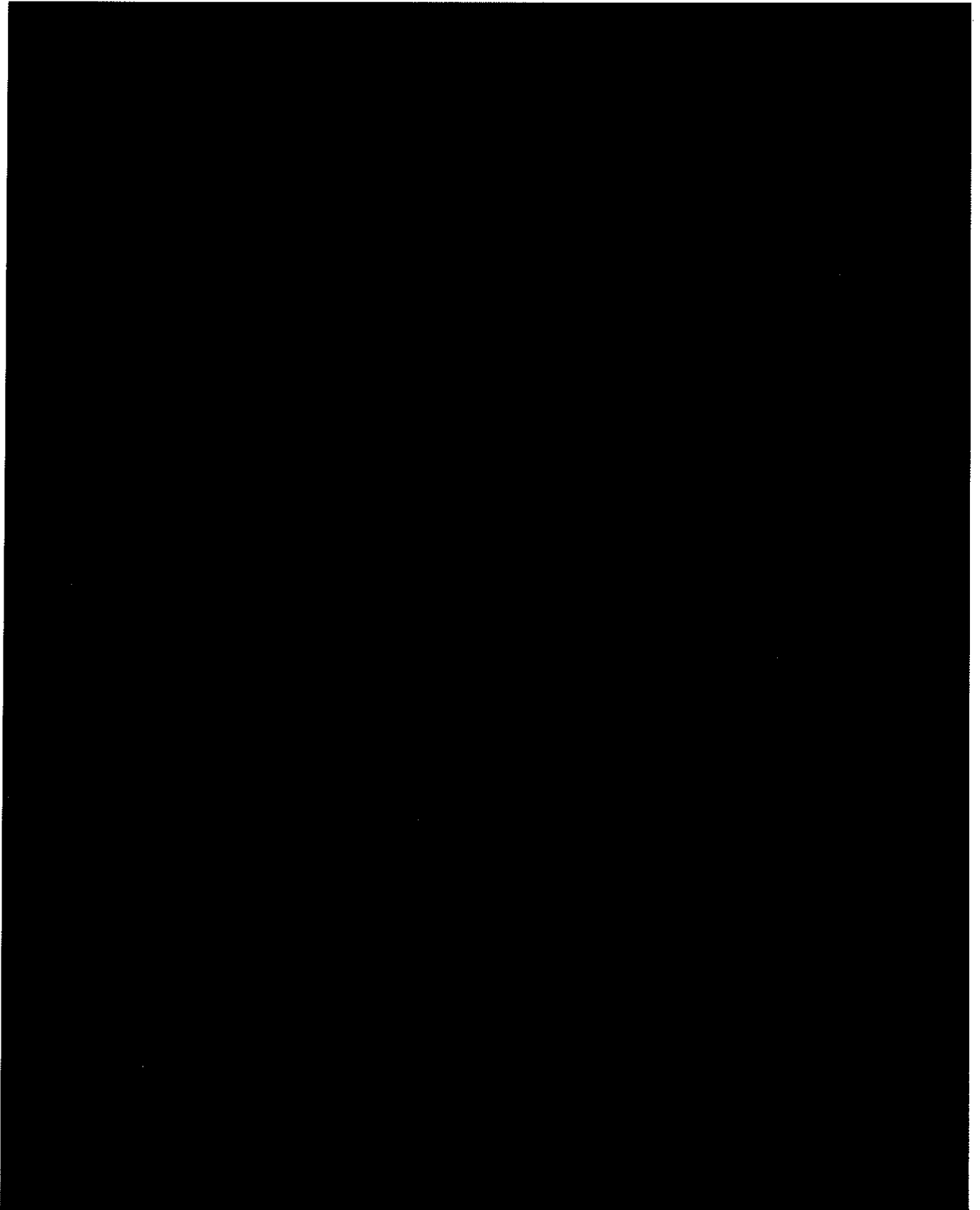
~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~



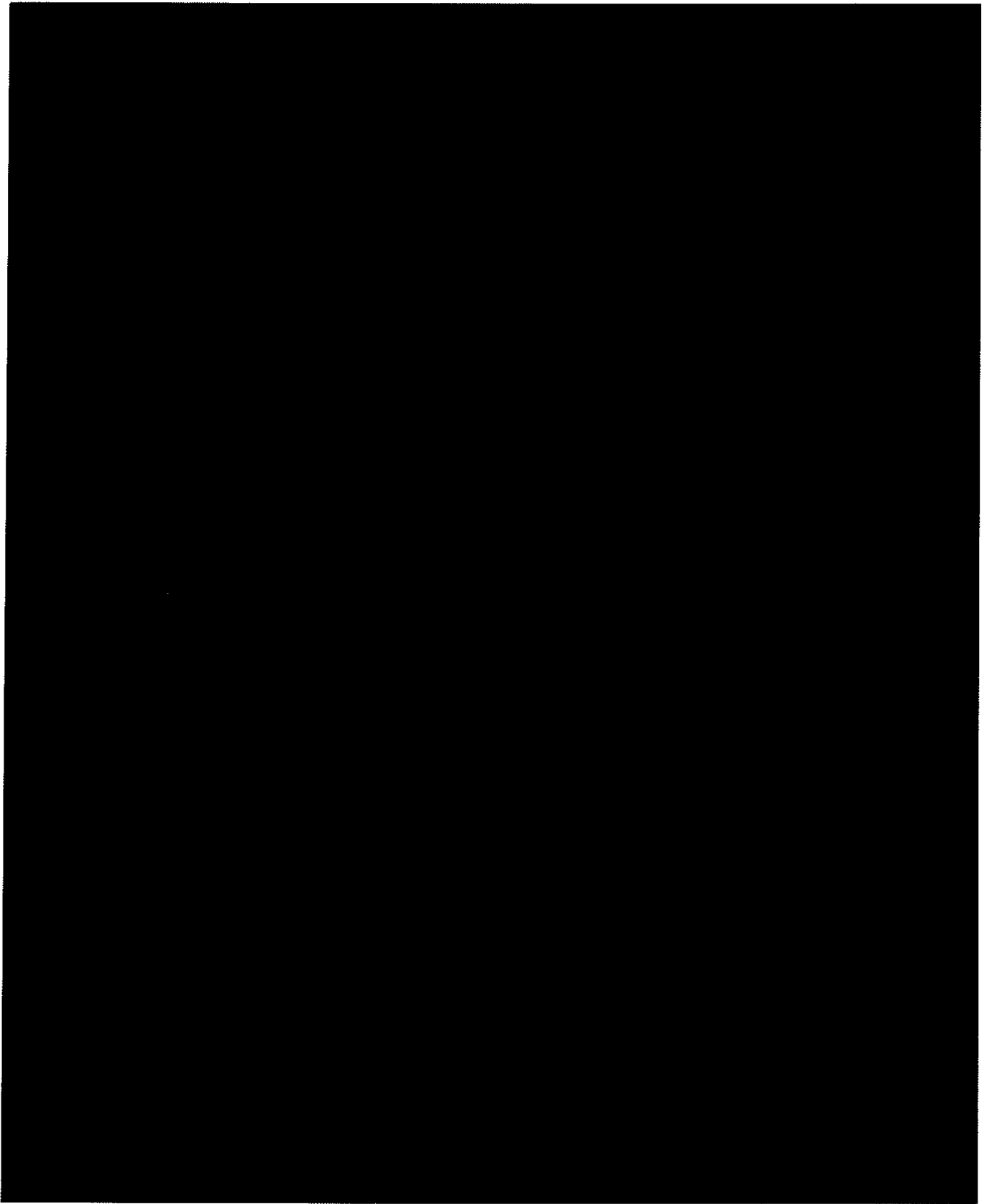
~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~



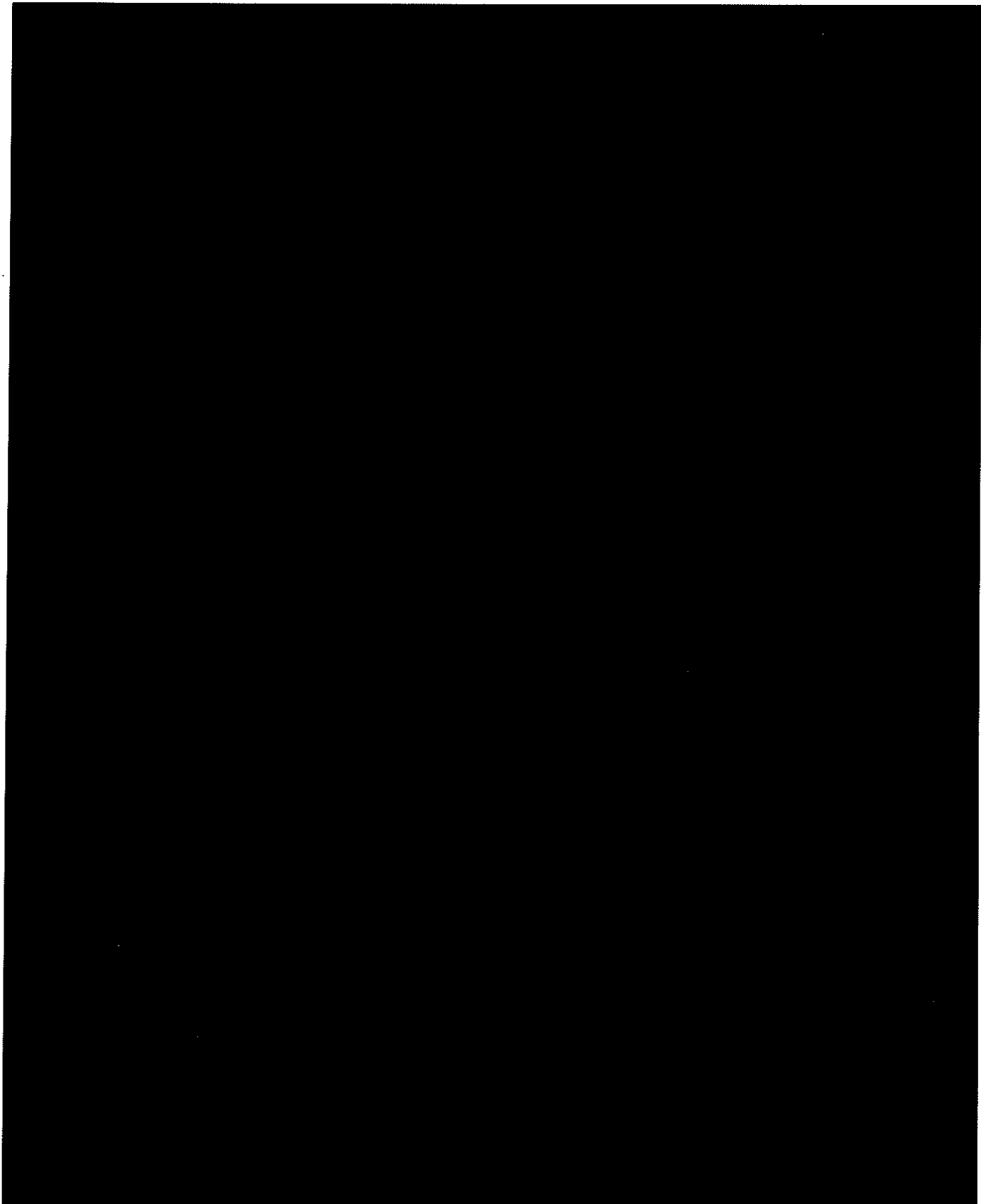
~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~



~~TOP SECRET//SI//NOFORN//20320108~~

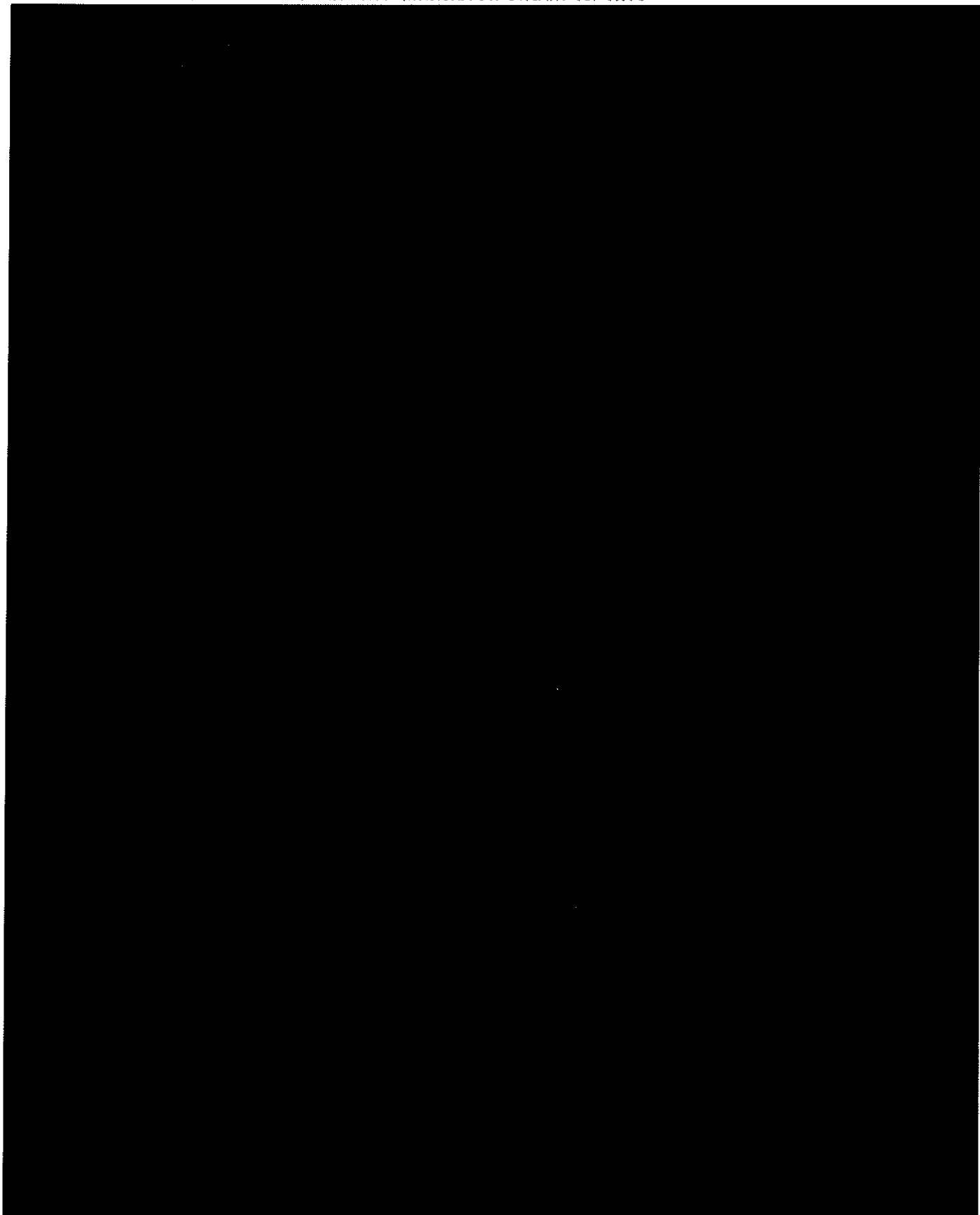
~~TOP SECRET//SI//NOFORN//20320108~~



~~TOP SECRET//SI//NOFORN//20320108~~

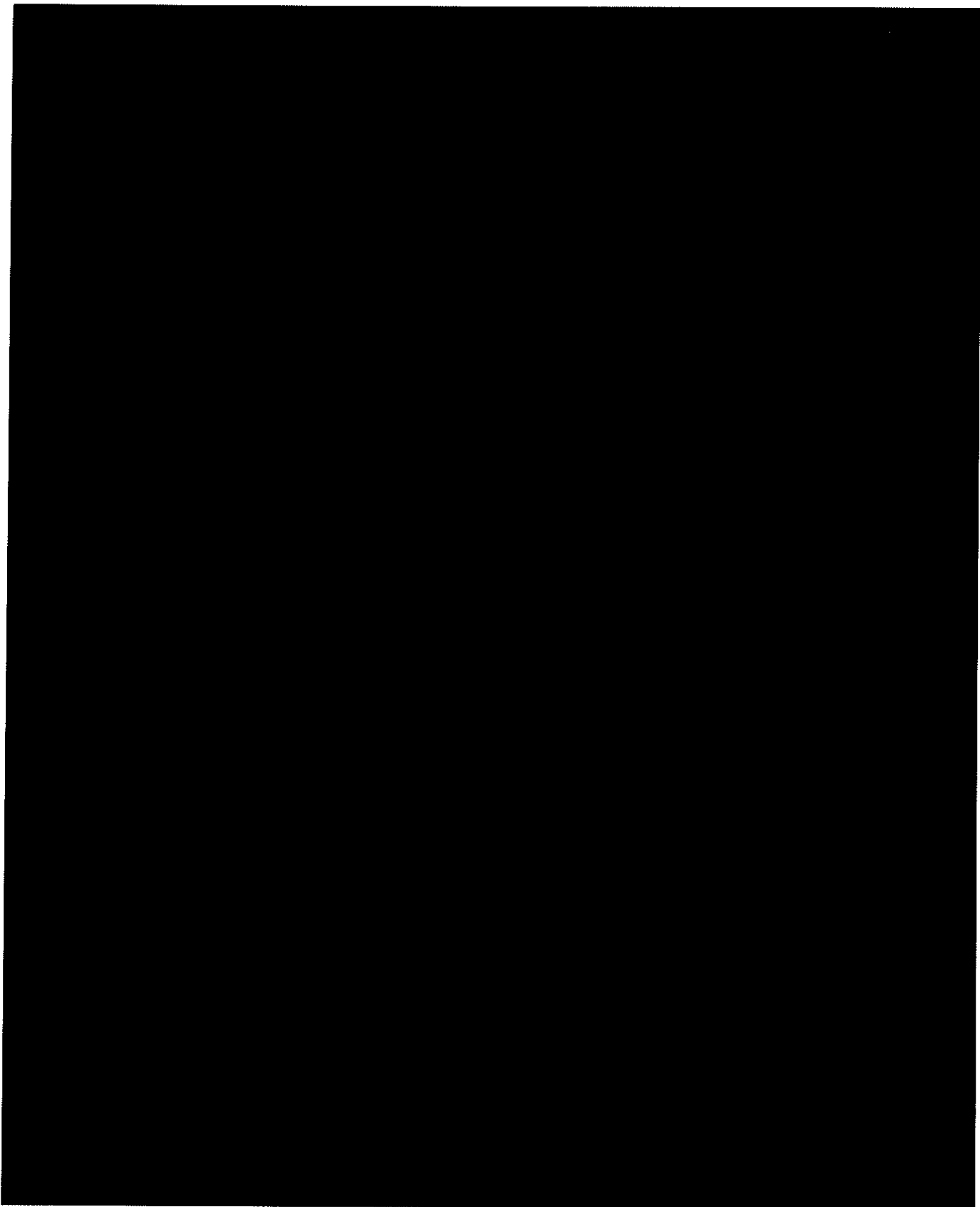


~~TOP SECRET//SI//NOFORN//20320108~~



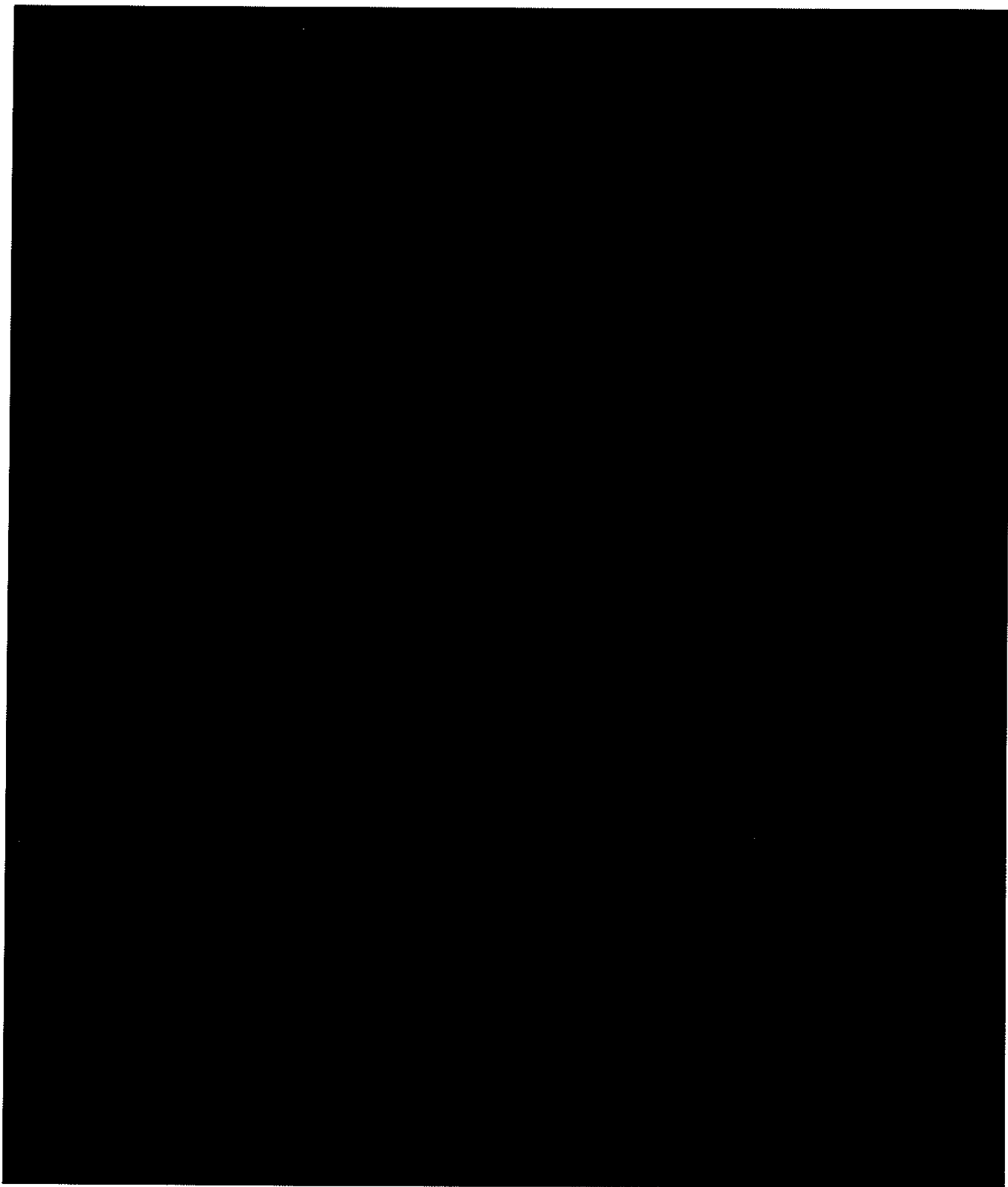
~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~



~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~



~~TOP SECRET//SI//NOFORN//20320108~~

~~SECRET//NOFORN//24 JULY 2039~~

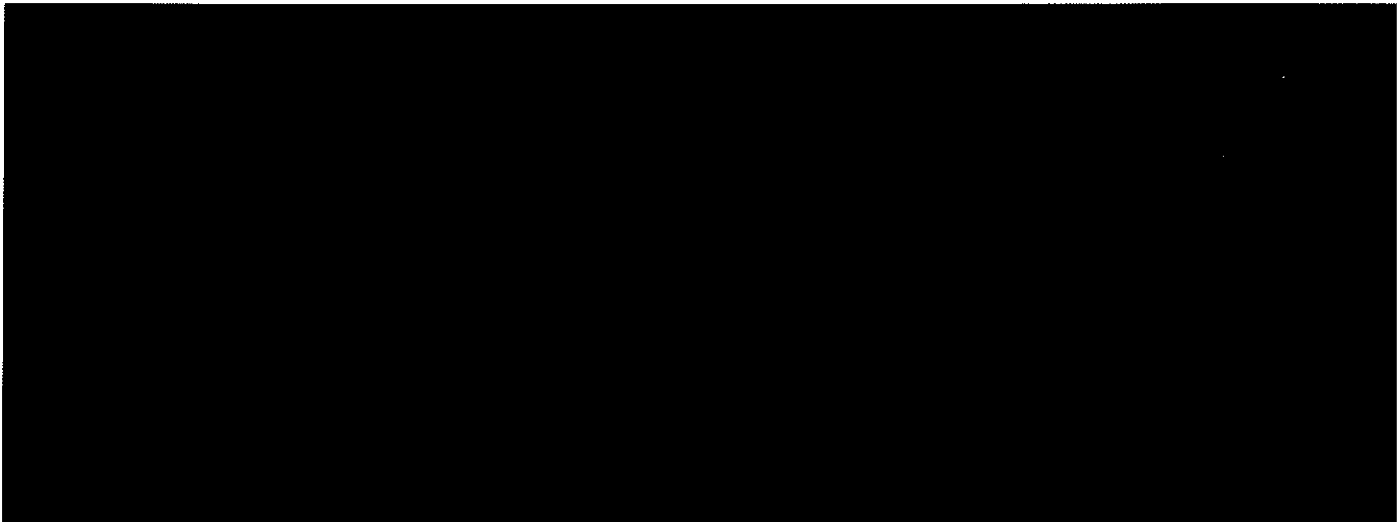
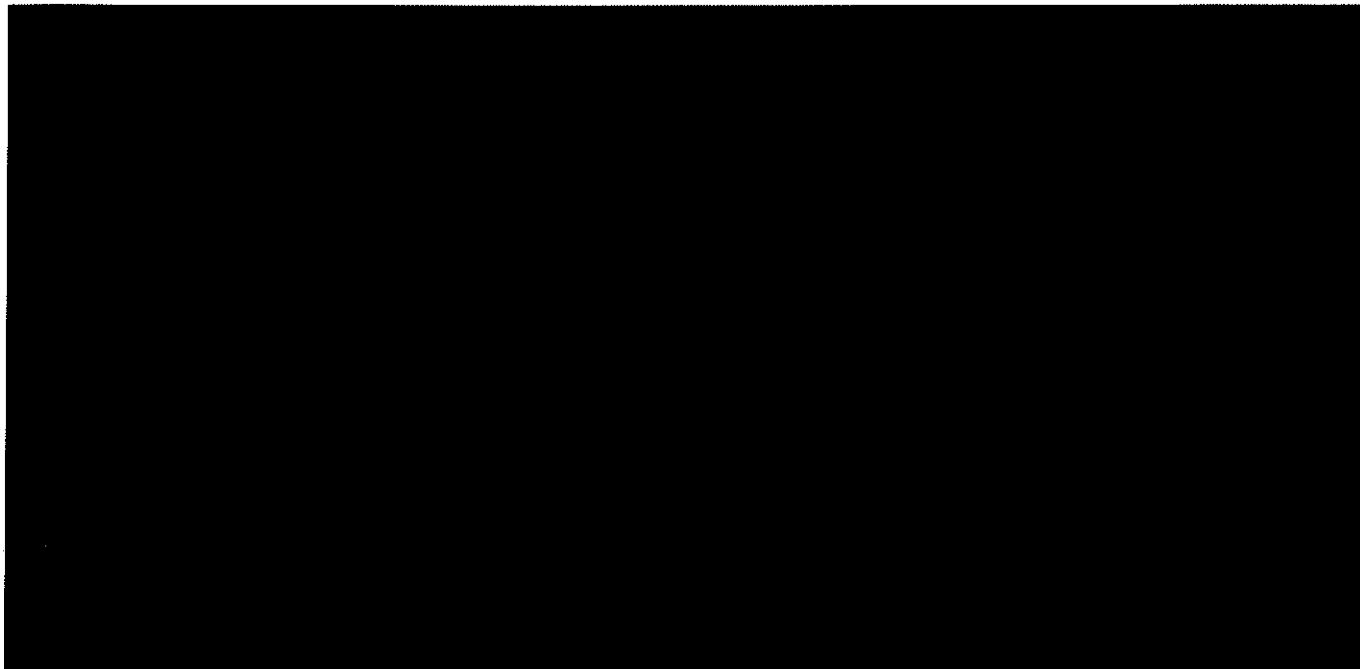
U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

EXHIBIT C

2014 JUL 28 PM 3:57

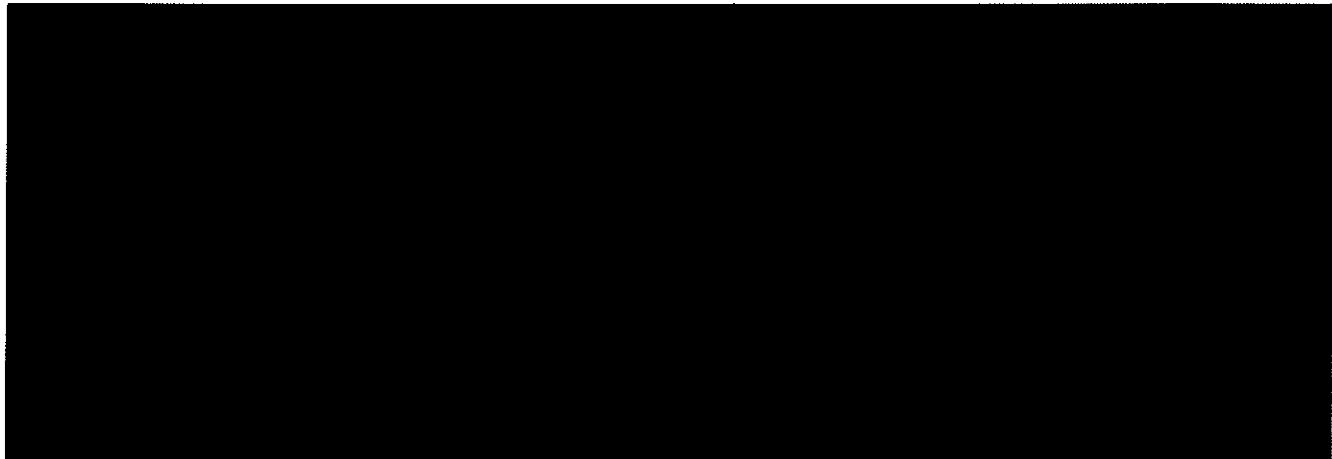
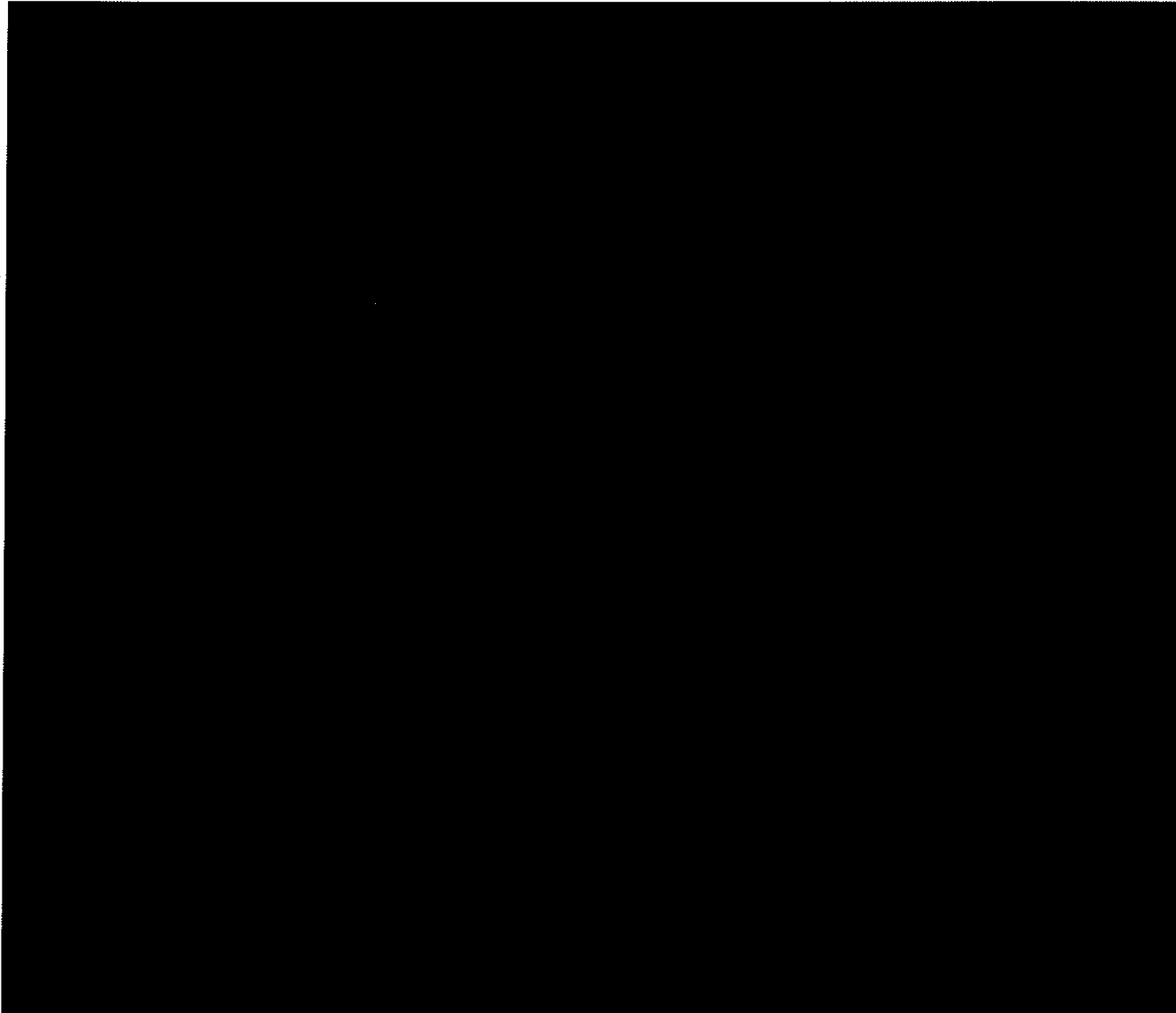
PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION FOR  
TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE  
LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN  
INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN  
INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

CLAYTON B. KENNEDY HALL  
U.S. SUPREME COURT



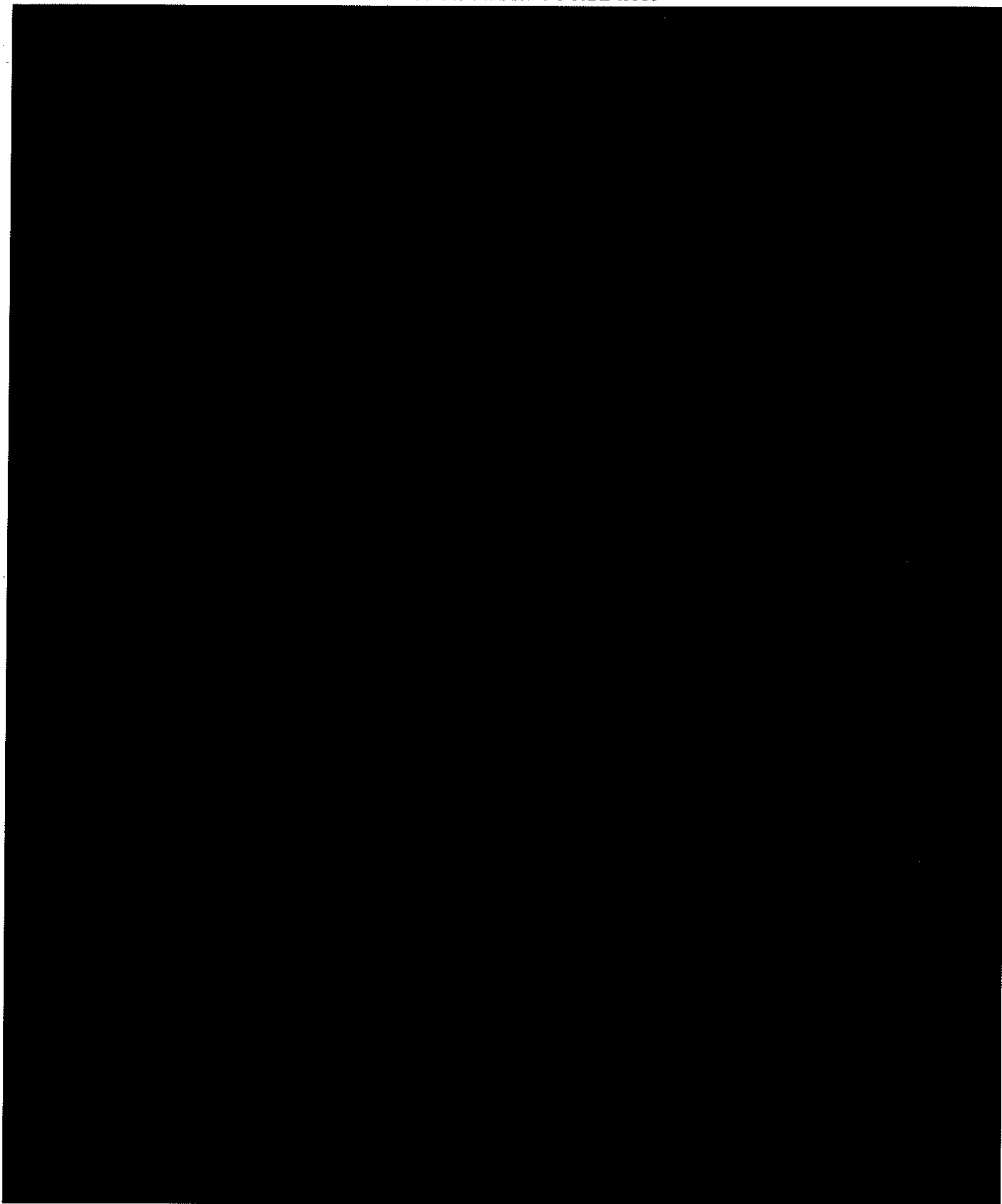
~~SECRET//NOFORN//24 JULY 2039~~

~~SECRET//NOFORN//24 JULY 2039~~



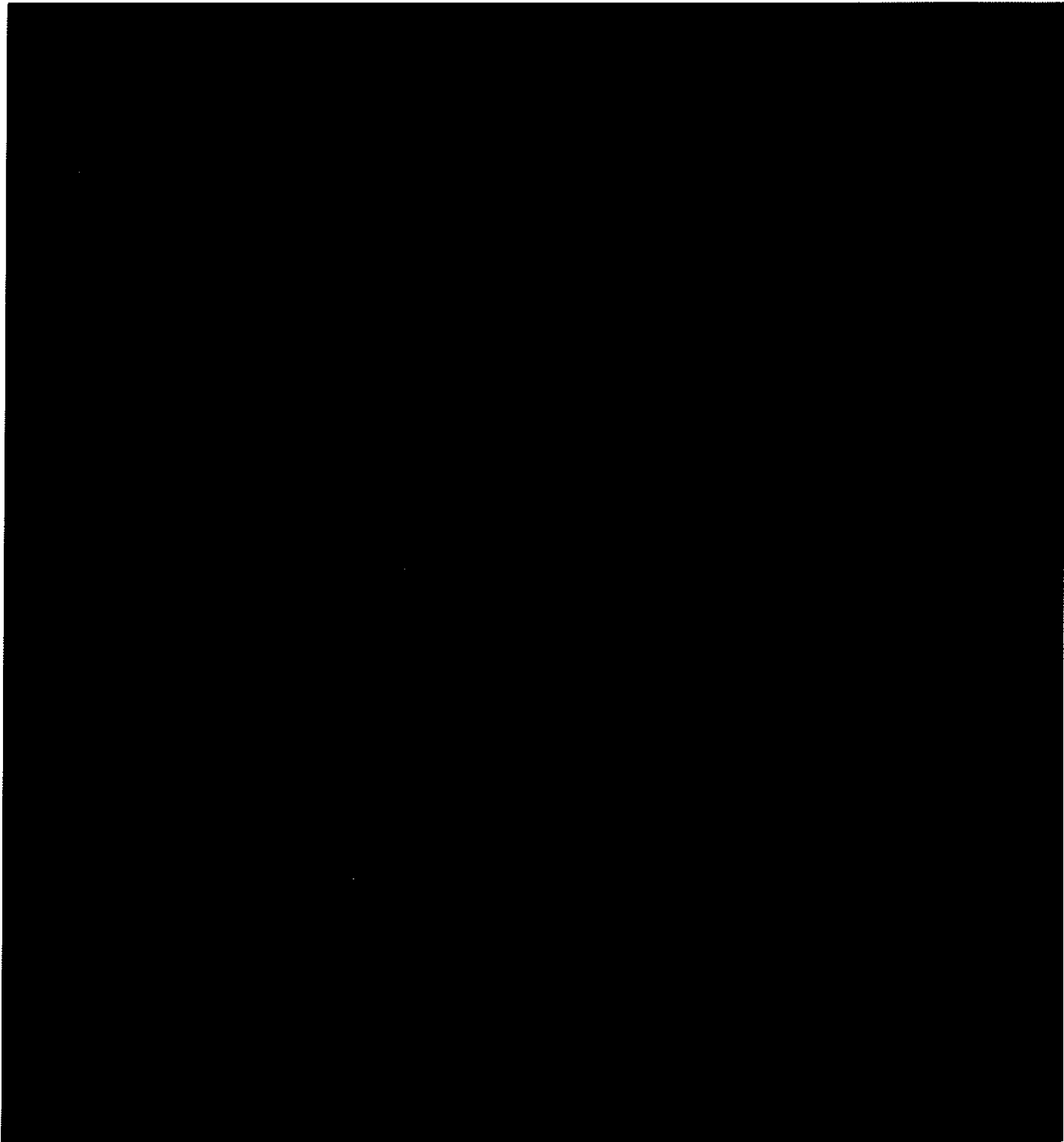
~~SECRET//NOFORN//24 JULY 2039~~

~~SECRET//NOFORN//24 JULY 2039~~



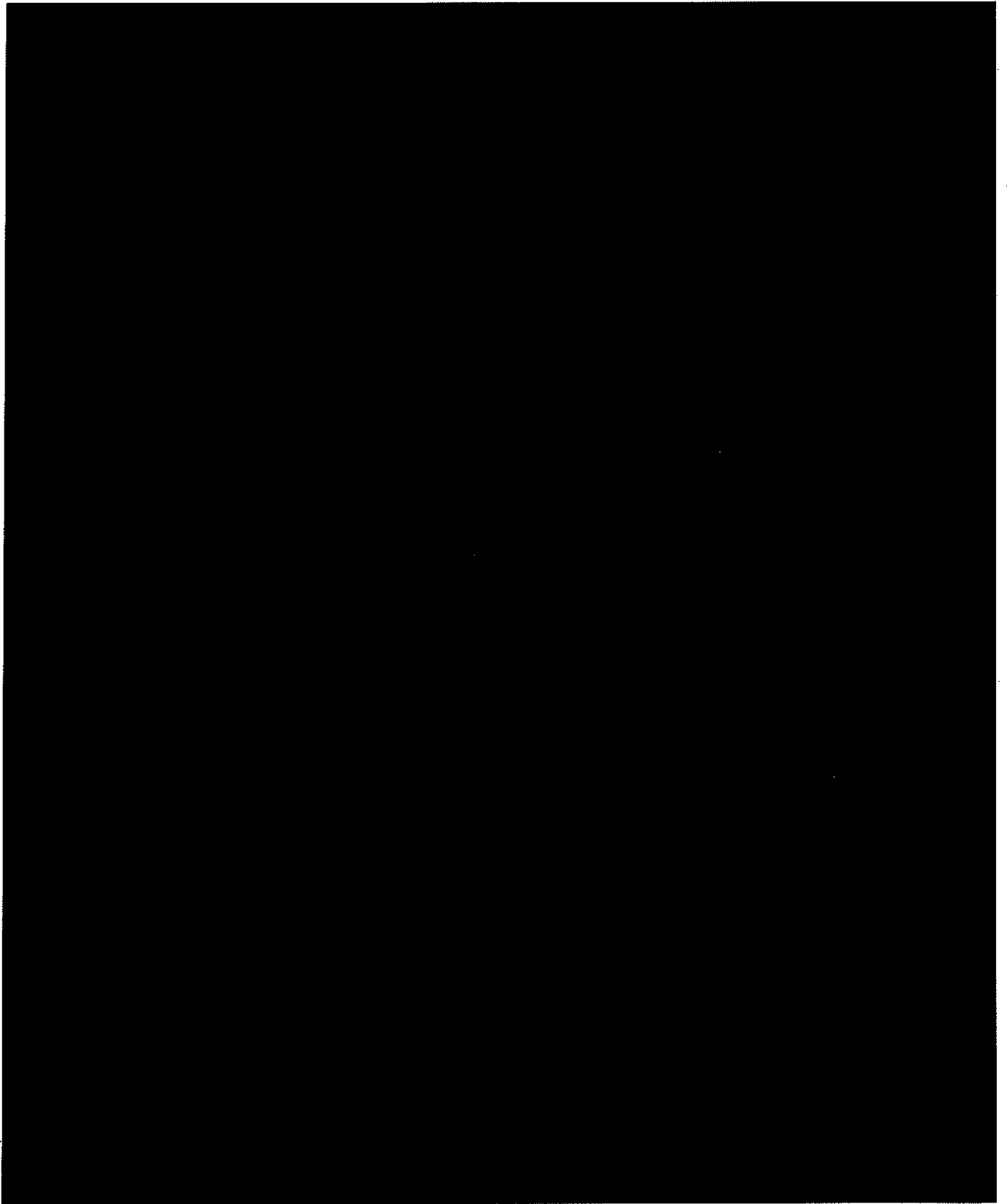
~~SECRET//NOFORN//24 JULY 2039~~

~~SECRET//NOFORN//24 JULY 2039~~



~~SECRET//NOFORN//24 JULY 2039~~

~~SECRET//NOFORN//24 JULY 2039~~



~~SECRET//NOFORN//24 JULY 2039~~

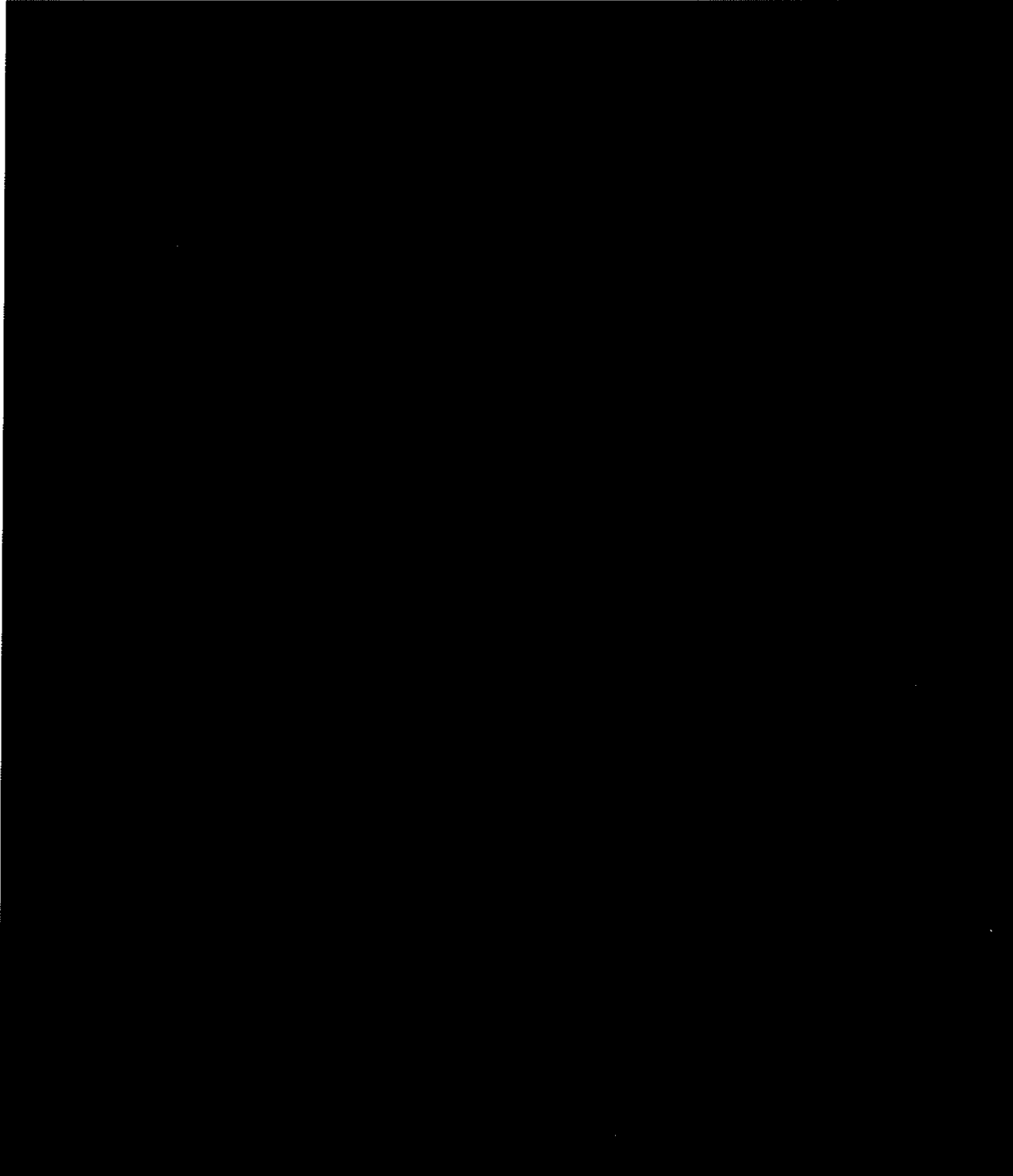


~~TOP SECRET//SI//ORCON//NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

EXHIBIT F

2014 JUL 29 PM



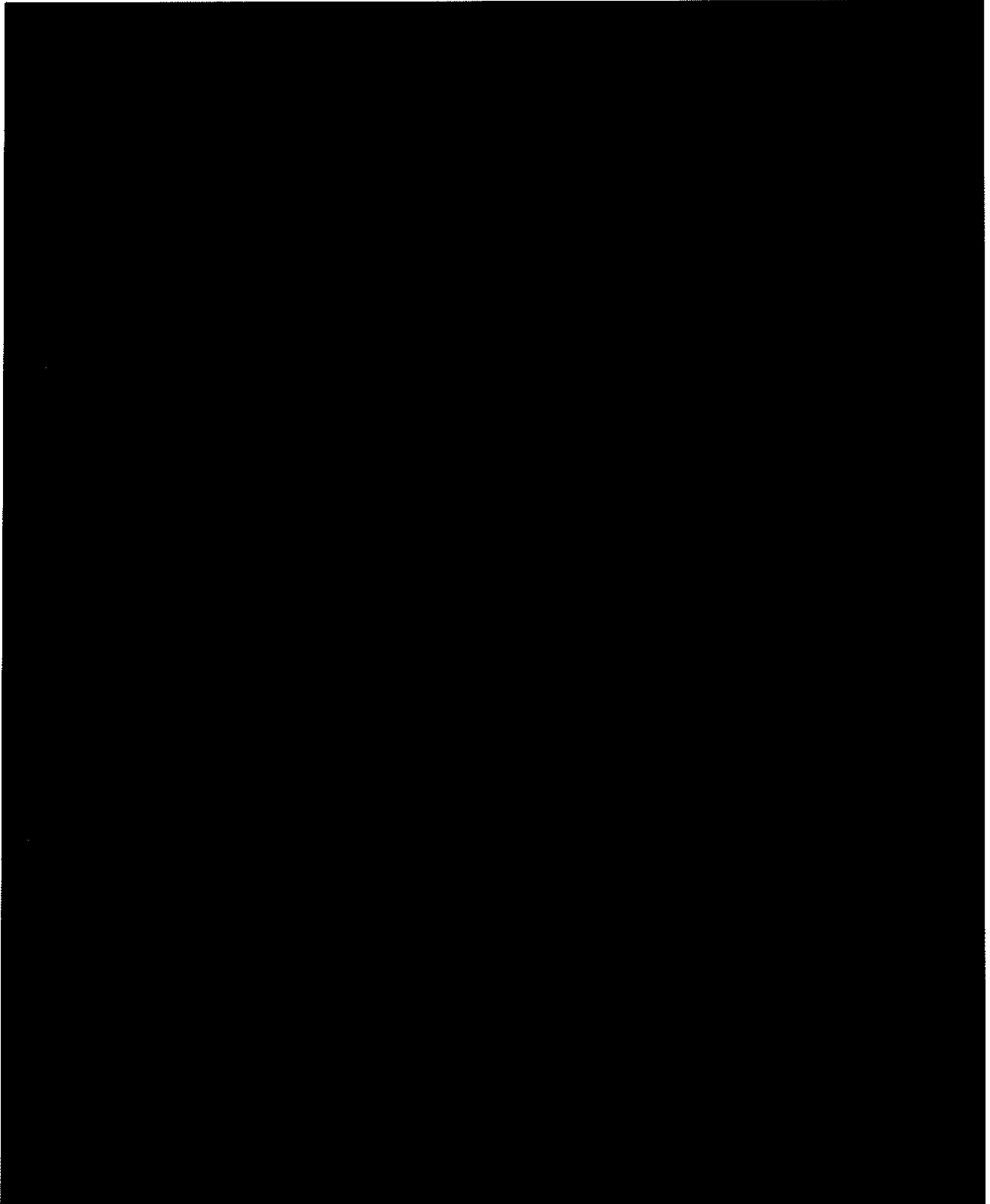
Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20340601

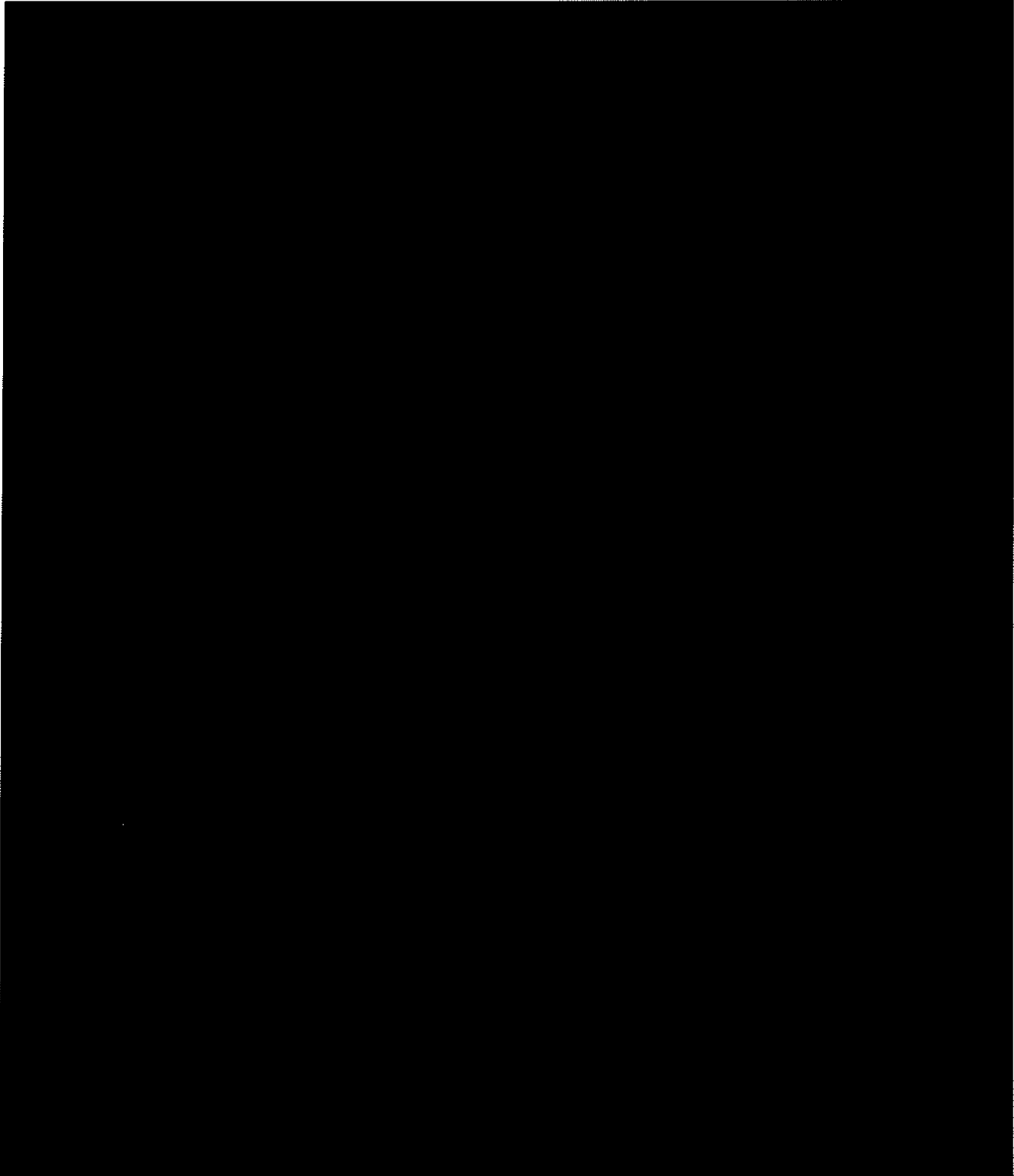
~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



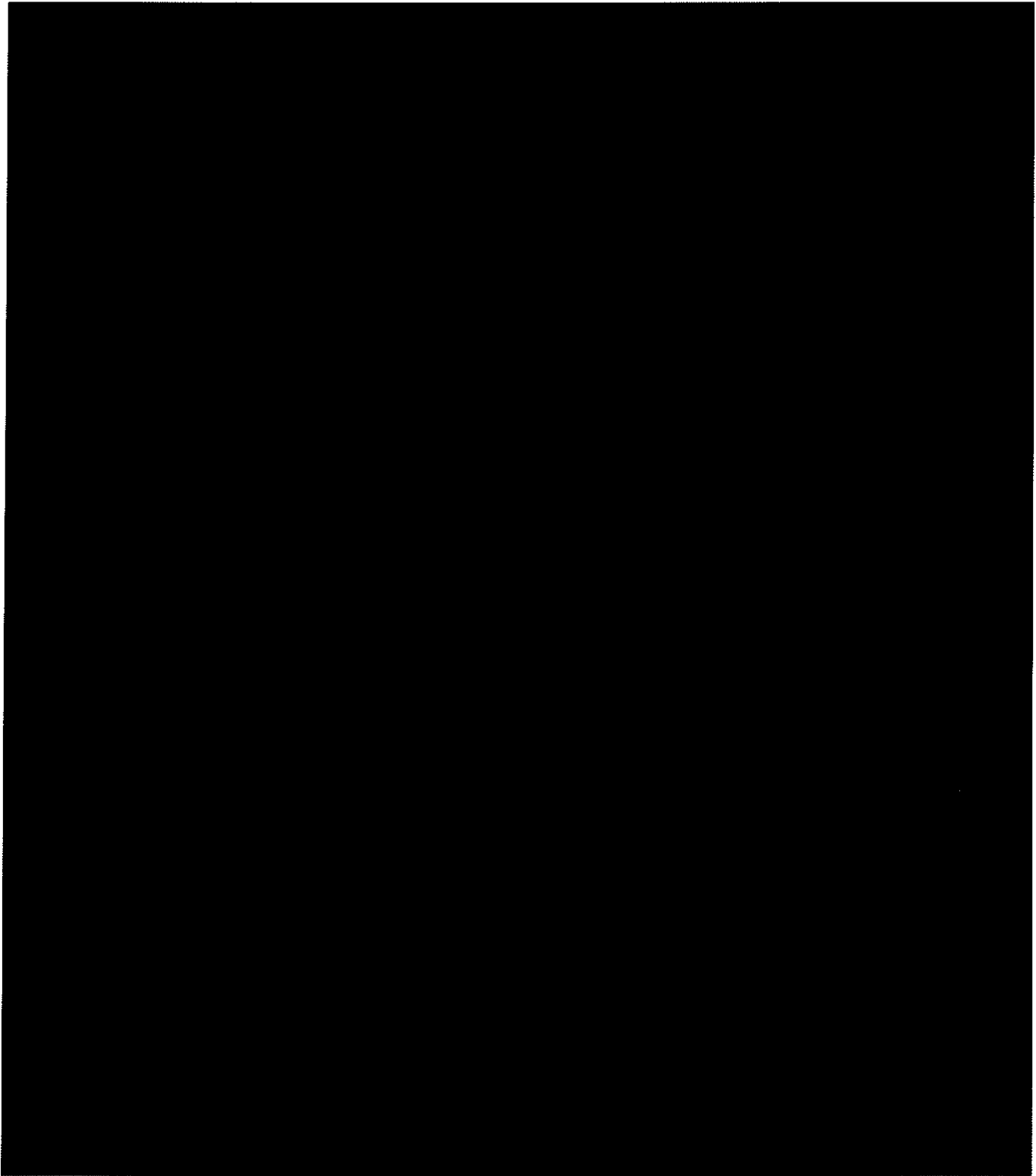
~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

~~SECRET//NOFORN~~

**EXHIBIT G**

**MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH INFORMATION ACQUIRED BY THE FEDERAL BUREAU OF INVESTIGATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED**

**I. (U) GENERAL PROVISIONS**

~~(S)~~ With respect to information obtained by the National Counterterrorism Center (NCTC) from the Federal Bureau of Investigation (FBI) and acquired pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), NCTC will follow the procedures set forth below. These procedures do not authorize NCTC to directly acquire or collect information pursuant to the Act. The Attorney General has adopted the procedures set forth below after concluding that they satisfy the requirements of minimization procedures, as defined in the Act at 50 U.S.C. §§ 1801(h) and 1821(4).

**II. (U) INFORMATION IN FBI GENERAL INDICIES**

~~(S)~~ With respect to section 702-acquired information that the FBI has determined satisfies the applicable retention and dissemination requirements set forth in the FBI Section 702 Minimization Procedures, and that the FBI has uploaded or otherwise placed into FBI general indices (such as the Automated Case Support (ACS) system or successor systems) under case classifications that are reasonably likely to contain information related to terrorism or counterterrorism, the following provisions shall apply. None of the following provisions shall affect additional restrictions that the FBI may impose on the retention, use, or dissemination of such information:

~~SECRET//NOFORN~~

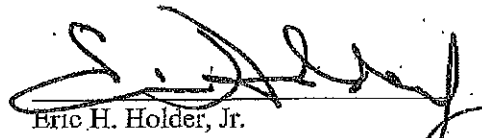
~~Classified by: The Attorney General  
Reason: 1.4(c)  
Declassify on: 20 August 2037~~

~~SECRET//NOFORN~~

1. ~~(S//NF)~~ For the purpose of these procedures, NCTC may consider all section 702-acquired information that it accesses in FBI general indices, and that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or necessary to assess the importance of foreign intelligence information, to have been disseminated by FBI to NCTC in accordance with the FBI Section 702 Minimization Procedures.
2. ~~(S//NF)~~ If NCTC accesses section 702-acquired information in FBI general indices that is evidence of a crime, but does not reasonably appear to be foreign intelligence information or necessary to understand or assess the importance of foreign intelligence information, NCTC may not retain, use, or disseminate this information.
3. ~~(S//NF)~~ If NCTC ingests or transfers section 702-acquired information from FBI general indices into NCTC systems before reviewing such information, NCTC may presume that such information reasonably appears to be foreign intelligence information, is necessary to understand or assess the importance of foreign intelligence information, or is evidence of a crime. If NCTC discovers any section 702-acquired information transferred from FBI general indices to NCTC systems that NCTC determines is evidence of a crime, but does not reasonably appear to be foreign intelligence information or necessary to understand or assess the importance of foreign intelligence information, NCTC shall promptly remove such information from all NCTC systems.
4. ~~(S//NF)~~ NCTC personnel may only access FBI general indices, or review section 702-acquired information from FBI general indices that has been ingested or transferred into NCTC systems, if they first receive training regarding these limitations.

### III. (U) INTERPRETATION

(U) NCTC shall refer all significant questions relating to the interpretation of these procedures to the Department of Justice, National Security Division.

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

8-22-12  
Date

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~(S)~~ **National Counterterrorism Center Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act**

~~(S)~~ With respect to the retention, processing, and dissemination of raw information the National Counterterrorism Center (NCTC) receives from the Federal Bureau of Investigation (FBI) that is acquired pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), 50 U.S.C. §§ 1801-1812, 1821-1829, 1881c, 1881d(b), NCTC will follow these minimization procedures. These procedures do not authorize NCTC to directly acquire or collect information pursuant to the Act.

~~(S)~~ Except as provided in Section E below, [REDACTED]

~~(S)~~ **A. GENERAL PROVISIONS**

- ~~(S)~~ The Attorney General has adopted these procedures after concluding that they meet the requirements of minimization procedures, as defined in the Act at Title 50, United States Code, Sections 1801(h) and 1821(4). In accordance with Title 50, United States Code, Section 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.
- ~~(S)~~ Pursuant to Title 50, United States Code, Sections 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 from electronic surveillance, [REDACTED] conducted under FISA concerning United States persons may be used and disclosed by NCTC employees without the consent of such 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, and do not apply to information that is acquired, retained, or disseminated with a United States person's consent. Except for the provisions set forth below regarding attorney-client communications, the use of FISA-acquired information in proceedings in the United States and foreign countries, the disclosure of raw FISA-acquired information, and the use of caveats and other markings on FISA-acquired or FISA-derived information, these procedures do not apply to information solely concerning non-United States persons.

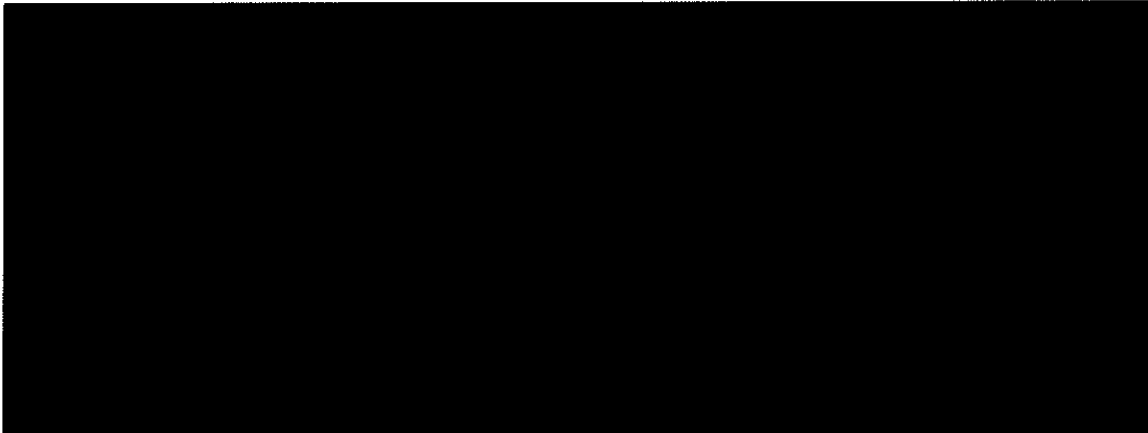
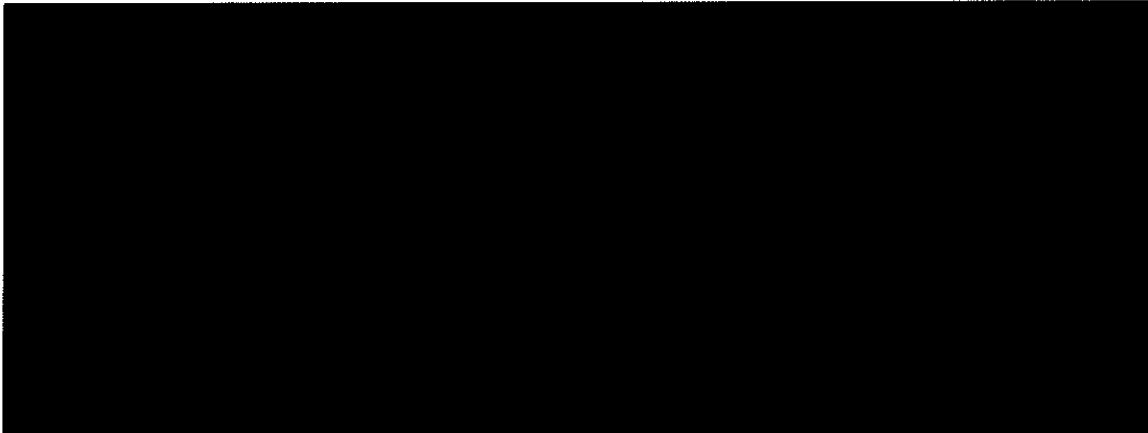
~~SECRET//NOFORN~~

Classified by: Eric H. Holder, Jr.  
Attorney General

Reason: 1.4(c)

Declassify on: 15 March 2037

~~SECRET//NOFORN~~

3. ~~(S)~~ **Definitions.** These procedures adopt all definitions set forth in 50 U.S.C. §§ 1801 and 1821, including those for the terms “foreign intelligence information,” “United States person,” and “Attorney General.” In addition, as used herein:
- a. “information” herein means all data and content acquired by FBI pursuant to the Act and provided to NCTC, including contents as defined in 50 U.S.C. § 1801(n).
  - b. “metadata” means dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport, or meaning of the communication.
  - c. “NCTC employee” means (i) individuals directly employed by NCTC, (ii) personnel detailed to NCTC from other departments or agencies who work under NCTC management and supervision in a manner substantially the same as individuals directly employed by NCTC, and (iii) contractors working under NCTC management and supervision who are authorized to perform services in support of NCTC on FISA-related matters.
  - d. “nonpublicly available information” means information that a member of the public could not obtain on request, by research in information generally available to the public, or by casual observation.
  - e. “raw” information is FISA-acquired information that (i) is in the same or substantially the same format as when FBI acquired it, or (ii) 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 or to be necessary to understand foreign intelligence information or assess its importance.
  - f. “review” of information occurs when an NCTC employee actually accesses information.
  - g. 
  - h. 
  - i. “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

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

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.

4. ~~(S)~~ **Presumptions.** For the purposes of these procedures:


- a. If an individual is known to be located in the United States, [REDACTED] he or she should be presumed to be a United States person unless the individual is identified as an alien who has not been admitted for permanent residence, or unless the totality of circumstances gives rise to the reasonable belief that the individual is not a United States person.
- b. If an individual is known or reasonably believed to be located outside the United States, he or she should be presumed to be a non-United States person unless the individual is identified as a United States person or the totality of circumstances gives rise to the reasonable belief that the individual is a United States person.
- c. In [REDACTED] if it is not known whether an individual is located in or outside the United States, he or she should be presumed to be a non-United States person unless the individual is identified as a United States person or the totality of circumstances gives rise to the reasonable belief that the individual is a United States person. NCTC shall only apply this presumption in cases that FBI has identified to NCTC as [REDACTED]

5. ~~(S)~~ **Departures.**

- a. If NCTC believes that a situation requires it to act inconsistently with these procedures to protect the national security of the United States, or to protect life or property from serious harm, NCTC will promptly contact the Office of Intelligence of the National Security Division (NSD) of the Department of Justice (DOJ) to request that these procedures be modified. NCTC will promptly notify FBI of any such request. 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 FISA.
- b. If NCTC determines that it must take action in apparent departure from these procedures in order to protect against an immediate threat to human life and that it is not feasible to obtain a timely modification of these procedures, NCTC may take such action immediately. NCTC will promptly report the action taken to NSD and FBI. NSD will promptly notify the Foreign Intelligence Surveillance Court (FISC) of any such activity.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

6. ~~(S//NF)~~ Nothing in these procedures shall prohibit:
- a. The retention or processing of information necessary for the maintenance of technical databases, so long as only administrative or technical personnel have access to such databases;
  - b. The retention or processing of information in emergency data backup systems, provided that only administrative 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, NCTC shall apply these procedures to the transferred data;
  - c. NCTC's access to FISA-acquired information that FBI, CIA, or NSA may disseminate to NCTC pursuant to their respective FISC-authorized minimization procedures; or
  - d. The retention, processing, or dissemination of information reasonably necessary to (i) comply with specific constitutional, judicial, or legislative mandates, or (ii) conduct lawful oversight of NCTC's retention, processing, or dissemination of information under any section of FISA.
7. ~~(S)~~ **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 Title 50, United States Code, Sections 1806(b) and 1825(c), Executive Order No. 12333 (as amended), and any other applicable crimes reporting requirements or procedures. See Section A(10) below.
- 

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

**B. ~~(S)~~ RETENTION**

1. ~~(S)~~ NCTC may maintain raw information. Raw information must be maintained in a manner that (a) clearly identifies it as raw information collected by FBI pursuant to FISA, (b) only permits such information to be accessed by NCTC employees who have received training in applying these procedures to raw FISA-acquired information, and (c) enables NCTC to mark or otherwise identify communications or other information that meet the standard set forth in paragraph B(3) herein. The retention provisions herein apply notwithstanding other Attorney General guidelines governing NCTC's retention of information.
  
2. ~~(S)~~ Subject to the above:



3. ~~(S)~~ Nonpublicly available information concerning a consenting United States person that an NCTC employee responsible for applying these procedures has determined 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 may also be retained and used for further analysis without the limitations set forth in paragraph B(1) above. Such information shall be clearly identified in NCTC systems and records as information that was collected by FBI pursuant to FISA and that is subject to these procedures. These procedures do not limit the time period for which NCTC may retain such information. Information that is evidence of a crime that has been, is being,

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

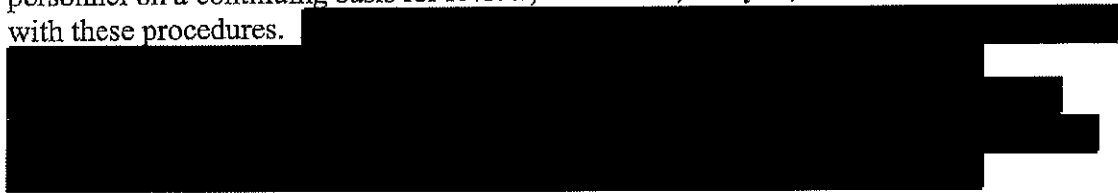
or is about to be committed, but is not foreign intelligence information, may only be retained or disseminated for law enforcement purposes.

C. ~~(S)~~ PROCESSING

1.



2. ~~(S)~~ NCTC may make raw FISA-acquired information available to authorized NCTC personnel on a continuing basis for review, translation, analysis, and use in accordance with these procedures.



3. ~~(S)~~ NCTC may find, extract, and analyze metadata associated with all communications received from FBI, regardless of whether such communications are determined to satisfy the standards set forth in these procedures for retention or dissemination. NCTC may use such metadata to analyze communications and may upload or transfer some or all of such metadata to NCTC electronic and data storage systems for authorized foreign intelligence purposes. FISA-acquired metadata received from FBI shall be identified as such in NCTC data repositories.

4. ~~(S)~~ **Third-Party Information.** NCTC may retain and use third-party information in accordance with these procedures if such information meets the standard set forth in Section B(3) of these procedures, and:

- a. is a communication made or received on behalf of the target(s);
- 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 meets the standard set forth in Section B(3) of these procedures but does not satisfy any of the above criteria may be retained in accordance with these procedures, but may not be disseminated or otherwise used. If NCTC believes

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

that such information should be disseminated or otherwise used, it shall proceed in accordance with Sections A(5)(a) or (b) of these procedures.

5. ~~(S)~~ **Sensitive Information.** Particular care should be taken when reviewing information that is sensitive information, as defined below. No sensitive information may be used in an analysis or report unless it is first determined that such information reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime. Information that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or necessary to assess the importance of foreign intelligence information may be retained, processed, and disseminated in accordance with these procedures even if it is sensitive information. Information that reasonably appears to be evidence of a crime may be retained, processed, and disseminated for law enforcement purposes in accordance with these procedures, even if it is sensitive information. Sensitive information consists of:
- a. Religious activities of United States persons, including consultations with clergy;
  - b. Educational and academic activities of United States persons, including consultations among professors or other teachers and their students;
  - c. Political activities of United States persons, including discussions with Members of Congress and their staff, and other elected officials;
  - d. Activities of United States persons involving the press and other media;
  - e. Sexual and other highly personal activities of United States persons;
  - f. Medical, psychiatric, or psychotherapeutic activities of United States persons; and
  - g. Matters pertaining to United States person minor children, including student requests for information to aid in academic endeavors.
6. ~~(S)~~ **Privileged Communications.**



~~SECRET//NOFORN~~

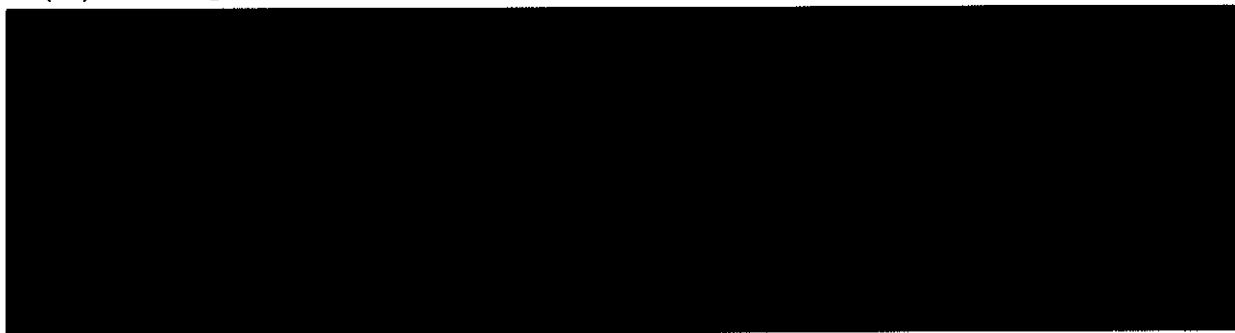
~~SECRET//NOFORN~~

- b. With respect to any other communication where it is apparent to NCTC personnel that the communication is between a person and the person's attorney (or someone acting on behalf of the attorney) concerning legal advice being sought by the former from the latter, such communications relating to foreign intelligence information may be retained and disseminated within the U.S. Intelligence Community if the communications are specifically labeled as being privileged. Such communications may not be disseminated outside of the U.S. Intelligence Community without the prior approval of the Attorney General or Attorney General's designee.
- c. If FBI informs NCTC that particular communications are privileged, NCTC will adopt FBI's conclusion that such communications are privileged. If FBI informs NCTC that particular communications, categories of communications, or communications acquired from particular facilities may contain privileged communications, NCTC will maintain a record of such notice and will maintain such communications in a manner that alerts personnel accessing the communications that they may contain privileged content.

**D. ~~(S)~~ DISSEMINATION AND DISCLOSURE**

- 1. ~~(S)~~ NCTC may disseminate to federal, state, local, or tribal agencies or officials with responsibilities relating to national security that require access to foreign intelligence information any nonpublicly available information concerning an unconsenting United States person that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or necessary to assess the importance of foreign intelligence information, if 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 manner because such person's identity is necessary to understand foreign intelligence information or assess its importance, NCTC may disseminate that identity. NCTC may only disseminate FISA-acquired or FISA-derived information received from FBI in raw form as provided herein.
- 2. ~~(S)~~ Information that is evidence of a crime that has been, is being, or is about to be committed, but is not foreign intelligence information, may only be retained or disseminated for law enforcement purposes. As to all such disseminations, see Section A(10) above regarding additional agreements between NCTC and FBI.

3.



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

a.

A large black rectangular redaction box covering the content of item 'a'.

b.

A very large black rectangular redaction box covering the content of item 'b' and extending down to item 'c'.

c.

4. ~~(S//NF)~~ In addition to disseminations otherwise permitted by these procedures, NCTC may disclose to FBI, the Central Intelligence Agency (CIA), and/or the National Security Agency (NSA) raw information, provided that the receiving agency handle such raw information in accordance with FISC-approved minimization procedures applicable to that agency. All disclosures of raw information under this paragraph shall be conducted in a manner that clearly indicates to the receiving agency or agencies that the disclosed information is raw FISA-acquired information collected by FBI.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

5. ~~(S)~~ **Procedures for technical or linguistic assistance.** NCTC may receive information or communications that, because of their technical or linguistic content, may require further analysis by other federal agencies (collectively, "assisting federal agencies") to assist NCTC in determining their meaning or significance. Consistent with the other provisions of these procedures, NCTC is authorized to disclose FISA-acquired information to assisting federal agencies for further processing and analysis. The following restrictions apply with respect to any materials so disseminated:
- a. Disclosure to assisting federal agencies will be solely for translation or analysis of such information or communications. Assisting federal agencies will make no use of any information or any communication of or concerning any person except to provide technical or linguistic assistance to NCTC. ~~(S)~~
  - b. Disclosure will be only to those personnel within assisting federal agencies involved in the translation or analysis of such information or communications. The number of such personnel shall be restricted to the extent reasonably feasible. There shall be no further disclosure of this raw data within assisting federal agencies. ~~(S)~~
  - c. Assisting federal agencies shall make no permanent agency record of information or communications of or concerning any person referred to in FISA-acquired information disclosure by NCTC to assisting federal agencies, provided that assisting federal agencies may maintain such temporary records as are necessary to enable them to assist NCTC with the translation or analysis of such information. Records maintained by assisting federal agencies for this purpose may not be disclosed within the assisting federal agency, except to personnel involved in providing technical assistance to NCTC. ~~(S)~~
  - d. Upon the conclusion of such technical assistance to NCTC, all copies in any form of the FISA-acquired information will either be returned to NCTC or be destroyed, with an accounting of such destruction made to NCTC. ~~(S)~~
  - e. Any information that assisting federal agencies provide to NCTC as a result of such technical assistance may be disseminated by NCTC in accordance with the applicable minimization procedures. ~~(S)~~
6. ~~(S)~~ **Caveats.**
- a. Disseminations pursuant to Section D(1) or (2) by NCTC of FBI-collected FISA-acquired or FISA-derived information to federal, state, local, or tribal agencies or officials of or within the United States will bear a legend indicating, in substance, that: (i) the dissemination includes FISA-acquired or FISA-derived information collected by the FBI; (ii) the information, and any information derived therefrom, may only be used in, or in connection with, a domestic or foreign legal or administrative proceeding with the advance authorization of the Attorney General; (iii) any recipient interested in obtaining such authorization should contact FBI Headquarters; and (iv) any reproduction, dissemination, or communication (including but not limited to oral

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

briefings) of the disseminated information must be accompanied by a statement of these restrictions. Wherever feasible, NCTC will indicate which portions of documents contain FBI-collected FISA-acquired or FISA-derived information, to permit recipients to identify the information to which the FISA-related restrictions apply.

- b. All disseminations pursuant to Section D(3) by NCTC of FBI-collected FISA-acquired information will bear a legend indicating that the disseminated information may not be used or disseminated for any purpose by the recipient without the advance authorization of the Director of NCTC. Such legend need not indicate that the information was collected by FBI or was acquired pursuant to FISA. NCTC shall refer any request for authorization to use or disseminate FBI-collected FISA-acquired information to FBI Headquarters. This caveat and authorization process may also be substituted for the caveat and process in paragraph D(6)(a) for specific disseminations under circumstances (e.g., security concerns) that require nondisclosure of the agency that collected the disseminated information, or nondisclosure of the authority pursuant to which the disseminated information was acquired.
- c. Any dissemination made for a law enforcement purpose must bear a caveat stating, in substance, that the disseminated information may only be used in a legal or administrative proceeding with the advance authorization of the Attorney General.
- d. In addition to disseminations otherwise authorized under these procedures, NCTC may disseminate foreign intelligence information as defined at 50 U.S.C. § 1801(e) to federal, state, local, territorial, and tribal authorities, foreign officials and entities, and private sector entities that have a substantial bearing on homeland security for the purposes of and in accordance with Homeland Security Presidential Directive 6 and the Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism and applicable addenda thereto. Disseminations made pursuant to this provision are not subject to the caveat requirements set forth above in sections 6(a), (b), and (c).

E.



1.

~~SECRET//NOFORN~~

2.

3.

4.

F. ~~(S)~~ TRAINING, DATA STORAGE AND ACCESS, AND OVERSIGHT

1. ~~(S)~~ In consultation with NSD, NCTC will develop and deliver training regarding the applicable procedures to ensure personnel responsible for applying these procedures understand their responsibilities under these procedures.
2. ~~(S)~~ NCTC will ensure that raw information is only accessible to NCTC employees (as defined above) who have received the required training. NCTC will maintain logs or records of users authorized to access the raw information. NCTC will ensure that the marking, moving, or other identification of information received in raw form as meeting the standard set forth in paragraph B(3) is tracked and auditable, and that a user who moves a particular communication is identifiable.
3. ~~(S)~~ All FISA-acquired information retained by NCTC will be retained under appropriately secure conditions that limit access to such information only to authorized users and recipients in accordance with these procedures. The retention procedures herein apply to FISA-acquired information retained in any form. NCTC electronic and data storage systems may permit multiple authorized users to access the information.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

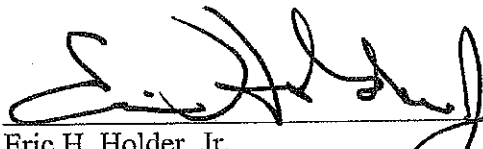
simultaneously or sequentially and to share or transfer FISA-acquired information between systems.

4. ~~(S)~~ NCTC's compliance with these procedures shall be subject to periodic review by NSD. NSD shall be permitted access to all information and materials necessary to evaluate NCTC's compliance with these procedures, consistent with the need to protect the security of NCTC sources and methods. NCTC shall maintain copies of disseminations of nonpublicly available information concerning unconsenting United States persons and make such disseminations available for review by NSD.
5. ~~(S)~~ NCTC shall refer all significant questions relating to the interpretation of these procedures to NSD.

**G. (U) REVIEW OF PROCEDURES**

~~(S)~~ The Attorney General, or a designee, in consultation with NCTC, shall review these procedures and determine whether they remain appropriate in light of the technology and practices used by NCTC no later than five years from the date these procedures are signed, 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.

4-20-12  
Date

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

~~SECRET//NOFORN~~



U.S. Department of Justice

National Security Division

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

2014 JUL 30 PM 4:47

~~TOP SECRET//SI//NOFORN~~

Washington, D.C. 20530

LEEANN FLYNN HALL  
CLERK OF COURT

July 30, 2014

The Honorable Thomas F. Hogan  
United States Foreign Intelligence Surveillance Court  
333 Constitution Avenue, N.W.  
Washington, D.C. 20001

Re: ~~(S)~~ Update Regarding Compliance Incidents  
Reported in the December 2013, March 2014, and  
June 2014 Section 702 Quarterly Reports

Dear Judge Hogan:

~~(S)~~ On July 17, 2014, representatives from the National Security Division (NSD) met with Court staff to discuss certain compliance incidents reported in the December 2013, March 2014, and June 2014 Section 702 Quarterly Reports. Below is the requested information.

1. ~~(S)~~ Facilities That Remain Tasked Pursuant to Section 702 While Questions are Resolved Concerning Documentation and/or Foreignness Issues

~~(S//NF)~~ There are occasional instances in which the National Security Agency's (NSA) post-tasking checks or NSD's review of tasking sheets reveals a potential issue with the pre-tasking foreignness checks performed by the analyst. For example, the June 2014 Quarterly Report identified the following issue with respect to [REDACTED]

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

~~TOP SECRET//SI//NOFORN~~

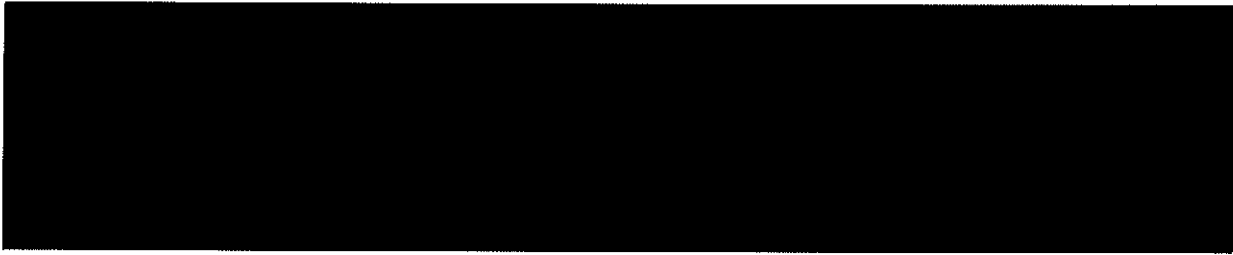
Classified by: Tashina Gauhar, Deputy Assistant  
Attorney General, NSD, DOJ

Reason: 1.4(e)

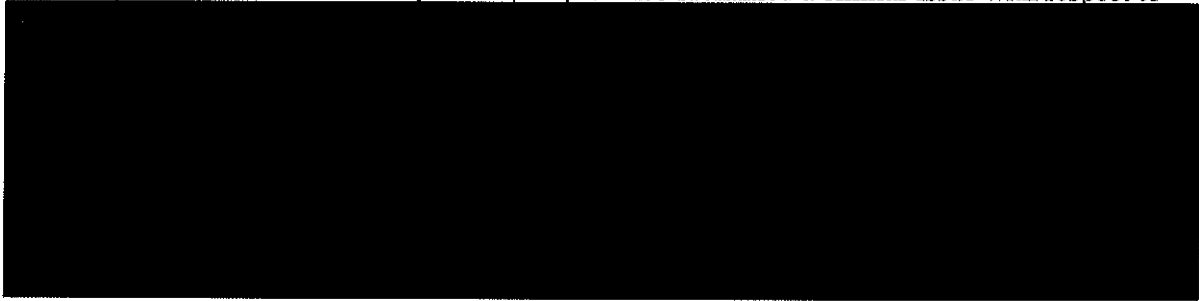
Declassify on: 30 July 2039

[REDACTED] 116742, 108444, 118965

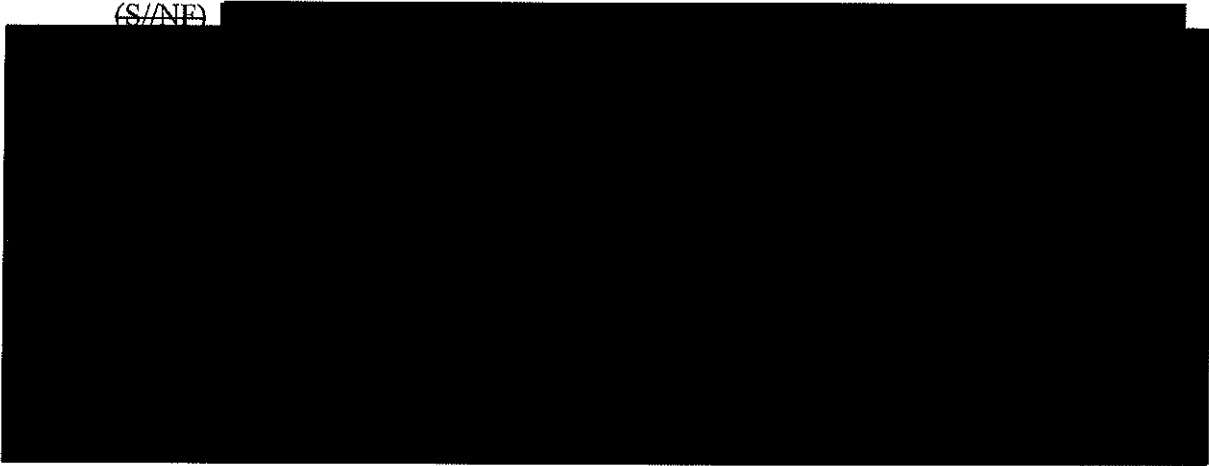
~~TOP SECRET//SI//NOFORN~~



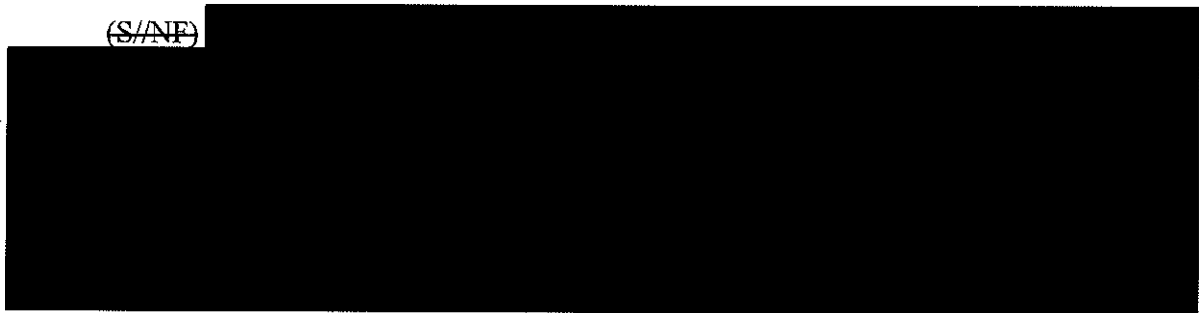
(S//NF) The June 2014 Quarterly Report also identified a similar issue with respect to



(S//NF)



(S//NF)



<sup>1</sup> (S)



~~TOP SECRET//SI//NOFORN~~

**TOP SECRET//SI//NOFORN**

(S//NF) As with any other possible compliance incident, if there is an issue with the pre-tasking foreignness justification, the Government immediately starts to investigate the possible instance of non-compliance. If the Government discovers that the pre-tasking foreignness justification was sufficient, that potential incident is closed. If, however, the pre-tasking record was incomplete (a documentation error) or the pre-tasking checks were not properly conducted (a tasking error), the incident will be reported/documentated to the Court. [REDACTED]

[REDACTED]

(S//NF) [REDACTED]

2. (S) [REDACTED]

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

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

<sup>2</sup> (S) [REDACTED]

**TOP SECRET//SI//NOFORN**

~~TOP SECRET//SI//NOFORN~~

[REDACTED]

(S) Subsequent to the June 2014 Quarterly Report, NSA advised [REDACTED]  
[REDACTED]

**3. (U) Notification Delays**

(S) NSA's targeting procedures require NSA to report certain incidents to NSD and ODNI even if these incidents do not involve noncompliance with the targeting procedures. Specifically, NSA is required to terminate acquisition and notify NSD and ODNI if [REDACTED]

[REDACTED]

(S) During the July 17, 2014, meeting with the Court, it was noted that there had been a significant improvement in the timeliness of NSA reporting of these incidents. The below information responds to the Court's request for certain metrics regarding the notification delays. Specifically, in the December 2013, March 2014, and June 2014 Quarterly Reports, the Government identified [REDACTED] instances, respectively, in which NSA did not provide NSD and ODNI the required notification within [REDACTED]. During the time periods covered by the December 2013, March 2014, and June 2014 Section 702 Quarterly Reports, there were approximately [REDACTED] matters, respectively, reported to NSD that were subject to the [REDACTED] reporting period.<sup>3</sup> For the time periods covered by the December 2013, March 2014, and June 2014 Section 702 Quarterly Reports, NSA exceeded the [REDACTED] notification requirement in 42%, 17%, and 3% of those matters, respectively.

**4. (U) Unauthorized Access to Section 702-Acquired Data**

(S//NF) On June 17, 2014, in a notice filed with the Court, and in the June 2014 Quarterly Report, the Government advised the Court of an incident involving certain NSA personnel who had gained access to unminimized Section 702-acquired information without the appropriate training. More specifically, NSA reported that on [REDACTED], while discussing operational matters, [REDACTED] personnel [REDACTED] had been put on an e-mail distribution list that regularly received unminimized Section 702-acquired

<sup>3</sup> (S) For additional context, during the time periods covered by the December 2013, March 2014, and June 2014 Quarterly Reports, NSD and ODNI received [REDACTED] incident reports, respectively. This means, for example, that of the [REDACTED] matters reported to NSD and ODNI during the period of time covered by the June 2014 Quarterly Report, [REDACTED] (80%) were properly reported within the required the [REDACTED]

~~TOP SECRET//SI//NOFORN~~

**TOP SECRET//SI//NOFORN**

information.<sup>4</sup> Some personnel [REDACTED] had not received the appropriate training to permit access to unminimized Section 702 data. As of the June 2014 Quarterly Report, NSA advised that it was difficult to assess the scope of information provided to personnel [REDACTED] given the passage of time and [REDACTED]. NSA also advised, however, that as of [REDACTED]<sup>5</sup> all personnel [REDACTED] were removed from the e-mail distribution list. NSA further advised that all personnel [REDACTED] have been instructed to delete the relevant e-mails. Given the operational practices of [REDACTED], NSA assessed that it is unlikely that personnel further disseminated any unminimized Section 702 data.

(S//NF) Subsequent to the June 2014 Quarterly Report, and in response to questions from the Court, NSA advised that certain NSA offices supporting [REDACTED] targets have an e-mail distribution list for Section 702-trained personnel. NSA employees [REDACTED] were inadvertently added to the distribution list in the above incident in approximately December 2012. NSA further advises that although Section 702-trained personnel who were on the distribution list recognized the information as Section 702-acquired, the e-mail distributions in this case did not specifically identify the collection as Section 702. Of the personnel [REDACTED], NSA has identified [REDACTED] non-Section 702-trained individuals who had access to the e-mail distribution list.<sup>6</sup> All [REDACTED] individuals have confirmed that all relevant e-mails have been deleted from their systems. As these [REDACTED] individuals advised that they did not read any of the e-mail messages containing unminimized Section 702 information,<sup>7</sup> NSA remains confident that no improper dissemination of the Section 702-acquired data resulted from this incident.

##### 5. (S) Review of Section 702 Collection Without the Use of a Required Review Team

(S//NF) Section III.E.1. of the Minimization Procedures Used by the Federal Bureau of Investigation (FBI) in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended, requires that FBI "implement procedures that ensure that the target's attorney-client privilege is protected." Specifically, Section III.E.1.a. provides for "[e]stablishment 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

<sup>4</sup> (S//NF) The distribution list was developed to encourage collaboration among NSA analysts working similar targets, and was not accessible to non-NSA personnel.

<sup>5</sup> (U) In the June 2014 notice and Quarterly Report, the Government incorrectly identified this date as [REDACTED]

<sup>6</sup> (S) As noted above, NSA advised that it is difficult to assess the full scope of information provided to personnel [REDACTED] including the total number of e-mails received, given the passage of time and [REDACTED]

<sup>7</sup> (S)-A Section 702-training analyst recognized the issue in [REDACTED]

**TOP SECRET//SI//NOFORN**



~~TOP SECRET//SI//NOFORN~~

surveillance or search of a target who is charged with a crime pursuant to the United States Code.”

(S//NF) In separate notices, and in the March and June 2014 Quarterly Reports, the Government identified [redacted] in which FBI personnel continued to review communications [redacted].<sup>8</sup> In a February notice and the March 2014 Quarterly Report, the Government reported an incident involving [redacted] accounts. Specifically, the user of [redacted]

but FBI monitored the [redacted]

FBI established the necessary [redacted]

(S//NF) In an April 2014 notice and the June 2014 Quarterly Report, the Government identified a separate incident involving [redacted] accounts. Specifically, the user of e-mail accounts [redacted]

collection from the [redacted]

FBI received [redacted]

(S) FBI currently requires specific training prior to any agent or analyst receiving authorization to review raw Section 702-acquired communications. This training includes a full discussion of the Section 702 minimization procedures, including attorney-client communications, and FBI’s policy guide. In addition to this training, NSD conducts reviews at approximately 31 FBI field offices each year. As part of those reviews, NSD lawyers provide

<sup>8</sup> (S) There have been additional, subsequent instances of this type of compliance incident.

~~TOP SECRET//SI//NOFORN~~

**TOP SECRET//SI//NOFORN**

additional training on Section 702 issues, and specifically address possible attorney-client issues. Finally, whenever any compliance incident arises, FBI ensures that the relevant personnel receive the necessary reminders. While there have been isolated instances in which FBI personnel have not established the necessary review teams, the Government believes that these were the result of individual failures or confusion and not a systematic issue. NSD and FBI will continue to provide training on the attorney-client communication provisions of the minimization procedures.

**6. (U) FBI Incomplete Purges**

(S//NF) In a May 7, 2014, notice and the June 2014 Quarterly Report, the Government advised the Court of [REDACTED] when FISA-acquired information has been [REDACTED]. The Court requested additional information on this matter during the July 17, 2014 meeting, and the Government filed a supplemental notice with the Court on July 25, 2014, that provides additional information on this issue.

**7. (S) NSA Incomplete Purges of [REDACTED]**

(S//SI//NF) In a [REDACTED] notice and the March and June 2014 Quarterly Reports, the Government advised the Court of a gap in NSA's purge discovery processes that affects purges of information under certain circumstances that, [REDACTED]

[REDACTED]

(S//NF) [REDACTED]

**TOP SECRET//SI//NOFORN**

~~TOP SECRET//SI//NOFORN~~

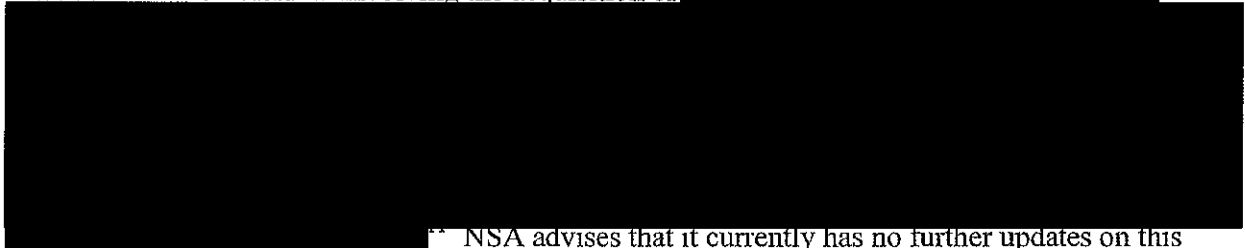


8. (S) [REDACTED] Incident

(S//NF) In February 2013, March 2013, August 2013, and July 2014 notices, and in the March 2013, June 2013, September 2013, December 2013, March 2014, and June 2014 Quarterly reports, the Government provided information regarding NSA's efforts to evaluate transcripts stored in a database [REDACTED] that may have been retained longer than permitted. NSA is using the identifying criteria that [REDACTED] used to delete the transcripts to identify whether any transcripts exist in [REDACTED] will use these criteria to identify and delete any transcripts identified, and the results of this action will be reported to the Court. To date, NSA has not identified any transcripts from [REDACTED] that have been sent to [REDACTED]

9. (S) Overcollection Incident Related to [REDACTED]

(S//NF) In a November 2011 notice, and in the December 2011, March 2012, June 2012, September 2012, December 2012, March 2013, June 2013, September 2013, December 2013, March 2014, and June 2014 Quarterly reports, the Government provided information regarding an overcollection incident involving the acquisition of [REDACTED]



[REDACTED] NSA advises that it currently has no further updates on this matter.

10. (S) FBI's [REDACTED] Systems

(S//NF) In an October 2013 notice and the December 2013 Quarterly Report, the Government advised the Court that there were multiple instances in which copies of [REDACTED] were provided to requesting FBI case agents after the information was [REDACTED] Agents would then place copies of the [REDACTED] information on [REDACTED] for additional analysis. On November 14, 2013,

<sup>11</sup> (S) In the prior Quarterly Reports, the Government incorrectly advised that NSA was continuing to sequester all [REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

the Attorney General and Director of National Intelligence approved amended certifications which included amended minimization procedures for FBI that permit FBI to process and retain raw Section 702-acquired information, subject to certain conditions and restrictions. [REDACTED]

The Court approved these minimization procedures on December 13, 2013.

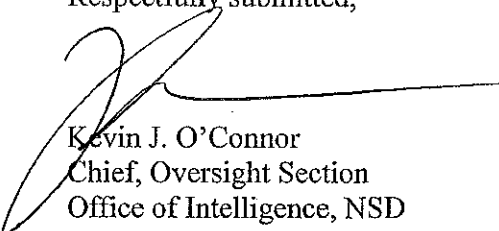
(S//NF) According to Section IV.B.2 of these amended procedures:

The FBI will implement procedures regarding storage of FISA-acquired information in an [REDACTED] database, which will require the FBI to (1) maintain adequate records of all persons who have been granted access to FISA-acquired information in an ad hoc database, (2) track the FISA-acquired information in an ad hoc database that has been determined to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime, and (3) maintain adequate records to ensure FBI can comply with the destruction requirement discussed in subparagraph B. 1. of this section.

The FBI adopted the procedures required by this section as of February 25, 2014.

(U) NSA and FBI have verified the accuracy of the relevant information in this letter.

Respectfully submitted,

  
Kevin J. O'Connor  
Chief, Oversight Section  
Office of Intelligence, NSD  
U.S. Department of Justice

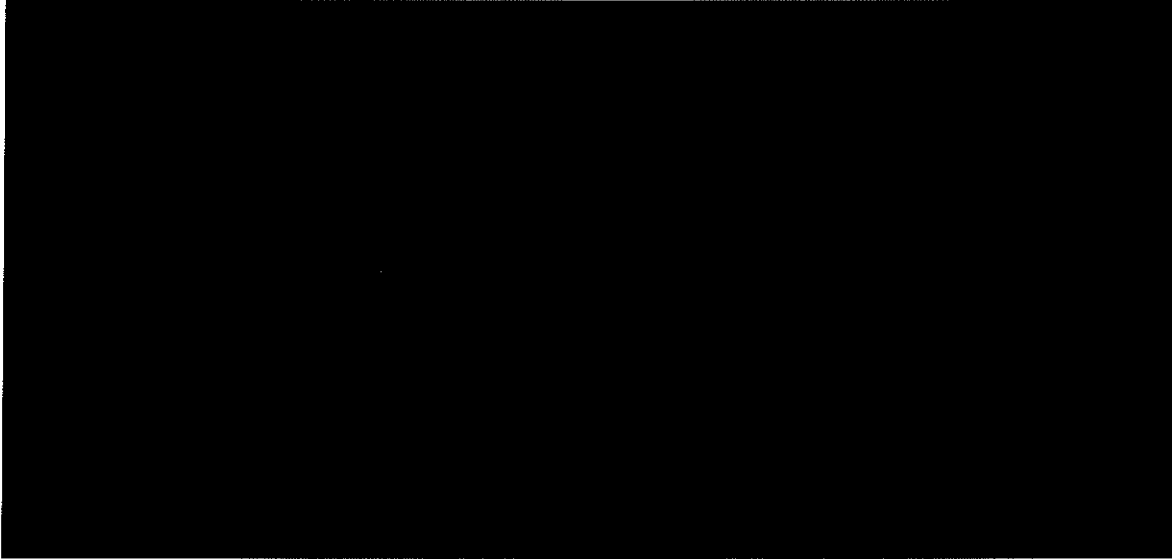
~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



**MEMORANDUM OPINION AND ORDER**

This matter is before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on the “Government’s Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications,” which was filed on July 28, 2014 (“July 28, 2014 Submission”). For the reasons explained below, the government’s request for approval is granted, subject to certain reporting requirements. The Court’s approval of the certifications, amended certifications, and accompanying targeting procedures and minimization procedures is set out in separate orders that are being entered contemporaneously herewith.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

I. BACKGROUND

The July 28, 2014 Submission includes [REDACTED] certifications that have been executed by the Attorney General (“AG”) and the Director of National Intelligence (“DNI”) pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), which is codified at 50 U.S.C. §

1881a: [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] certifications (collectively referred to as “the 2014 Certifications”) is accompanied by the supporting affidavits of the Acting Director of the National Security Agency (“NSA”), the Director of the Federal Bureau of Investigation (“FBI”), and the Director of the Central Intelligence Agency (“CIA”); two sets of targeting procedures, for use by the NSA and FBI respectively;<sup>1</sup> and four sets of minimization procedures, for use by the NSA, FBI, CIA, and the National Counterterrorism Center (“NCTC”), respectively.<sup>2</sup> The July 28 Submission also includes an explanatory memorandum prepared by the Department of Justice (“DOJ”) (“July 28, 2014 Memorandum”).

---

<sup>1</sup> The targeting procedures for [REDACTED] 2014 Certifications are identical. The targeting procedures for the NSA (“NSA Targeting Procedures”) appear as Exhibit A to [REDACTED] 2014 Certifications. The targeting procedures for the FBI (“FBI Targeting Procedures”) appear as Exhibit C to [REDACTED] 2014 Certifications.

<sup>2</sup> The minimization procedures for [REDACTED] 2014 Certifications are identical. The minimization procedures for the NSA (“NSA Minimization Procedures”) appear as Exhibit B to [REDACTED] 2014 Certifications. The minimization procedures for the FBI (“FBI Minimization Procedures”) appear as Exhibit D to [REDACTED] 2014 Certifications. The minimization procedures for the CIA (“FBI Minimization Procedures”) appear as Exhibit E to [REDACTED] 2014 Certifications. The minimization procedures for the NCTC (“NCTC Minimization Procedures”) appear as Exhibit G to [REDACTED] 2014 Certifications.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

FISC review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather, the Court also examines how the procedures have been and will be implemented. See, e.g., [REDACTED] Memorandum Opinion entered on April 7, 2009, at 22-24 (“April 7, 2009 Opinion”); [REDACTED], [REDACTED], Memorandum Opinion entered on Aug. 30, 2013, at 6-11 (“August 30, 2013 Opinion”). Accordingly, for purposes of its review of the July 28, 2014 Submission, the Court has examined quarterly compliance reports submitted by the government<sup>3</sup> since the most recent FISC review of Section 702 certifications and procedures was completed on December 13, 2013,<sup>4</sup> as well as individual notices of non-compliance relating to implementation of Section 702. Based on its review of these submissions, the Court, through its staff, orally conveyed a number of compliance-related questions to the government, to which the government has responded in writing.<sup>5</sup> On August 4, 2014, the Court conducted a hearing, which addressed certain revisions to the targeting and minimization procedures included in the July 28, 2014 Submission, as well as certain compliance matters.

[REDACTED] 2014 Certifications involves “the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence

---

<sup>3</sup> See Quarterly Reports to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on June 20, 2014; March 21, 2014; and Dec. 20, 2013.

<sup>4</sup> See [REDACTED] Memorandum Opinion entered on Dec. 13, 2013 (“December 13, 2013 Opinion”).

<sup>5</sup> See July 28, 2014 Memorandum at 18-22; Letter from Kevin J. O’Connor, Chief, Oversight Section, Office of Intelligence, National Security Division, U.S. Department of Justice, filed on July 30, 2014 (“July 30, 2014 Letter”).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

information.” [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] 2014 Certifications generally proposes to continue acquisitions of foreign intelligence information that are now being conducted under certifications that were made in 2013 (“the 2013 Certifications”). July 28, 2014 Memorandum at 2. The 2013 Certifications,

[REDACTED] were approved by the FISC on December 13, 2013. See December 13, 2013 Opinion.<sup>6</sup> The 2013

---

<sup>6</sup> More specifically, the 2013 Certifications were first submitted on July 31, 2013. The FISC approved the 2013 Certifications and accompanying minimization and targeting procedures on August 30, 2013. See August 30, 2013 Opinion. At that time, however, the Court was unable to make the statutory findings required to approve the accompanying amendments to minimization procedures governing information acquired under prior Section 702 certifications. See id. at 4 n.2. On November 15, 2013, the government filed amendments to all Section 702

(continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

Certifications, in turn, generally renewed authorizations to acquire foreign intelligence information under a series of certifications made by the AG and DNI pursuant to Section 702 that date back to 2008.<sup>7</sup> In its July 28, 2014 Submission, the government also seeks approval of amendments to the certifications in all of the Prior 702 Dockets, such that the NSA, CIA, and FBI henceforward will apply the same minimization procedures to information previously obtained under prior certifications as they will to information to be obtained under the 2014 Certifications. See July 28 Memorandum at 2-3; [REDACTED]

[REDACTED]<sup>8</sup>

II. REVIEW OF CERTIFICATIONS [REDACTED] AND OF THEIR PREDECESSOR CERTIFICATIONS AS AMENDED BY THE JULY 28, 2014 SUBMISSION.

The Court must review a certification submitted pursuant to Section 702 “to determine whether [it] contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court’s examination of [REDACTED] confirms that:

---

<sup>6</sup>(...continued)  
certifications that had been issued to that date, including the 2013 Certifications. See December 13, 2013 Opinion at 1-2. Those amendments, which provided for use of revised minimization procedures, were approved by the FISC. See *id.* at 2.

<sup>7</sup> See [REDACTED]  
[REDACTED] These dockets, together with [REDACTED] are collectively referred to as “the Prior 702 Dockets”).

<sup>8</sup> The July 28, 2014 Submission does not propose any changes to the minimization procedures applied by the NCTC. July 28, 2014 Memorandum at 3 n.3.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

- (1) the certifications have been made under oath by the AG and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see [REDACTED]
- (2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see [REDACTED]
- (3) as required by 50 U.S.C. § 1881a(g)(2)(B), [REDACTED] certifications is accompanied by the applicable targeting procedures and minimization procedures;
- (4) [REDACTED] certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);<sup>9</sup> and
- (5) [REDACTED] certifications includes an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D) – specifically, the certifications become effective on August 28, 2014, or on the date upon which this Court issues an order concerning the certification under § 1881a(i)(3), whichever is later, see [REDACTED]<sup>10</sup>

The Court therefore finds that [REDACTED]

[REDACTED] contain all the required statutory elements. See 50 U.S.C. § 1881a(i)(2)(A).

Similarly, the Court has reviewed the certifications in the Prior 702 Dockets, as amended by the 2014 Certifications, and finds that they also contain all the elements required by the statute. Id.<sup>11</sup>

---

<sup>9</sup> See Affidavits of Richard H. Ledgett, Jr., Acting Director, NSA (Tab 1 to [REDACTED] (“Ledgett Affidavits”); Affidavits of James B. Comey, Director, FBI (Tab 2 to [REDACTED] (“Comey Affidavits”); and Affidavits of John O. Brennan, Director, CIA (Tab 3 to [REDACTED] (“Brennan Affidavits”).

<sup>10</sup> The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no “exigent circumstances” determination under Section 1881a(c)(2).

<sup>11</sup> The effective dates for the amendments to the certifications in the Prior 702 Dockets (continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

### III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is also required, pursuant to 50 U.S.C. § 1881a(i)(2)(B) and (C), to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). Pursuant to 50 U.S.C. § 1881a(i)(3)(A), the Court further determines whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

Section 1881a(d)(1) requires targeting procedures that are “reasonably designed” to “ensure that any acquisition authorized under [the certification] 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.” In addition to these statutory requirements, the government uses the targeting procedures as a means of complying with Section 1881a(b)(3), which provides that acquisitions “may not intentionally target a United States person reasonably believed to be located outside the United States.” See NSA Targeting Procedures at 1, 3-4, 7; FBI Targeting Procedures at 1-4. The FISC considers steps taken pursuant to these procedures to avoid targeting United States persons as relevant to its assessment of whether the procedures are consistent with the requirements of the Fourth Amendment. See Docket No. 702(i)-08-01, Memorandum Opinion entered on Sept. 4, 2008, at 14 (“September 4, 2008 Opinion”).

---

<sup>11</sup>(...continued)  
are the same as the effective dates for the 2014 Certifications. See [REDACTED]  
[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

Section 1881a(e)(1) requires minimization procedures that “meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4).” The applicable statutory definition is fully set out at pages 15-16 below.

A. As Written, the NSA and FBI Targeting Procedures Comply With Statutory Requirements and Are Reasonably Designed to Prevent the Targeting of United States Persons.

Under the procedures adopted by the government, NSA is the lead agency in making targeting decisions under Section 702. Pursuant to its targeting procedures, NSA may target for acquisition a particular “selector” (i.e., a facility such as a telephone number or email address). The FBI Targeting Procedures come into play in cases where the government [REDACTED] [REDACTED] that has been tasked under the NSA Targeting Procedures. See FBI Targeting Procedures at 1. “Thus, the FBI Targeting Procedures apply in addition to the NSA Targeting Procedures, whenever [REDACTED] are acquired.” September 4, 2008 Opinion at 20 (emphasis in original).

In comparison to the targeting procedures previously approved by the FISC and now being implemented, the July 28, 2014 Submission presents two substantive revisions to the NSA Targeting Procedures and one substantive revision to the FBI Targeting Procedures.

1. Defining the Target of Acquisition

The first revision to the NSA Targeting Procedures concerns who will be regarded as a “target” of acquisition or a “user” of a tasked facility for purposes of those procedures. As a general rule, and without exception under the NSA targeting procedures now in effect, any user of a tasked facility is regarded as a person targeted for acquisition. This approach has sometimes

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

resulted in NSA's becoming obligated to detask a selector when it learns that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] See July 28, 2014 Memorandum at 4-5.

The relevant revision would permit continued acquisition for such a facility. It provides that

[REDACTED]

NSA Targeting Procedures at 1. In support of this revision, the government contends that, in the narrow circumstances described in this provision, [REDACTED]

[REDACTED]. See July 28, 2014 Memorandum at 5-6.

For purposes of electronic surveillance conducted under 50 U.S.C. §§ 1804-1805, the "target" of the surveillance "is the individual or entity . . . about whom or from whom information is sought." In re Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, at 73 (1978)). As the FISC has previously observed, "[t]here is no reason to think that a different meaning should apply" under Section 702. September 4, 2008 Memorandum Opinion at 18 n.16. It is evident that the Section 702 collection on a particular facility does not seek information from or about [REDACTED]

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

**TOP SECRET//SI//ORCON/NOFORN**

[REDACTED]

[REDACTED]

[REDACTED]

This amended provision might be read literally to apply where [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] But those circumstances fall outside the accepted rationale for

this amendment. The provision should be understood to apply only where [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Finally, implementation of this provision is not expected to slow the required analysis of whether tasked facilities have come to be used by a United States person or someone located in the United States. See NSA Targeting Procedures at 6-7. That post-tasking analysis relies importantly on [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

[REDACTED] See July 28, 2014

Memorandum at 7.

2. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] *Id.*<sup>12</sup> NSA remains responsible for routinely conducting separate [REDACTED] reviews for indicia that a user of a targeted facility is in the United States.<sup>13</sup>

Because the only change effected by this revision is to assign [REDACTED] to the agency that is most fully engaged in the review of the same communications for foreign intelligence purposes, the Court concludes that this revision does not present problems in finding the NSA Targeting Procedures satisfy the requirements of Section 1881a(d)(1) and are reasonably designed to prevent the targeting of United States persons.

3. [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

---

<sup>12</sup> [REDACTED]  
[REDACTED]

<sup>13</sup> See NSA Targeting Procedures at 6-7; July 28, 2014 Memorandum at 7; see also, e.g., August 30, 2013 Opinion at 7 (government had represented that [REDACTED] and reviewed by experienced NSA analysts [REDACTED]; Court had “expressly relied upon these assurances in concluding that NSA’s targeting procedures are reasonably designed to ensure that targeting is limited to non-U.S. persons reasonably believed to be located outside the United States and consistent with the Fourth Amendment”).

~~TOP SECRET//SI//ORCON/NOFORN~~



~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]

[REDACTED]

[REDACTED] 14 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

14 [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

4. Conclusion

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA Targeting Procedures and the FBI Targeting Procedures, as written, are reasonably designed, as required by Section 1881a(d)(1): (1) to ensure that any acquisition authorized under the 2014 Certifications is limited to targeting persons reasonably believed to be located outside the United States, and (2) 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. Moreover, for the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA and FBI Targeting Procedures, as written, are reasonably designed to prevent United States persons from being targeted for acquisition – a finding that is relevant to the Court's analysis of whether those procedures are consistent with the requirements of the Fourth Amendment. See pages 38-40 below.

B. As Written, the FBI, NSA, and CIA Minimization Procedures Comply With Statutory Requirements.

The FBI, NSA, and CIA all have access to unreviewed information obtained under Section 702. Each agency is governed by its own set of minimization procedures in its handling of Section 702 information. Under Section 1881a(i)(2)(C), the Court must determine whether the agencies' respective minimization procedures included as part of the July 28, 2014 Submission meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

1801(h) or 1821(4), as appropriate. Sections 1801(h) and 1821(4) define "minimization procedures" in pertinent part as:

(1) 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 [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;<sup>[15]</sup>

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is

---

<sup>15</sup> Section 1801(e) defines "foreign intelligence information" 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 a 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//SI//ORCON/NOFORN~~

being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

50 U.S.C. § 1801(h); see also id. § 1821(4).<sup>16</sup>

In comparison to the FBI minimization procedures now in effect, the FBI Minimization Procedures before the Court include three substantive revisions. The CIA and NSA Minimization Procedures now before the Court include one substantive revision, which pertains to [REDACTED]

1. Provision of Information by the FBI to the National Center for Mission and Exploited Children

The FBI Minimization Procedures include new provisions respecting the transmittal of information to the National Center for Missing and Exploited Children (NCMEC). See July 28, 2014 Memorandum at 10-13; FBI Minimization Procedures at 28, 30-31. Specifically, the FBI may “disseminate, for law enforcement purposes, FISA-acquired information<sup>[17]</sup> that reasonably appears to be evidence of a crime related to child exploitation material, including child pornography, to [the NCMEC].” FBI Minimization Procedures at 28. “The FBI may also disclose, for the purpose of obtaining technical or linguistic assistance, FISA-acquired

---

<sup>16</sup> The definitions of “minimization procedures” set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to “the purposes . . . of the particular physical search”) (emphasis added). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h)).

<sup>17</sup> For purposes of these procedures, “FISA-acquired information” refers to communications and information acquired under Section 702. See FBI Minimization Procedures at 1.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

information that reasonably appears to be evidence of a crime related to child exploitation material, including child pornography, to NCMEC for further processing and analysis.” Id. at 30. Such disclosures to obtain technical or linguistic assistance are subject to several restrictions: for example, the NCMEC may not make use of the information except to provide such assistance; shall restrict such information to personnel involved in providing such assistance; and may not retain such information permanently. Id. at 30-31. These restrictions are similar to those now in effect when the FBI discloses unreviewed Section 702 information to other federal agencies for the purpose of obtaining technical or linguistic assistance. See FBI minimization procedures submitted on Nov. 15, 2013, as Exhibit D to the amended 2013 Certifications at 29-30 (“2013 FBI Minimization Procedures”).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The FISC

stated:

Congress established NCMEC in 1984 as a non-governmental organization and it is funded through grants administered by the Department of Justice. One of its purposes is to assist law enforcement in identifying victims of child pornography and other sexual crimes. Indeed, Congress has mandated Department of Justice coordination with NCMEC on these and related issues. Furthermore, this Court has approved modifications to [minimization procedures] in individual cases to permit the Government to disseminate information to NCMEC. Because of its unique role as a non-governmental organization with a law enforcement function, and because it will be receiving what reasonably

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

appears to be evidence of specific types of crimes for law enforcement purposes, the [proposed amendments] comply with FISA under Section 1801(h)(3).

[REDACTED] The Court adopts the same reasoning and finds that the NCMEC-related amendments to the FBI Minimization Procedures under Section 702 comport with the applicable statutory definition of “minimization procedures.”<sup>18</sup>

## 2. Provision of Information to Mitigate Serious Harm

The FBI minimization procedures now in effect permit the FBI to disseminate information that reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime and that it reasonably believes may assist in the mitigation or prevention of computer intrusions or attacks to private entities or individuals that have been or are at risk of being victimized by such intrusions or attacks, or to private entities or individuals . . . capable of providing assistance in mitigating or preventing such intrusions or attacks. Wherever reasonably practicable, such dissemination should not include United States person identifying information unless the FBI reasonably believes it is necessary to enable the recipient to assist in the mitigation or prevention of computer intrusions or attacks.

2013 FBI Minimization Procedures at 32 (emphasis added).<sup>19</sup>

<sup>18</sup> [REDACTED]

<sup>19</sup> The FISC first approved a version of this provision under Section 702 on September 20, 2012, in connection with a prior Section 702 certification. See [REDACTED] Memorandum opinion entered on Sept. 20, 2012, at 22 (“September 20, 2012 Opinion”). At that time, the FISC noted that the provision at issue [REDACTED]

(continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

The government anticipates situations that would require dissemination of Section 702 information to someone in the private sector in order to mitigate other forms of serious harm, such as “a plot to destroy a building or monument.” See July 28, 2014 Memorandum at 16. The FBI Minimization Procedures now before the Court would permit the FBI to make certain disseminations to the private sector that are unrelated to computer intrusion or attack.

Specifically, the FBI could disseminate

information that reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime to a private individual or entity in situations where the FBI determines that said private individual or entity is capable of providing assistance in mitigating serious economic harm or serious physical harm to life or property. Wherever reasonably practicable, such dissemination should not include United States person identifying information unless the FBI reasonably believes it is necessary to enable the recipient to assist in the mitigation or prevention of the harm. The FBI will report to [the DOJ, National Security Division (NSD)] all disseminations made pursuant to this paragraph within ten business days of such dissemination.

FBI Minimization Procedures at 33. Although the procedures currently authorize the FBI to act in apparent departure from their requirements in order “to protect against an immediate threat to human life” under circumstances where it is not feasible to obtain timely modification of the procedures, see id. at 3, this new provision enables the FBI to disseminate information to private parties in less extreme cases.

---

<sup>19</sup>(...continued)

 The FISC approved the current version of this provision under Section 702 on August 30, 2013. See August 30, 2013 Opinion at 17-19.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

The definition of “minimization procedures” at Section 1801(h) does not speak specifically to the circumstances warranting dissemination to private sector individuals or entities. That definition does, however, provide that such procedures should be “reasonably designed” to prohibit dissemination of United States person information, “consistent with the need of the United States” to “disseminate foreign intelligence information.” See Section 1801(h)(1). “Foreign intelligence information,” in turn, is defined in substantial part by reference to several types of harm threatened by foreign powers and their agents (e.g., sabotage and acts of international terrorism) against which foreign intelligence information may be used to protect. See Section 1801(e)(1) (quoted in note 15 above). In combination, these definitions suggest that foreign intelligence information may be disseminated to responsible parties – including those in the private sector – who are in a position to mitigate serious harm, and that such disseminations may include United States person information when necessary to mitigate that harm.<sup>20</sup> Moreover, FISA’s legislative history expressly contemplates that information may be disseminated to the private sector in appropriate cases.<sup>21</sup> Accordingly, the Court concludes that this provision is consistent with the statute’s minimization requirements.

---

<sup>20</sup> Similarly, disseminations of evidence of a crime to private individuals and entities so that they can mitigate serious harm would serve a law enforcement purpose and for that reason fall under Section 1801(h)(3).

<sup>21</sup> “Federal agents may learn of a terrorist plot to kidnap a business executive. Certainly in such cases they should be permitted to disclose such information to the executive and his company in order to provide for the executive’s security.” H.R. Rep. 95-1283, at 88 (1978).

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

3. Preservation of Information for Litigation Purposes by the FBI

As a general rule, Section 702 information retained by the FBI that has not been “identified as information that reasonably appears to be foreign intelligence, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime” is subject to a retention/destruction schedule. See FBI Minimization Procedures at 20-21.<sup>22</sup> The FBI Minimization Procedures now before the Court would permit the FBI to retain information otherwise subject to destruction under this schedule if “the FBI and NSD determine that such information is reasonably believed to be necessary for, or potentially discoverable in, administrative, civil, or criminal litigation. Such determination shall be made in writing and shall identify the specific information to be retained and the particular litigation for which it is retained.” Id. at 21-22. Information retained under this provision may only be accessed for litigation-related purposes by personnel working on the particular litigation in question. Id. The FBI shall promptly destroy the information as required by the generally applicable destruction schedule once the litigation need to preserve the information has passed. Id. The government

---

<sup>22</sup> In brief, information that the FBI retains on an electronic and data storage system, but has not reviewed, generally must be destroyed after “██████████ from the expiration date of the certification authorizing the collection.” FBI Minimization Procedures at 20. Information retained on such systems that has been reviewed, “but not identified as information that reasonably appears to be foreign intelligence, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime” is generally subject to special access controls after ██████████ from such expiration date, and shall be destroyed after ██████████ from such date. Id. at 20-21. Information retained by the FBI in any other form “shall be destroyed in accordance with the Attorney General Guidelines and relevant National Archives and Records Administration procedures regarding the retention of information in FBI investigations,” except that “an original copy” that cannot be accessed through an electronic and data storage system may be retained indefinitely, subject to special access controls after five years. Id. at 21.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

undertakes to report to the FISC on an annual basis regarding implementation of this provision.

See July 28, 2014 Memorandum at 15.

[REDACTED]

[REDACTED]

[REDACTED] restrictions on access that the Government proposes, along with the reporting requirements that would be required, strike an appropriate balance between the competing concerns of not retaining data longer than necessary and having the Government comply with its litigation obligations. [REDACTED]

[REDACTED] The annual reporting requirement regarding Section 702 information is set out below at page 42.

4. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>23</sup> [REDACTED]

[REDACTED]

---

<sup>23</sup> For example, under other provisions of the NSA Minimization Procedures, the NSA may not retain telephony and certain forms of Internet communications for “longer than five years from the expiration date of the certification authorizing the collection” unless the NSA determines that specified retention criteria are met. NSA Minimization Procedures at 7. For “Internet transactions acquired through NSA’s upstream collection techniques,” that retention period is two years from such expiration date. *Id.*

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]

[REDACTED] the Court is satisfied that this approach -- [REDACTED] -- strikes a proper balance between the protection of United States person information, on the one hand, and [REDACTED]. Nonetheless, two points regarding these provisions merit further discussion.

First, the provisions do not permit [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

[REDACTED] In the interests of efficiency and consistency, the Court encourages the government to consider further revision of these procedures to address such situations with generally applicable rules, rather than on a piecemeal basis.

The second point concerns [REDACTED]

[REDACTED]

[REDACTED] That approach appears sensible: [REDACTED]

[REDACTED]

The July 28, 2014 Submission contains similar, but broader language:

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The FISC has a continuing role in determining and enforcing compliance with these procedures. See 50 U.S.C. § 1803(h); FISC Rule 13(b). Section 702 explicitly provides a mechanism for the AG and DNI to modify minimization procedures, subject to FISC approval, whenever circumstances warrant.<sup>24</sup> In view of these considerations, and because the government has provided no support for its suggestion that equivalent relief can or should be obtained [REDACTED]

[REDACTED] the Court expects the government to bring to the FISC issues arising [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Because

the point does not arise under the language of the [REDACTED]

[REDACTED], it does not preclude the Court from finding that those

minimization procedures are consistent with the definition at Section 1801(h).

---

<sup>24</sup> Section 702 permits the AG and the DNI to amend previously adopted minimization procedures "as necessary at any time," subject to FISC review. See § 1881a(i)(1)(C).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

## 5. Conclusion

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA, FBI, and CIA Minimization Procedures, as written, comport with the definition of minimization procedures at Section 1801(h).

### C. The Compliance and Implementation Issues Reported by the Government Do Not Preclude a Finding That the NSA and FBI Targeting Procedures and the NSA, FBI, and CIA Minimization Procedures Comply With Statutory Requirements.

As noted above at page 3, the FISC examines the government's implementation of, and compliance with, the targeting and minimization procedures as part of assessing whether those procedures comply with the applicable statutory (and Fourth Amendment) requirements.

In conducting this assessment, the Court is mindful that the controlling norms are ones of reasonableness, not perfection.<sup>25</sup> This distinction is particularly important in the context of a large and complex endeavor such as the government's implementation of Section 702. While in absolute terms, the scope of acquisitions under Section 702 is substantial, the acquisitions are not conducted in a bulk or indiscriminate manner. Rather, they are effected through [REDACTED] discrete targeting decisions for individual facilities.<sup>26</sup> Each targeting decision requires

---

<sup>25</sup> See Section 1881a(d)(1) (requiring targeting procedures that are "reasonably designed" to limit targeting to "persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition" of communications to which all parties are known to be in the United States); Section 1801(h)(1) (requiring minimization procedures that are "reasonably designed" to minimize acquisition and retention, and to prohibit dissemination, of information concerning United States persons, consistent with foreign intelligence needs); United States v. Knights, 534 U.S. 112, 118 (2001) ("The touchstone of the Fourth Amendment is reasonableness . . .").

<sup>26</sup> For example, the NSA reports that, "on average, approximately [REDACTED] individual (continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

application of the pre-tasking provisions of the applicable targeting procedures. See NSA Targeting Procedures at 1-6; FBI Targeting Procedures at 1-3. For each facility while it is subject to tasking, there are post-tasking requirements designed to ascertain, for example, whether the targeted user of the facility has entered the United States. See NSA Targeting Procedures at 6-7. And pursuant to the minimization procedures, there are detailed rules concerning the retention, use, and dissemination of information obtained pursuant to Section 702. See NSA Minimization Procedures at 3-15; FBI Minimization Procedures at 5-33; CIA Minimization Procedures at 1-9.

Given the number of decisions and volume of information involved, it should not be surprising that occasionally errors are made. Moreover, the government unavoidably relies on [REDACTED], see, e.g., July 28, 2014 Memorandum at 18-20; August 30, 2013 Opinion at 7-9, [REDACTED] see, e.g., April 7, 2009 Opinion at 17-22. Because of factors such as changes in communications technology or inadvertent error, these processes do not always function as intended.

---

<sup>26</sup>(...continued)

[REDACTED] were tasked for acquisition “at any given time between March 1 and May 31, 2014.” Quarterly Report to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on June 20, 2014, at 1 (footnote omitted) (“June 20, 2014 Compliance Report”). Facilities tasked for acquisition include “telephone numbers, e-mail accounts [REDACTED] [REDACTED] Additionally, between March 1 and May 31, 2014, the [FBI] reports that it received and processed approximately [REDACTED] requests.” Id. at 1.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

It is apparent to the Court that the implementing agencies, as well as the Office of the Director of National Intelligence (ODNI) and NSD, devote substantial resources to their compliance and oversight responsibilities under Section 702. As a general rule, instances of non-compliance are identified promptly and appropriate remedial actions are taken, to include purging information that was improperly obtained or otherwise subject to destruction requirements under applicable procedures.<sup>27</sup> Accordingly, the Court's overall assessment of the implementation of, and compliance with, the targeting and minimization procedures permits a finding that these procedures, as implemented, satisfy the applicable statutory requirements. Nonetheless, the Court believes it is useful to discuss the following aspects of implementation and, in some respects, to direct the government to provide additional information.

1. Timely Resolution of [REDACTED] by the NSA

The NSA is required to discontinue acquisition for a facility if it determines that the user of the facility is in the United States. NSA Minimization Procedures at 7, 9; see also 50 U.S.C. § 1881a(b)(1) (the government "may not intentionally target any person known at the time of acquisition to be located in the United States"). The NSA routinely checks each electronic communications facility that is subject to tasking for acquisition [REDACTED] [REDACTED] for indications that a tasked facility may have been accessed from inside the United States. NSA Targeting Procedures at 6-7; July 28, 2014 Memorandum at 18.

---

<sup>27</sup> A notable exception involved protracted delays in detasking facilities used by [REDACTED] [REDACTED] there was reason to believe was a United States person. See June 20, 2014 Compliance Report at 14-15. The FISC probed the reasons for such delay at a hearing on June 26, 2014, [REDACTED] [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

The Court, through its staff, inquired why, in some cases, it may take [REDACTED] from the receipt of such an indication – [REDACTED] – for the NSA to determine that the user of the tasked facility is in the United States and discontinue collection. See, e.g., June 20, 2014 Compliance Report at 31.

In response, the government has advised that the NSA employs [REDACTED] to conduct these checks and to prioritize the results for research by NSA analysts. July 28, 2014 Memorandum at 18-19. These [REDACTED] a large percentage of false positives: “Although the number fluctuates, NSA reports that for 2014 more than 90% of the [REDACTED] generated were false positives, i.e., not indicative of access of the facility by a user inside the United States.” Id. at 19 n.6.

The NSA further prioritizes within the subset of [REDACTED] that are deemed to indicate potential access from within the United States. [REDACTED] that are assessed to be [REDACTED] of a user inside the United States” result in immediate detasking. Id. at 20. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

Diligent and prompt response to credible indications that a tasked facility has been accessed from the United States goes to the heart of the requirement of 50 U.S.C. § 1881a(d)(1)(A) that targeting procedures be reasonably designed to ensure that acquisitions target persons reasonably believed to be outside the United States. Nonetheless, given the high rate of false positives associated with these [REDACTED] and the potentially complex nature of the analysis required to resolve them, the Court believes that the NSA's current practices in responding to [REDACTED] are consistent with a finding that the NSA Targeting Procedures comply with that statutory requirement.

2. [REDACTED] Under the FBI Targeting Procedures

The FBI Targeting Procedures state:

[REDACTED]

28

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

a.

[Redacted]

29

29

[Redacted]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]

b.

[REDACTED]

c.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The Court has questions about whether [REDACTED] comply with this requirement in every context. The Court assesses, however, that these outstanding questions about compliance with the FBI Targeting Procedures do not preclude a finding that the government's targeting procedures satisfy the requirements of Section 1881a(d)(1). Recently reported instances of non-compliance with the FBI Targeting Procedures do not appear to have resulted in the acquisition of [REDACTED] from an account used by a United States

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

person or someone located in the United States. See, e.g., June 20, 2014 Compliance Report at 54, 56-57; Quarterly Report to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on March 22, 2014, at 67-69. Moreover, as noted above, see page 8, the FBI Targeting Procedures apply in addition to the NSA Targeting Procedures for accounts from which [REDACTED] are sought, so that every account subject to the FBI Targeting Procedures will already have been approved pursuant to the NSA Targeting Procedures. The Court is, however, directing the government to report further on the questions raised by the August 6, 2014 Letter. See page 42 below.

### 3. Purge Issues

Various types of data are generally required to be purged: for example, information obtained from a tasked facility during a time when it is later assessed that a user of that facility was in the United States or a United States person.<sup>30</sup> Purge processes for the CIA, NSA, and FBI all permit data otherwise subject to purge requirements to be retained on backup systems, with access limited to technical personnel. June 20, 2014 Compliance Report at 3-5. NSA's purge processes also do not reach [REDACTED] (as distinct from the repositories of information used for intelligence analysis), certain systems that [REDACTED] [REDACTED] Id. at 3 n.6.

Implementation of these purge requirements relies substantially on [REDACTED] processes, as well as [REDACTED]. Experience has shown that purge processes are not always perfectly

---

<sup>30</sup> See, e.g., NSA Minimization Procedures at 8-10; FBI Minimization Procedures at 6; CIA Minimization Procedures at 8.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

effective in identifying and destroying data in all repositories subject to those processes. The NSA reports substantial improvement in the efficacy of its purges,<sup>31</sup> but difficulties on certain systems or for certain types of data are still encountered.<sup>32</sup> Given the volume of information acquired under Section 702 and the complexities of routing, processing, storing, and analyzing that information, the Court finds that the reported limitations on purge processes, and the government's efforts to overcome these limitations, are consistent with finding that the targeting and minimization procedures presented in the July 28, 2014 Submission comply with the applicable statutory requirements. The Court encourages and expects the government to continue to work toward improving the efficacy of its purge processes, both as applied to systems or records currently within their compass and as potentially extended to other systems or records

[REDACTED]

---

<sup>31</sup> The NSA has performed annual studies that examined samples of [REDACTED] to see if they had actually been removed from systems subject to its purge processes. The 2011 study found [REDACTED] objects that had not been purged; the 2012 study found [REDACTED] objects that had not been purged; the 2013 study found [REDACTED] objects that had not been purged; and the 2014 study found [REDACTED] objects that had not been purged. June 20, 2014 Compliance Report at 50-51.

<sup>32</sup> See Letter from Kevin J. O'Connor, Chief, Oversight Section, Office of Intelligence, NSD, DOJ, filed on July 25, 2014, at 2-5 ("July 25, 2014 Letter") (describing [REDACTED] [REDACTED] July 30, 2014 Letter at 7-8 (describing incomplete NSA purges of metadata for [REDACTED]).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

4. The FBI's Non-compliance With Attorney-Client Minimization Procedures

FISA's definition of minimization procedures at Section 1801(h) does not, by its terms, afford any special protection to communications subject to the attorney-client privilege.<sup>33</sup>

Nevertheless, the minimization procedures under review have specific rules for handling attorney-client communications. See NSA Minimization Procedures at 9; FBI Minimization Procedures at 12-16, 25-27; CIA Minimization Procedures at 5. Because the FBI has law enforcement responsibilities and often works closely with prosecutors in criminal cases, its procedures have detailed requirements for cases in which a target is known to be charged with a federal crime. Unless otherwise authorized by the NSD, the FBI must establish a separate review team whose members "have no role in the prosecution of the charged criminal matter" to conduct the initial review of such a target's communications. FBI Minimization Procedures at 12

[REDACTED]

Since February 2014, the FISC has received written notice of [REDACTED] separate instances in which the responsible FBI case agent knew that a person targeted under Section 702 faced federal criminal charges, but did not establish the required review team. See July 30, 2014 Letter at 5-6. Although the government attributes those lapses to "individual failures or confusion and not a

---

<sup>33</sup> FISA does provide that "[n]o otherwise privileged communication obtained in accordance with, or in violation of, the provisions of [FISA] shall lose its privileged character." 50 U.S.C. § 1806(a).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

systematic issue,” *id.* at 7, the government at the August 4, 2014 hearing provided partial information about [REDACTED] more recent cases where the FBI failed to establish the required review team.

The record does not indicate what percentage of Section 702 targets have been charged with federal crimes; however, given that these targets are reasonably believed to be non-United States persons located outside the United States, one would expect the percentage to be fairly small. For that reason, the Court regards [REDACTED] recent cases as a potentially significant rate of non-compliance. Nonetheless, because circumstances triggering the obligation to establish a review team presumably arise infrequently in the context of Section 702 acquisitions, the Court does not believe that these instances of non-compliance prevent a finding that the minimization procedures under review comply with the requirements of Section 1801(h). The Court intends to monitor compliance with this provision of the FBI Minimization Procedures closely, and to that end is directing that the government fully report on the [REDACTED] additional instances of non-compliance noted above. *See* pages 42-43 below.

##### 5. Anticipated Delay in the CIA’s Implementation of Destruction Requirements

As a general rule under the CIA Minimization Procedures, “[un]minimized communications that may contain United States person information that does not otherwise qualify for retention . . . may be retained . . . for no longer than five years from the expiration date of the certification authorizing the collection . . .” CIA Minimization Procedures at 2. On August 18, 2014, the government orally advised the Court, through its staff, that the first two sets of communications subject to this provision are due to be destroyed on September 4 and

~~TOP SECRET//SI//ORCON/NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

September 18, 2014, respectively, and that the CIA did not expect to have completed their destruction by those dates. The government principally attributes this delay to the amount of time it took to finalize guidance from the DOJ to the CIA regarding [REDACTED]. It is expected that the destruction of these communications will have been completed within thirty days after the applicable due date.

The Court does not see a basis for finding that retention for an additional month would render these minimization procedures non-compliant with the requirements of Section 1801(h). The government is being directed, however, to report to the Court on the CIA's implementation of this destruction requirement.

D. The NCTC Minimization Procedures Comply With Statutory Requirements.

The NCTC does not have access to raw Section 702 information, but it does have access to minimized Section 702 information on certain FBI data systems. See June 20, 2014 Compliance Report at 1-2 n.4. The NCTC Minimization Procedures now before the Court are identical to those approved in the August 30, 2013 Opinion, see July 28, 2014 Memorandum at 2 n.1, as well as those approved in the September 20, 2012 Opinion. See August 30, 2013 Opinion at 23. For the same reasons that these procedures were approved in 2012, see September 20, 2012 Memorandum Opinion at 22-25, and because no significant compliance issues have arisen under these procedures, the Court again finds that the procedures satisfy the requirements of Section 1801(h).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

E. The Targeting and Minimization Procedures Are Consistent with the Fourth Amendment.

Finally, the Court must determine whether the targeting and minimization procedures included in the July 28, 2014 Submission are consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A). The Fourth Amendment does not require the government to obtain a warrant to conduct surveillance “to obtain foreign intelligence for national security purposes . . . [that] is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.” In re Directives Pursuant to Section 105B of FISA, Docket No. 08-01, Opinion at 18-19 (FISA Ct. Rev. Aug. 22, 2008) (“In re Directives”).<sup>34</sup> This exception to the Fourth Amendment’s warrant requirement applies even when a United States person is the target of such a surveillance. See id. at 25-26 (discussing internal Executive Branch criteria for targeting United States persons). The FISC has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within this “foreign intelligence exception” to the warrant requirement of the Fourth Amendment. See September 4, 2008 Opinion at 34-36; accord United States v. Mohamud, 2014 WL 2866749 at \*15-18 (D. Or. June 24, 2014).

It follows that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment if those procedures, as implemented, are reasonable. In assessing the reasonableness of a governmental action under the Fourth Amendment, a court

---

<sup>34</sup> A declassified version of the opinion in In re Directives is available at 551 F.3d 1004 (FISA Ct. Rev. 2008).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

must “balance the interests at stake” under the totality of the circumstances presented. In re Directives at 19-20.

If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government’s actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20.

The government’s national security interest in conducting acquisitions pursuant to Section 702 “is of the highest order of magnitude.” September 4, 2008 Opinion at 37 (quoting In re Directives at 20). With regard to the individual privacy interests involved, the Court has concluded, as discussed above, that the targeting procedures now before it are reasonably designed to target non-United States persons who are located outside the United States. Such persons fall outside the ambit of Fourth Amendment protection. See September 4, 2008 Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)).

That is not the end of the matter, however, because the government acquires under Section 702 communications to which United States persons and persons within the United States are parties. Such acquisitions can occur when those non-targeted persons are parties to a communication that is to or from, or that contains a reference to, a tasked selector. See September 4, 2008 Opinion at 15-20. Such communications may also be acquired when they constitute part of a larger “Internet transaction” (e.g., [REDACTED] [REDACTED] that also contains one or more communications that are to or from, or that contain a reference to, a tasked selector. In the latter case, the entire

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

transaction may be unavoidably acquired by the NSA's "upstream" collection. See [REDACTED]  
[REDACTED] Memorandum Opinion entered on Oct. 3, 2011, at  
5, 30-31 ("October 3, 2011 Opinion").<sup>35</sup>

In the Prior 702 Dockets, the FISC has found that earlier versions of the various agencies' targeting and minimization procedures adequately protected the substantial Fourth Amendment interests that are implicated by the acquisition of communications of such United States persons. See, e.g., August 30, 2013 Opinion at 24-25; September 20, 2012 Opinion at 43-44. In the FISC's assessment, the combined effect of these procedures has been "to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated" and to ensure that "non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary." See August 30, 2013 Opinion at 24-25 (internal quotations omitted). Neither the amendments before the Court nor the compliance concerns discussed above undermine that conclusion. The Court has balanced the competing interests at stake and found that the targeting and minimization procedures put forward in the July 28, 2014 Submission are consistent with the requirements of the Fourth Amendment.

---

<sup>35</sup> FISA minimization protects the privacy interests of United States persons in communications in which they are discussed, regardless of whether they were parties to such communications. See Section 1801(h)(1) (protecting "nonpublicly available information concerning unconsenting United States persons") (emphasis added). In contrast, non-targets generally do not have a Fourth Amendment-protected interest in communications in which they are discussed, unless they are also parties to the communication. See Alderman v. United States, 394 U.S. 165, 174-76 (1969).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

#### IV. CONCLUSION

For the foregoing reasons, the Court finds that: (1) the 2014 Certifications, as well as the certifications in the Prior 702 Dockets as amended by the 2014 Certifications, contain all the required statutory elements; (2) the targeting and minimization procedures to be implemented regarding acquisitions conducted pursuant to the 2014 Certifications comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment; and (3) the minimization procedures to be implemented regarding information acquired under prior Section 702 certifications comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment. Orders approving the certifications, amended certifications, and use of the accompanying procedures are being entered contemporaneously herewith.

For the reasons discussed above, it is HEREBY ORDERED as follows:

1. On or before December 31 of each calendar year, the government shall submit in writing a report to the Court containing the following information: (a) the number of Section 702-acquired products disseminated or disclosed to the NCMEC; and (b) the number of disseminations or disclosures by the NCMEC to other law enforcement entities of Section 702-acquired information. Additionally, prior to implementing changes to policies or practices concerning: (c) the release of Section 702-acquired information from the NCMEC to Interpol's International Child Sexual Exploitation database; or (d) approval to use Section 702-acquired information disseminated to the NCMEC in any proceeding, the government shall make a written submission to the Court describing such changes and explaining why implementing them would be consistent with applicable minimization procedures and statutory minimization requirements.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

[REDACTED]

2. On or before December 31 of each calendar year, the government shall submit in writing a report to the Court containing the following information [REDACTED] (a) all administrative, civil, or criminal litigation matters necessitating preservation of Section 702 information that would otherwise be subject to destruction requirements under applicable minimization procedures; (b) the docket numbers and court information for those administrative, civil, or criminal litigation matters; (c) a description of the Section 702-acquired information preserved for each such litigation matter; and (d) a description of the status of each such litigation matter. [REDACTED]

[REDACTED]

3. On or before September 30, 2014, the government shall submit in writing a report describing in detail the [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4. On or before September 30, 2014, the government shall submit in writing a report describing in detail the [REDACTED] recent instances of non-compliance with the attorney-client minimization requirements of the FBI Minimization Procedures that have not been reported in writing to the FISC, as referenced on pages 35-36 above. This report shall also provide an assessment of the adequacy of the government's training, guidance, and oversight efforts with

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

regard to those requirements, to include a statement of any planned modifications or enhancements.

5. On or before October 24, 2014, the government shall submit in writing a report about the status of the CIA's efforts to comply with the destruction deadlines of September 4 and September 18, 2014, as discussed on pages 36-37. The government shall submit subsequent reports on that subject at monthly intervals thereafter, until it is reported that the destruction of information subject to such requirements has been completed.

ENTERED this 26<sup>th</sup> day of August 2014, in [REDACTED]

[REDACTED]

*Thomas F. Hogan*  
THOMAS F. HOGAN  
Judge, United States Foreign  
Intelligence Surveillance Court

(b)(6) I, [REDACTED] Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

[REDACTED]

(b)(6)

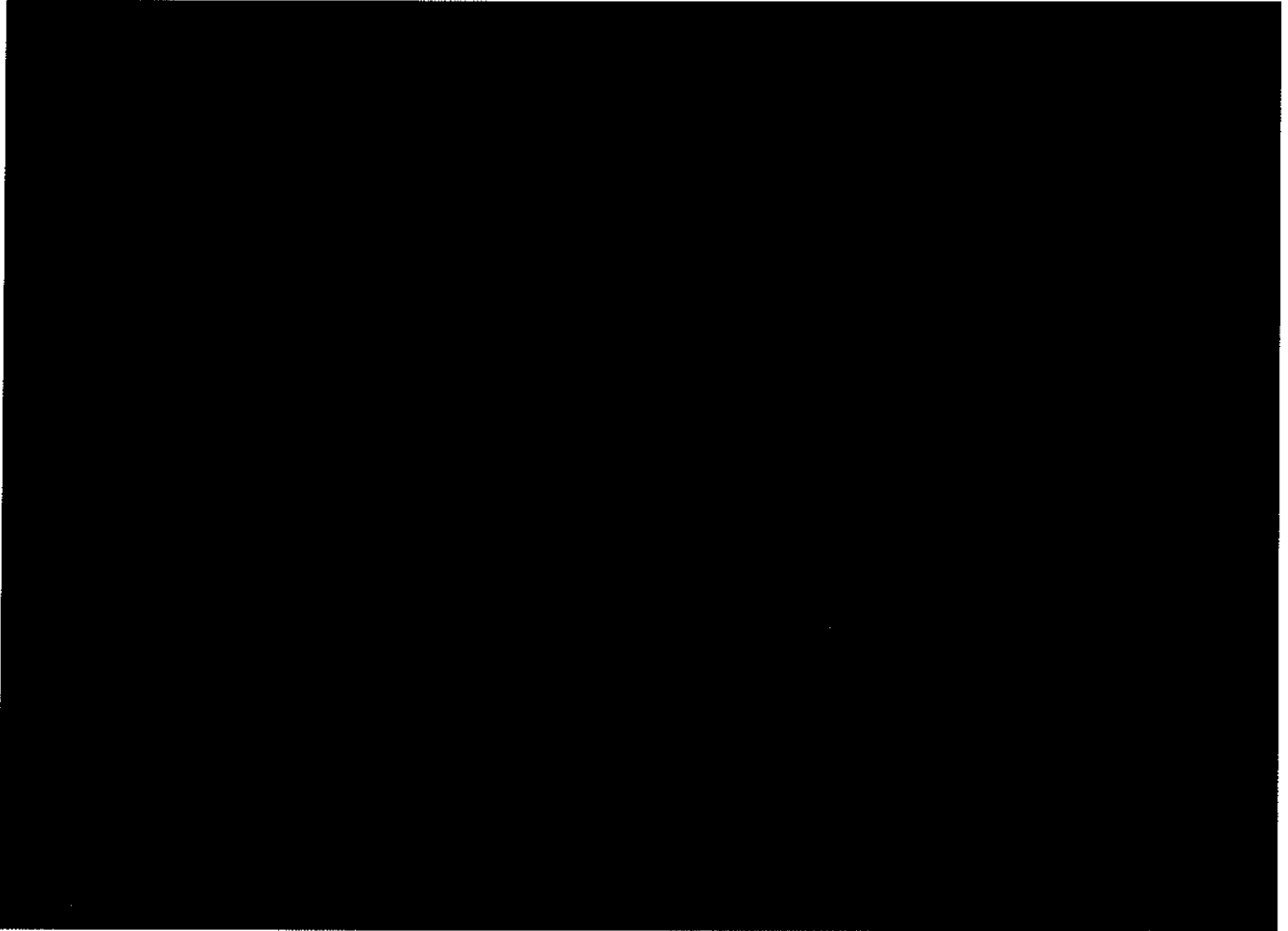
~~TOP SECRET//SI//ORCON//NOFORN~~

~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



**ORDER**

For the reasons stated in the Memorandum Opinion and Order issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds pursuant to 50 U.S.C. § 1881a(i)(3)(A) that the certifications referenced above, as amended in the above-captioned docket numbers, contain all the required statutory elements and that the revised

~~SECRET~~



~~SECRET~~

minimization procedures adopted for use in connection with those amended certifications are consistent with the requirements of Section 1881a(e) and with the Fourth Amendment.

Accordingly, it is hereby ORDERED pursuant to Section 1881a(i)(3)(A) that the amended certifications and the use of such procedures are approved.

ENTERED this 26<sup>th</sup> day of August 2014, in [REDACTED]

[REDACTED]



**THOMAS F. HOGAN**  
Judge, United States Foreign  
Intelligence Surveillance Court

(b)(6) I, [REDACTED] Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

[REDACTED]

(b)(6)

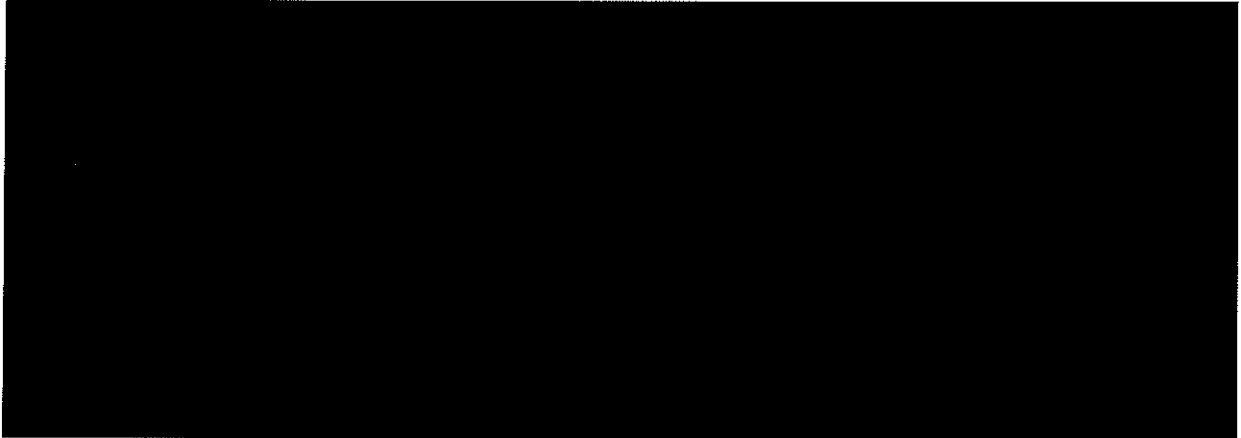
~~SECRET~~

~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



**ORDER**

For the reasons stated in the Memorandum Opinion and Order issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications referenced above contain all the required statutory elements and that the targeting procedures and minimization procedures approved for use in connection with those certifications are consistent with the requirements of 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

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

ENTERED this 26<sup>th</sup> day of August 2014, in [REDACTED]



THOMAS F. HOGAN  
Judge, United States Foreign  
Intelligence Surveillance Court

(b)(6)

[REDACTED] Deputy  
Clerk, FISC, certify that this  
document is a true and  
correct copy of the original.



(b)(6)

~~SECRET~~