

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

Approved for Public Release

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

UNITED STATES

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

FOREIGN INTELLIGENCE SURVEILLANCE COURT ~~ZEN~~ JUL 28 PM 3:56

WASHINGTON, D.C.

LEEFANN 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(e)
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.¹

{S//OC/NF} In addition, [REDACTED]

[REDACTED] also include amendments to the certifications being reauthorized, [REDACTED]

[REDACTED] and their predecessors.² 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]

¹ {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.

[REDACTED]

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

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

[REDACTED]

(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.

³ (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] 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~~



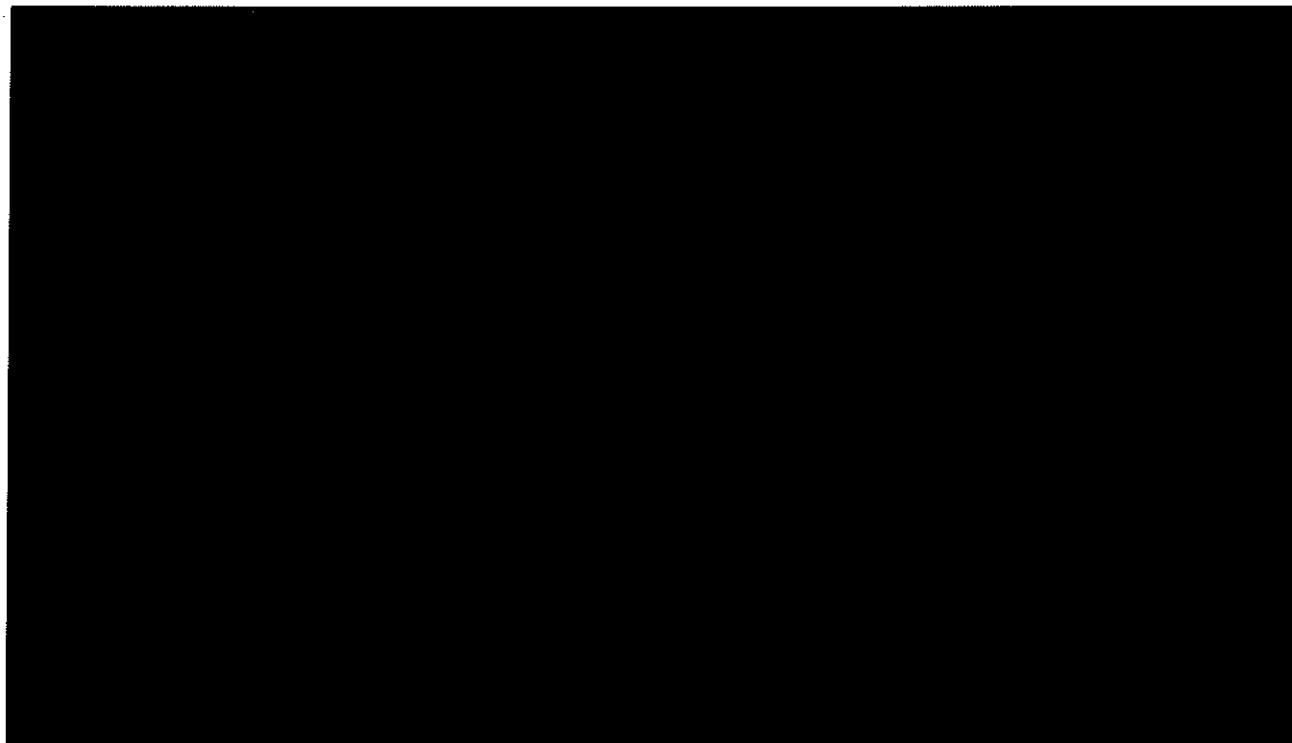
(S//OC/NF) Section 702 permits the Director of National Intelligence (DNI) and the Attorney General (AG) to authorize the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information," 50 U.S.C. § 1881a(a). As previously explained by the 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]

[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.

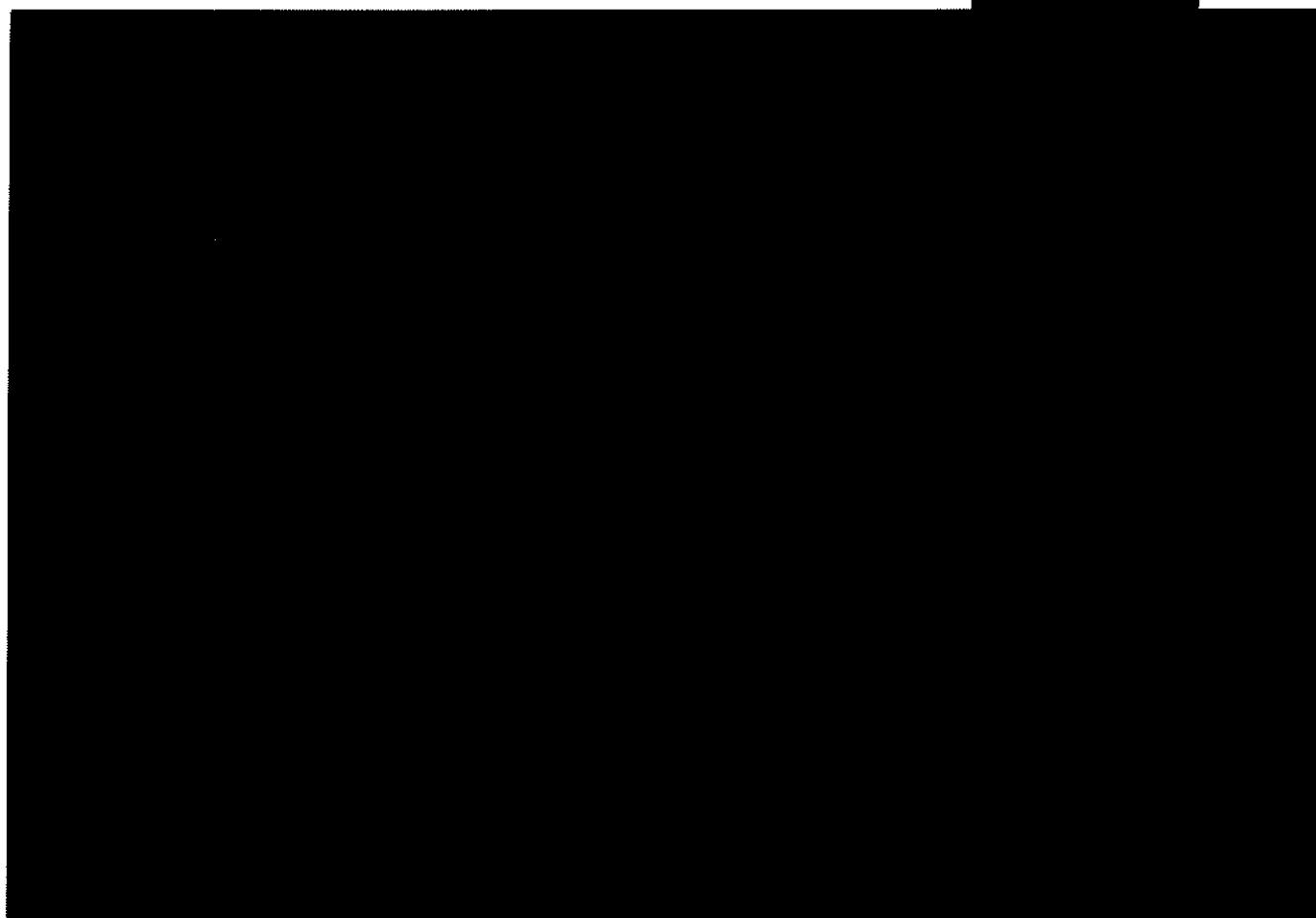
(S) The Government does not believe that this change to NSA's targeting procedures will affect the amount of time NSA takes to resolve [REDACTED] concerning section 702-tasked electronic communications [REDACTED] that may have been accessed from inside the United States. [REDACTED]
[REDACTED]
[REDACTED]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

[REDACTED]

(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 [REDACTED]

[REDACTED] These proposed [REDACTED] 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 [REDACTED]

[REDACTED] contain substantially similar provisions, described in more [REDACTED]

[REDACTED]

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

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

detail below.⁵

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

[REDACTED]

~~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 (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]

(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] 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] [REDACTED] allow for the retention of section 702-acquired information associated with FBI [REDACTED] 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~~

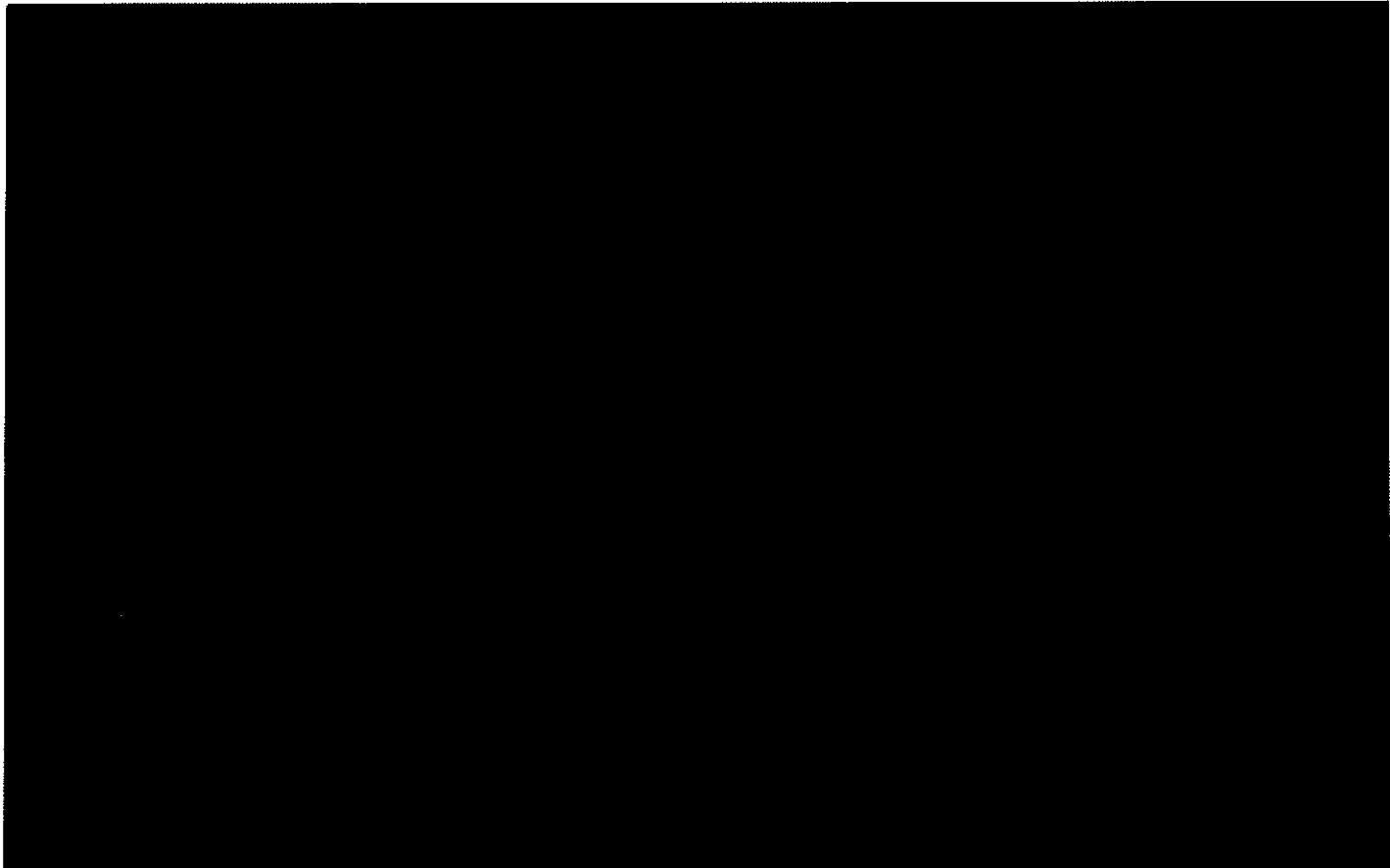
~~TOP SECRET//SI//ORCON/NOFORN~~

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

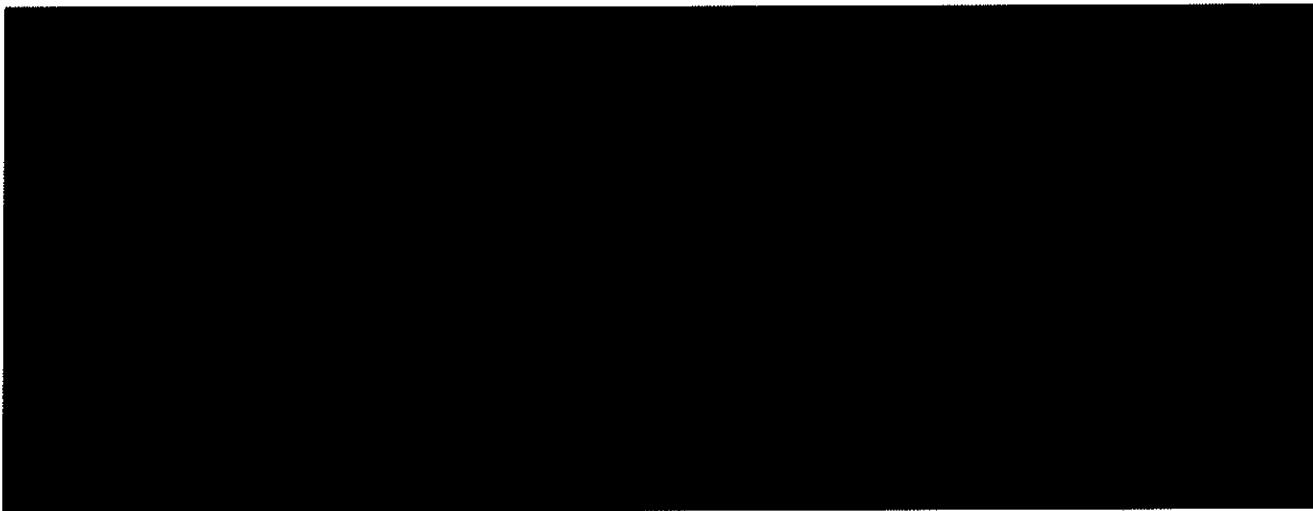
~~(S//NF)~~ As with the minimization procedures used by the FBI and discussed in further detail above, the Government has added language to the minimization procedures used by the NSA and CIA and submitted as Exhibits B and E, respectively,

to [REDACTED]



~~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]

[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.⁶ It is important to note that a single facility may generate [REDACTED]
[REDACTED] and not all [REDACTED] are indicative of compliance incidents.⁷

(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]

⁶ (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.

⁷ (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]
Third,

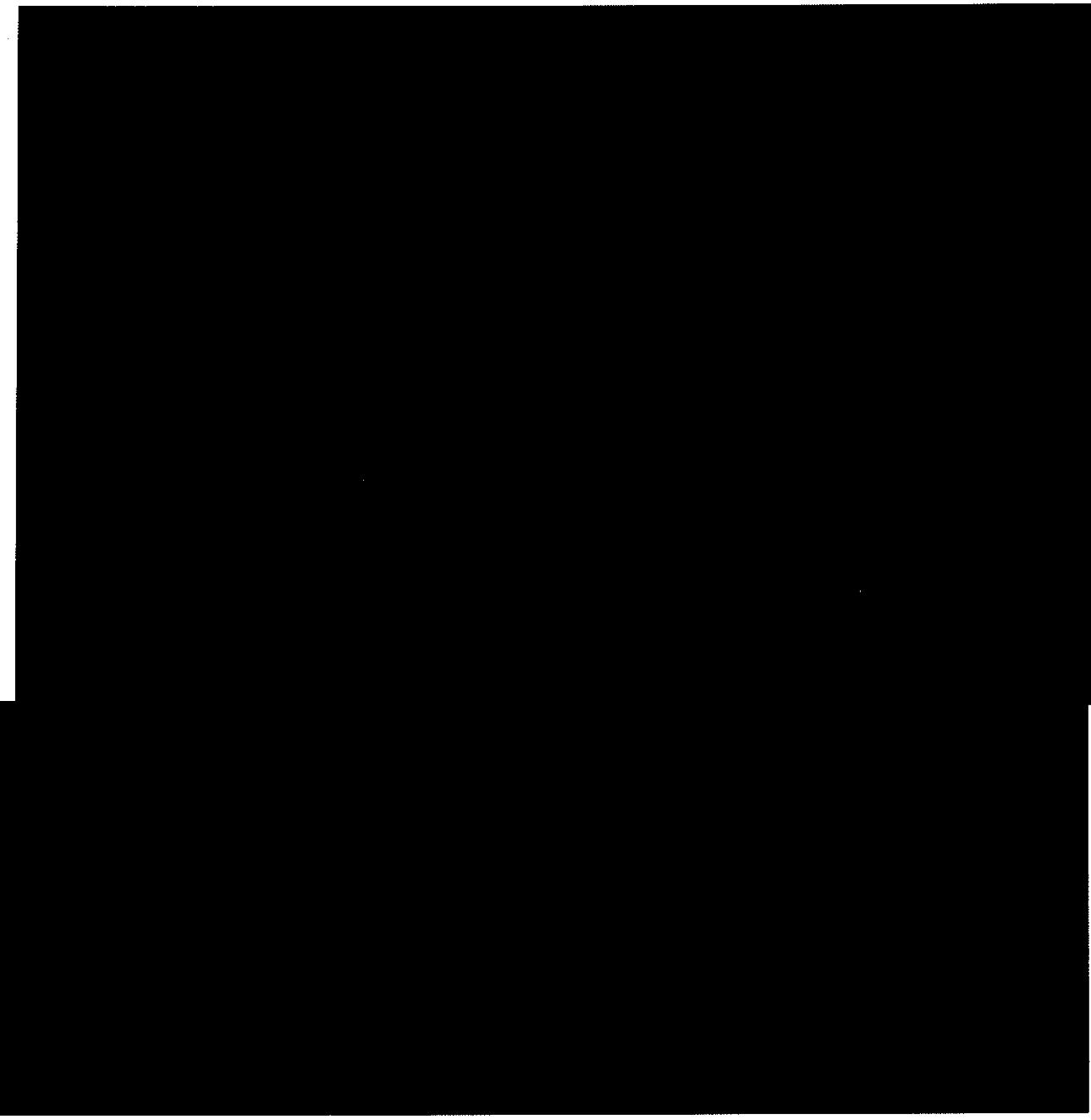
[REDACTED]

[REDACTED]

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

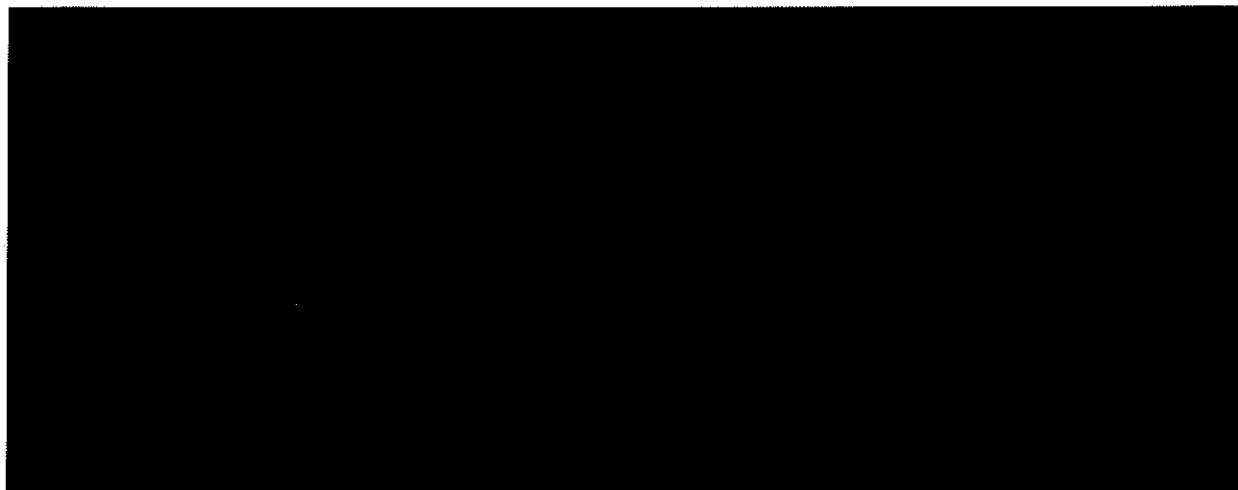
~~TOP SECRET//SI//ORCON/NOFORN~~

(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

(b)(6)

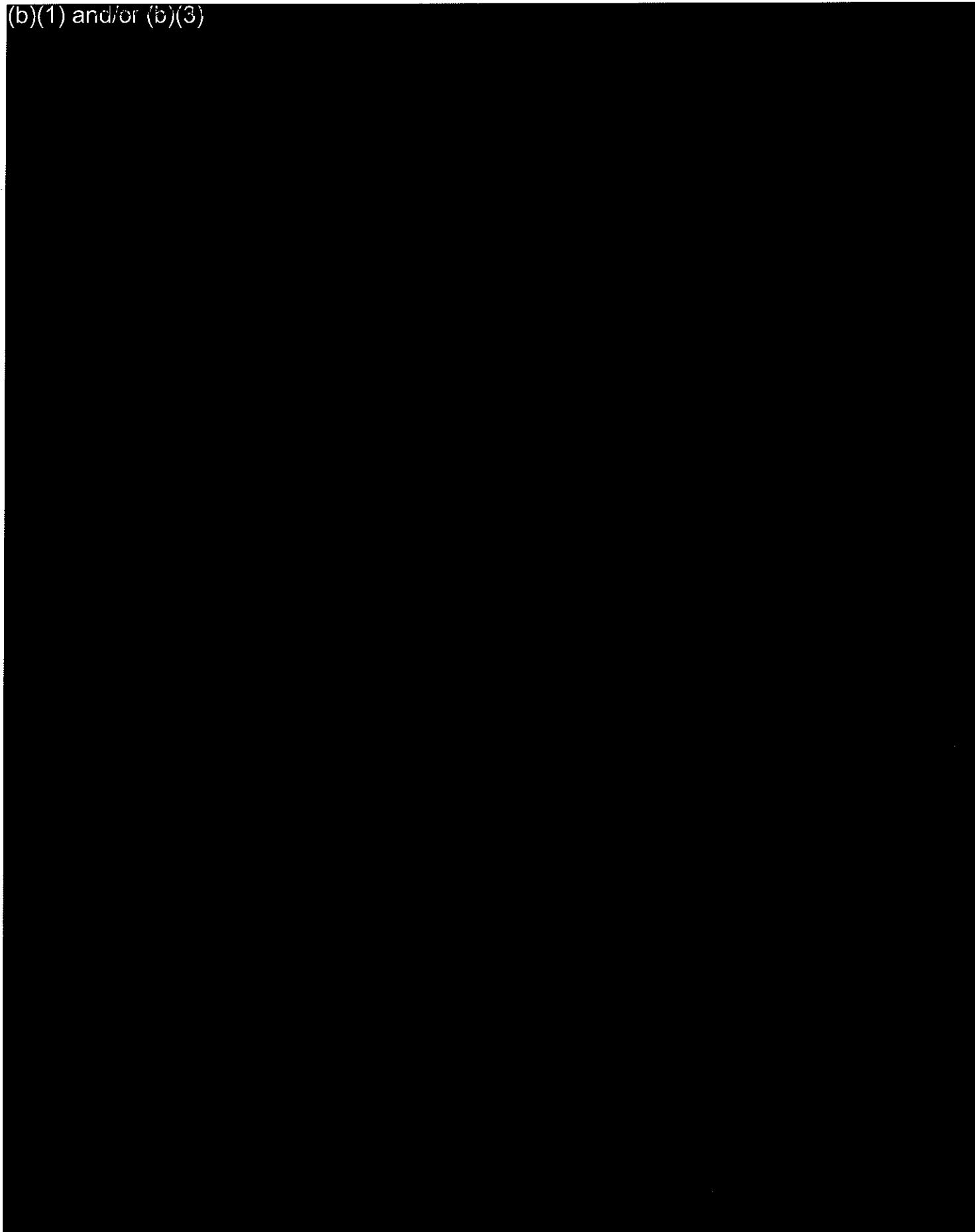
By:

(b)(6)

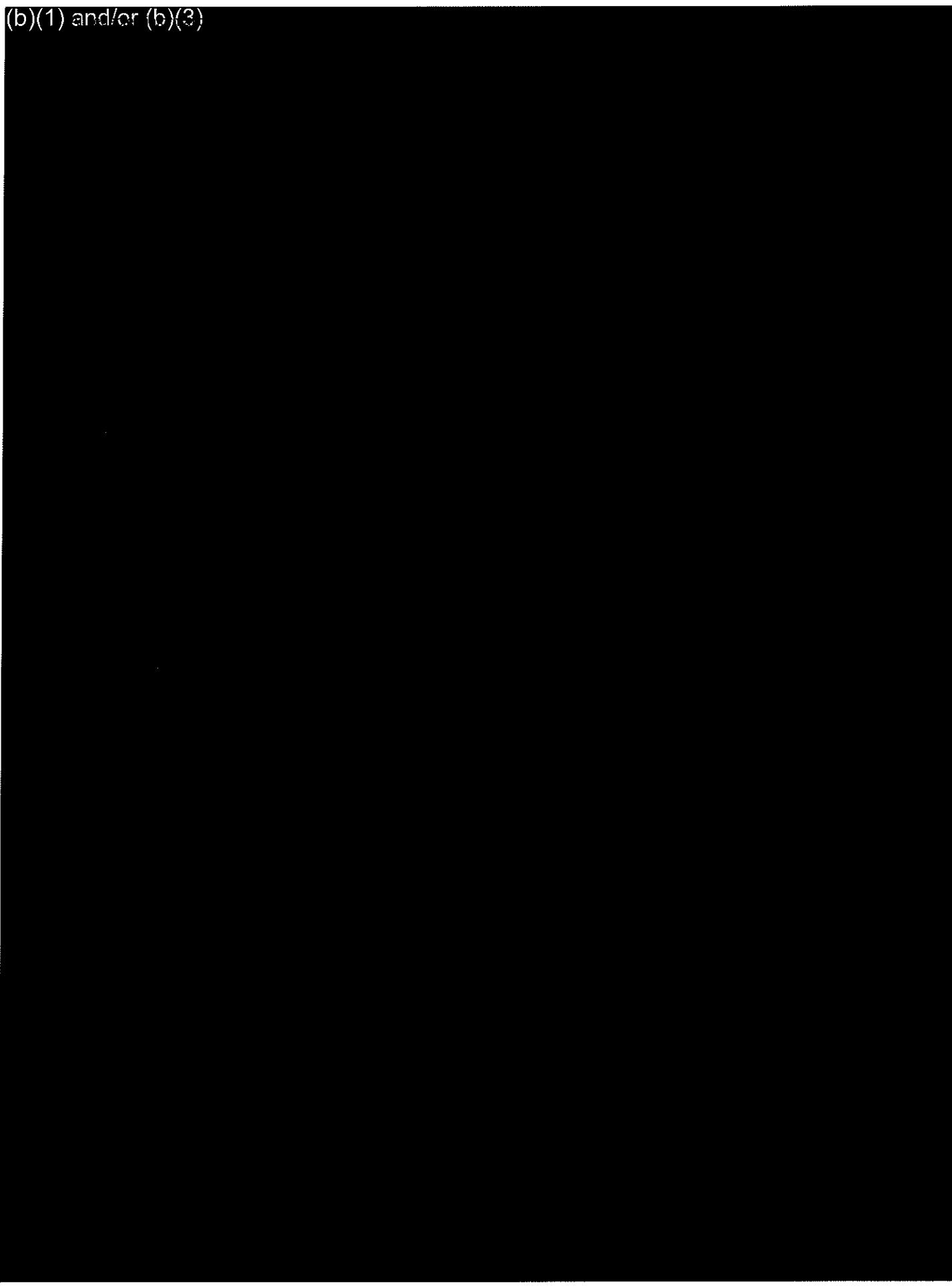
Office of Intelligence
National Security Division
U.S. Department of Justice

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

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



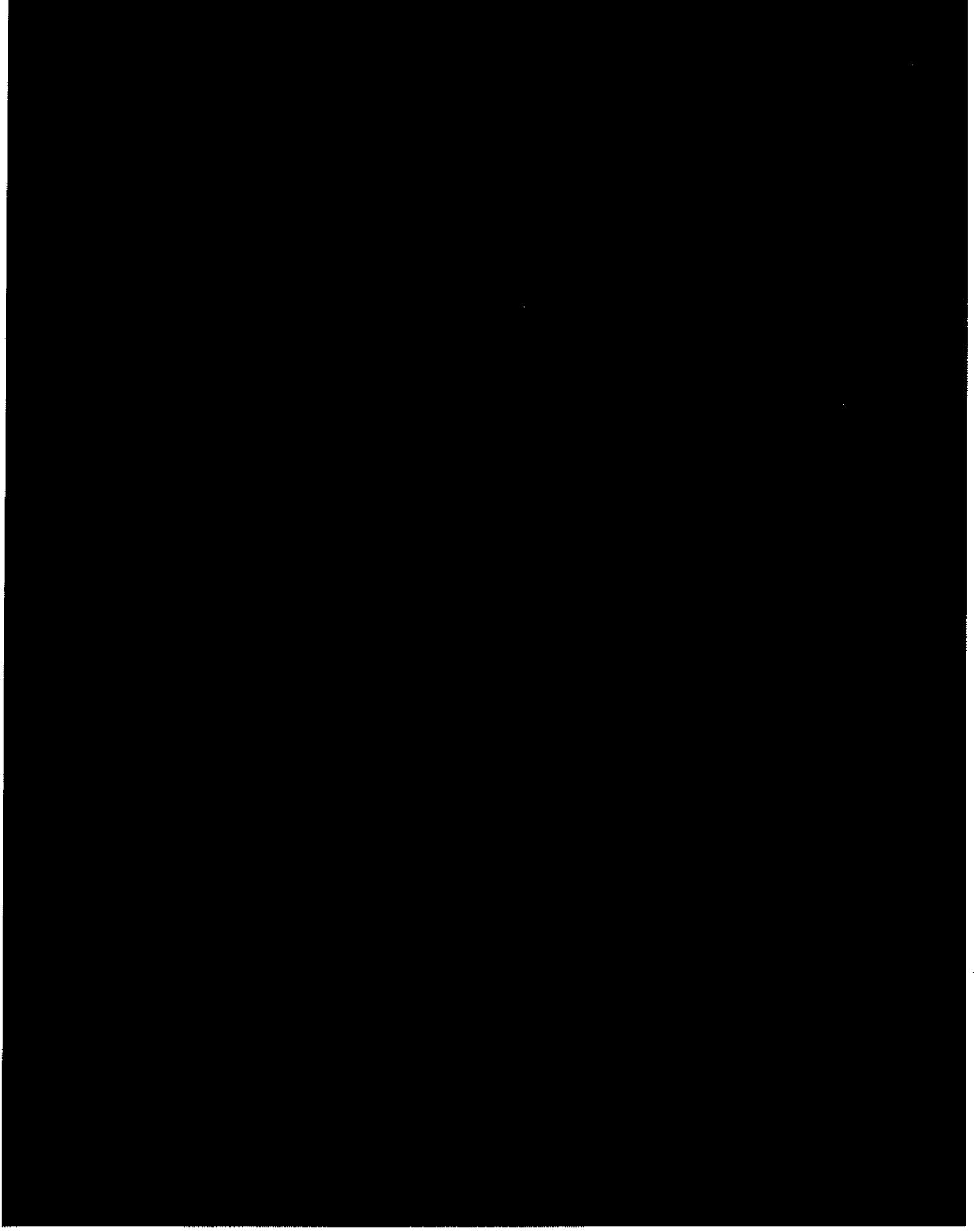
(b)(1) and/or (b)(3)



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

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

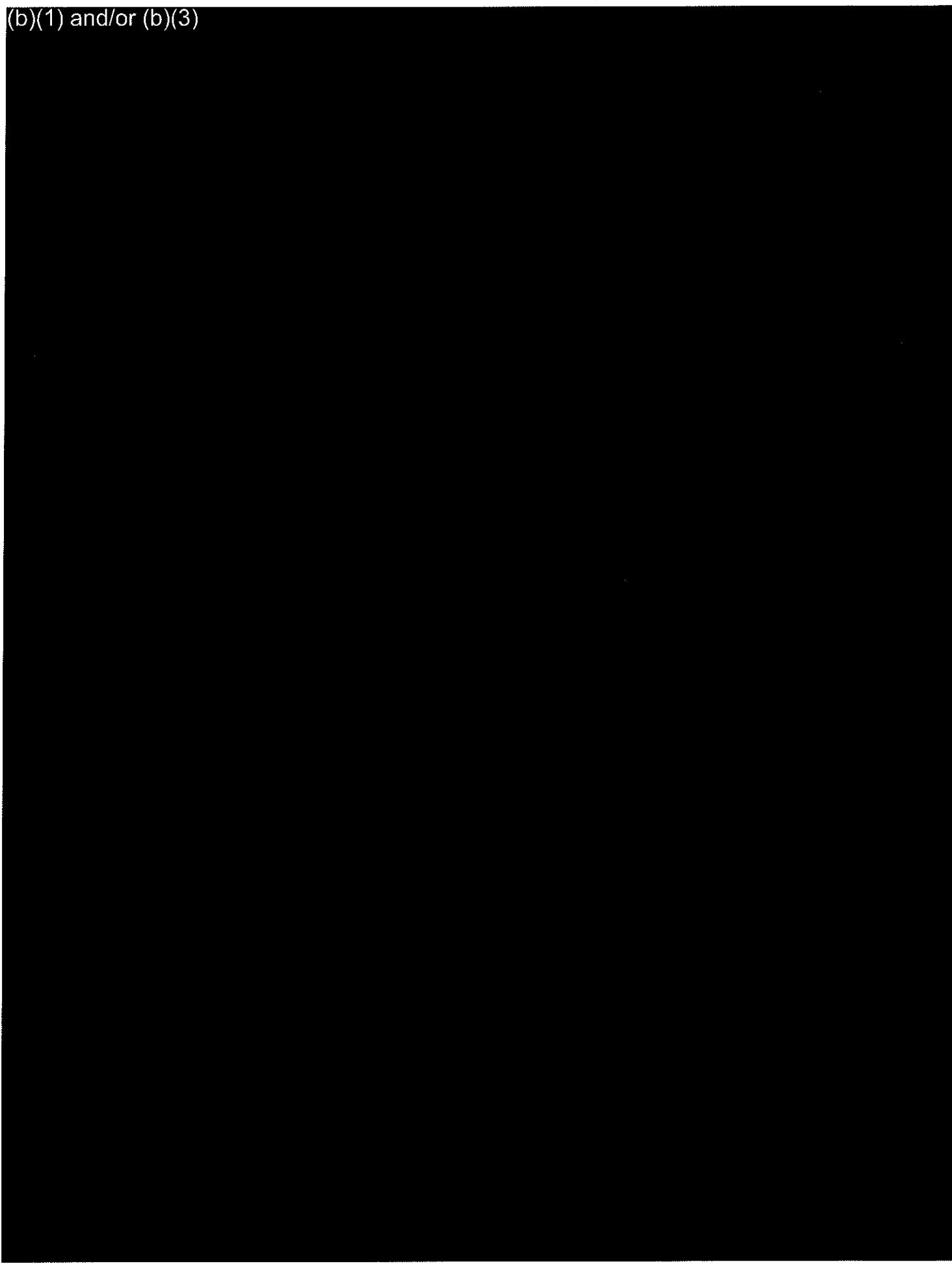
(b)(1) and/or (b)(3)



(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

LEE ANN 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]

[REDACTED] As detailed in the July 29 letter,

[REDACTED] On July 6, 2011, NSA further reported that [REDACTED] 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 [REDACTED] 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 [REDACTED] additional facilities did not involve compliance

¹ NSA tasked this account pursuant to [REDACTED] on [REDACTED] and collection continued pursuant to [REDACTED] (S)

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

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

Reason: 1.4(e)

Declassify on: 11 January 2037

~~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]

[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]

[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) [REDACTED]

/ 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(e)

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]

[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]

[REDACTED]

(TS//SI//NF) In [REDACTED] NSA identified training issues related to such [REDACTED] Section 702-tasked 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]

[REDACTED]

[REDACTED]

[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,

A handwritten signature in black ink, appearing to read "KJOC".

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]

[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]

[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]

[REDACTED] For example, during [REDACTED]

[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,

[REDACTED] (b)(6)

Office of Intelligence

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