

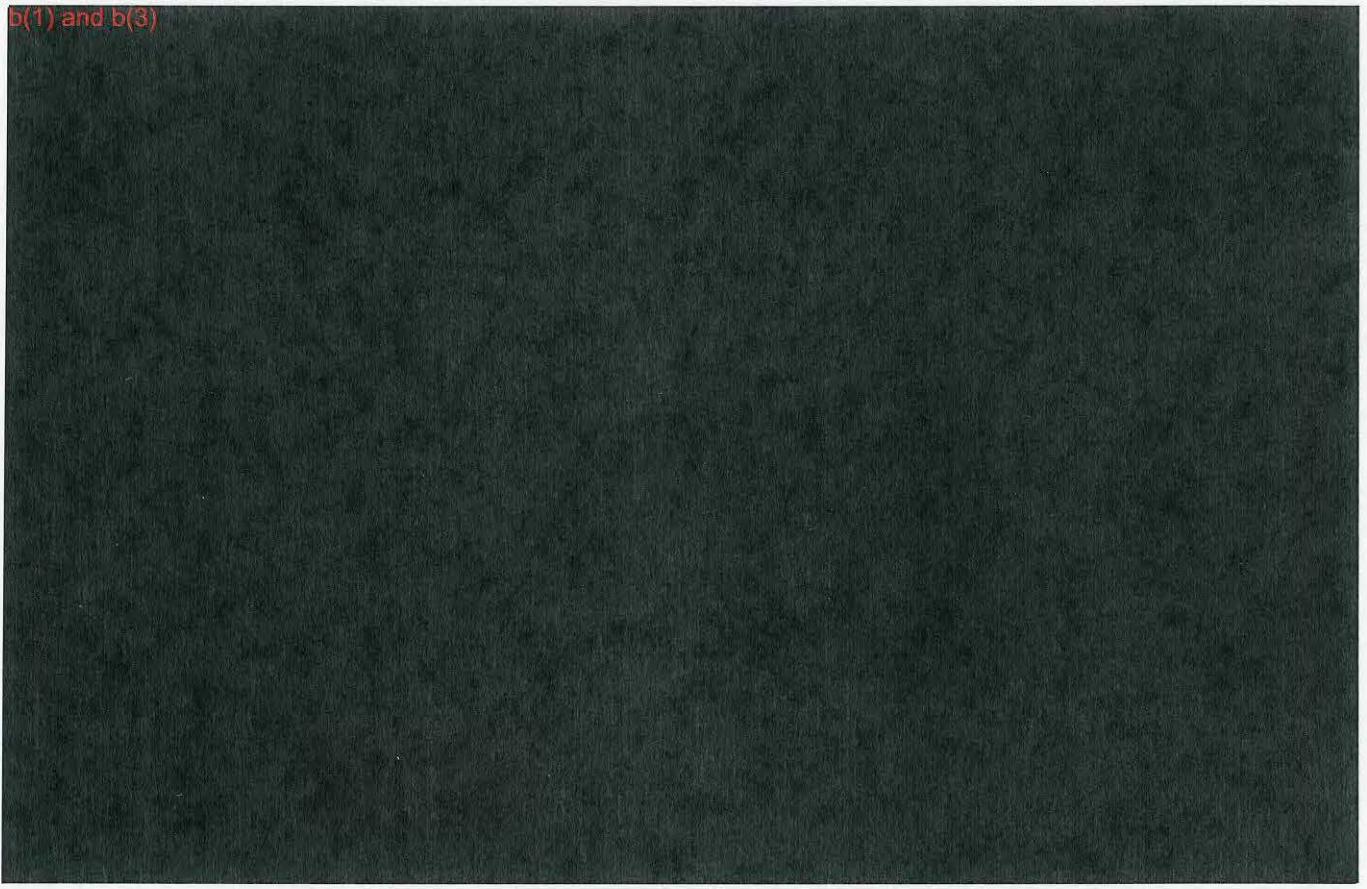
~~TOP SECRET//SI//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

b(1) and b(3)



MEMORANDUM OPINION

This matter is before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications,” which was filed on August 24, 2012

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

(“August 24 Submission”). Through the August 24 Submission, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or the “Act”), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth below, the government’s request for approval is granted.

I. BACKGROUND

The August 24 Submission includes (b)(1) and (b)(3)

b(1) and b(3)

(b)(1) and (b)(3) all of which were executed by the Attorney

General and the Acting Director of National Intelligence (“DNI”) pursuant to Section 702. Each of the (b)(1) and (b)(3) 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 NSA and FBI respectively; and four sets of minimization procedures, for use by NSA, FBI, CIA, and the National Counterterrorism Center (“NCTC”), respectively.

Like the acquisitions approved by the Court in all prior Section 702 dockets, collection under Certifications (b)(1) and b(3) is limited to “the targeting of non-United

States persons reasonably believed to be located outside the United States.”

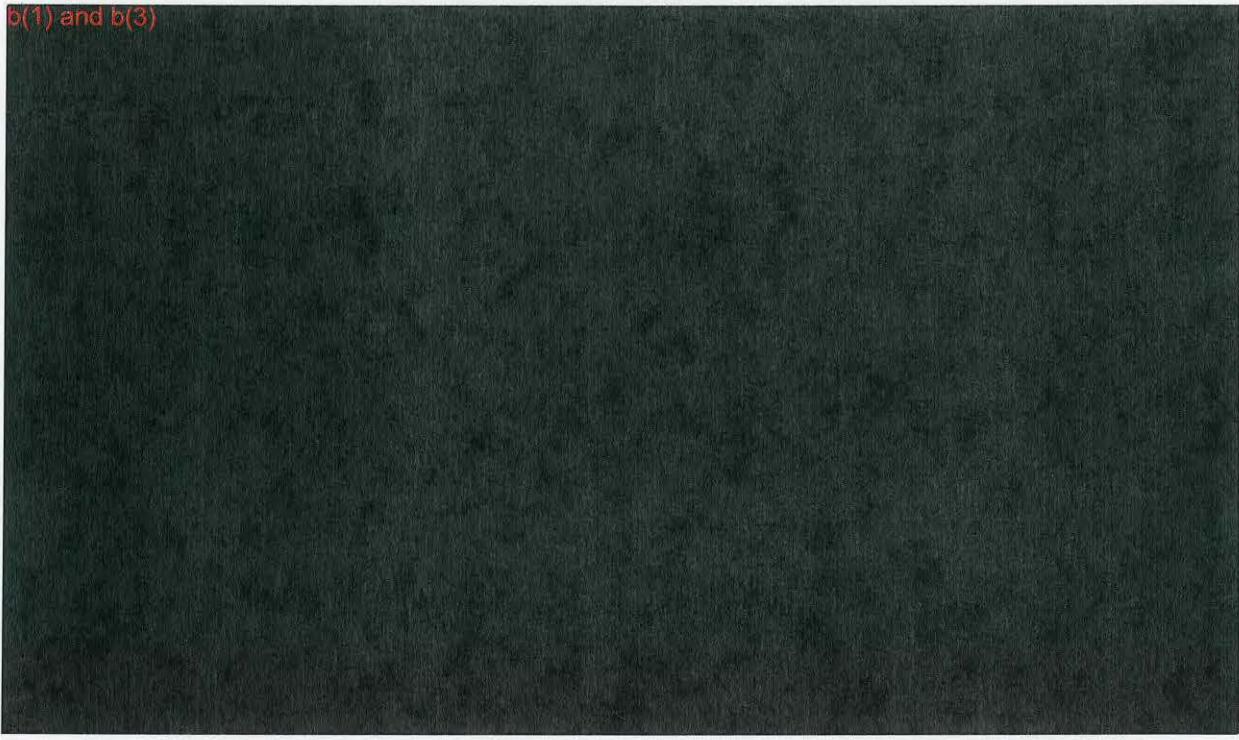
b(1) and b(3)

b(1) and b(3)

b(1) and b(3)

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

b(1) and b(3)



The August 24 Submission also includes amendments to certifications that have been submitted by the government and approved by the Court in all prior Section 702 dockets. See
b(1) and b(3)

Docket Nos.

b(1) and b(3)

(collectively, the "Prior

702 Dockets"). The amendments, which have been authorized by the Attorney General and the DNI, provide that information collected under the certifications in the Prior 702 Dockets will, effective upon the Court's approval of Certifications b(1) and b(3)

be handled

subject to the same minimization procedures that have been submitted for use in connection with

b(1) and b(3)
Certifications

b(1) and b(3)

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

Page 3

~~b(1) and b(3)~~

II. REVIEW OF CERTIFICATIONS

The Court must review a certification submitted pursuant to Section 702 of FISA "to determine whether [it] contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court's examination of Certifications ~~b(1) and b(3)~~ confirms that:

- (1) the certifications have been made under oath by the Attorney General and the DNI,¹ as required by 50 U.S.C. § 1881a(g)(1)(A), see ~~b(1) and b(3)~~
~~b(1) and b(3)~~
- (2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see ~~b(1) and b(3)~~
~~b(1) and b(3)~~
- (3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures² and minimization procedures;³
- (4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);⁴ and
- (5) each of the certifications includes an effective date for the authorization in compliance

¹ The Principal Deputy Director of National Intelligence, in her capacity as Acting DNI, executed the Certifications in accordance with 50 U.S.C. § 403-3A(a)(6), which provides in pertinent part that "the Principal Deputy Director of National Intelligence shall act for, and exercise the powers of, the Director of National Intelligence during the absence or disability of the Director of National Intelligence."

² The NSA targeting procedures and FBI targeting procedures are attached to each of the certifications as Exhibits A and C, respectively.

³ The NSA minimization procedures, FBI minimization procedures, CIA minimization procedures, and NCTC minimization procedures are attached to each of the ~~b(1) and b(3)~~ certifications as Exhibits B, D, E, and G, respectively.

⁴ See Affidavits of John C. Inglis, Acting Director, NSA (Tab 1 to ~~b(1) and b(3)~~; Affidavits of Robert S. Mueller, III, Director, FBI (Tab 2 to ~~b(1) and b(3)~~; Affidavits of David H. Petraeus, Director, CIA (Tab 3 to ~~b(1) and b(3)~~

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

with 50 U.S.C. § 1881a(g)(2)(D), see b(1) and b(3)
b(1) and b(3) 5

The Court therefore finds that b(1) and b(3)

b(1) and b(3) contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE AMENDMENTS TO THE CERTIFICATIONS IN THE PRIOR DOCKETS

Under the judicial review procedures that apply to amendments by virtue of Section 1881a(i)(1)(C), the Court must review each of the amended certifications “to determine whether the certification contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court has previously determined that each of the certifications filed in the Prior 702 dockets, as originally submitted to the Court and previously amended, contained all the required elements. Like the prior certifications and amendments, the amendments now before the Court were executed under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), and submitted to the Court within the time allowed under 50 U.S.C. § 1881a(i)(1)(C). See b(1) and b(3)

Pursuant to

Section 1881a(g)(2)(A)(ii), the latest amendments include the attestations of the Attorney General and the DNI that the accompanying NSA and CIA minimization procedures meet the statutory definition of minimization procedures, are consistent with the requirements of the Fourth Amendment, and will be submitted to the Court for approval. b(1) and b(3)

b(1) and b(3)

The latest amendments also

⁵ 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).

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

include effective dates that comply with 50 U.S.C. § 1881a(g)(2)(D) and § 1881a(i)(1).

b(1) and b(3)

All other aspects

of the certifications in the Prior 702 dockets – including the further attestations made therein in accordance with Section 1881a(g)(2)(A), the FBI and NSA targeting procedures submitted therewith in accordance with Section 1881a(g)(2)(B),⁶ and the affidavits executed in support thereof in accordance with Section 1881a(g)(2)(C) – are unaltered by the latest amendments.

In light of the foregoing, the Court finds that the certifications in the Prior 702 Dockets, as amended, each contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

IV. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is required 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). See 50 U.S.C. § 1881a(i)(2)(B) and (C); see also 50 U.S.C. § 1881a(i)(1)(C) (providing that amended procedures must be reviewed under the same standard). Section 1881a(d)(1) provides that the targeting procedures must be “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.” Section 1881a(e)(1) requires that the minimization procedures “meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4),” which is set out

⁶ Of course, targeting under the certifications filed in the Prior 702 Dockets will no longer be permitted once b(1) and b(3) take effect.

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

Page 6

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

in full in Subpart B below. Finally, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A).

A. The NSA and FBI Targeting Procedures Meet the Statutory Requirements.

The NSA and FBI targeting procedures included as Exhibits A and C, respectively, to the August 24 Submission differ in several respects from the corresponding procedures that have previously been approved by the Court. The government has edited Sections II and IV of the NSA targeting procedures, which address “Post-Targeting Analysis by NSA” and “Oversight and Compliance,” respectively. Section II.b of the targeting procedures describes the process used by NSA to determine when collection on a tasked electronic communications facility (e.g., an e-mail account) must stop because a user of the facility has entered the United States. See Amended NSA Targeting Procedures at 6 (§ II.b). The changes, which are clarifying rather than substantive in nature, serve the purpose of describing this process more precisely. The revised provision is consistent with the government’s prior representations to the Court regarding NSA’s post-targeting analysis and presents no difficulty under Section 1881a(d). See Docket Nos.

(b)(1) and (b)(3) June 2, 2010 Mem. Op. at 19-23.

The government has made three changes to Section IV of the NSA targeting procedures. First, the provision has been amended to require NSA to “implement a compliance program” and “conduct ongoing oversight, with respect to its exercise of the authority under section 702 of the Act, including the associated targeting and minimization procedures adopted in accordance with Section 702.” Amended NSA Targeting Procedures at 7 (§ IV). The addition of this undertaking

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

Page 7

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

obviously raises no issue under Section 1881a(d). Second, the government has replaced several references to particular components of NSA in Section IV with references to NSA generally. Id. at 7-8 (§ IV). This change has the effect of making the entire agency, rather than any particular component, responsible for ensuring adherence to particular oversight and compliance requirements set forth in the procedures. Because this change does not alter what must be done, it also presents no concern for the Court under Section 1881a(d). Third, no issue is presented by changing the required frequency for oversight reviews by the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) “at least once every sixty days,” see b(1) and b(3) Docket No. [REDACTED] NSA Targeting Procedures at 8 (§ IV), to “approximately once every two months,” see Amended NSA Targeting Procedures at 8 (§ IV).

The government has made only one change to the FBI targeting procedures that have previously been approved by the Court. b(1), b(3), and b(7)(E) [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] See Amended FBI Targeting Procedures at 2 (§ I.4). b(1), b(3), and b(7)(E) [REDACTED]

[REDACTED] his alteration does not result in any substantive change and, therefore, presents no issue under Section 1881a(d)(1).

For the reasons stated above and in the Court’s opinions in the Prior 702 Dockets, the Court concludes that the revised NSA and FBI targeting procedures are reasonably designed: (1) to ensure that any acquisition authorized under Certifications b(1) and b(3) [REDACTED] is

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

Page 8

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

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, as required by Section 1881a(d).

B. All Four Sets of Minimization Procedures Satisfy the Statutory Requirements.

The NSA, FBI, and CIA minimization procedures attached as Exhibits B, D, and E of the August 24 Submission differ in some respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications b(1) and b(3) [REDACTED] b(1) and b(3) [REDACTED] The NCTC minimization procedures included as Exhibit G to the August Submission are entirely new.

As noted above, the Court must determine whether these procedures meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) and 1821(4). See 50 U.S.C. § 1881a(e)(1). The definitions at Sections 1801(h) and 1821(4) are substantively identical for present purposes and 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;[⁷]

⁷ 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 –

(continued...)

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

(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 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).⁸ For the reasons set forth below, the Court concludes that the minimization procedures filed as part of the August 24 Submission satisfy this definition, as required by 50 U.S.C. § 1881a(e).

⁷(...continued)

(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.

⁸ 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).

1. *The CIA Minimization Procedures.*

The government has made several changes to the CIA minimization procedures.

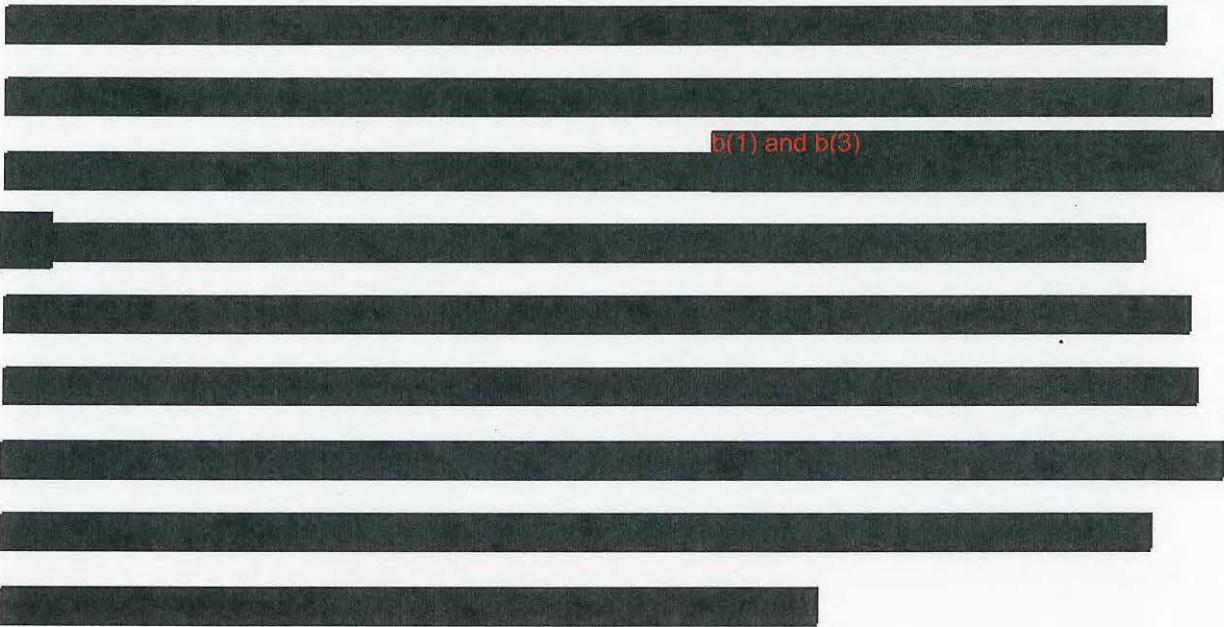
Queries of Section 702 Information. The government has modified Section 4, which addresses the querying by CIA of information collected pursuant to Section 702. Like the previously-approved provision, the revised provision still generally requires that CIA queries of Section 702 information be “reasonably designed to find and extract foreign intelligence information”; that CIA keep records of such queries; and that DOJ and ODNI review the query records. See Amended CIA Minimization Procedures at 3 (§ 4). However, new qualifying language in the amended provision states that notwithstanding these general requirements, CIA personnel may: (1) “query CIA electronic and data storage systems that contain metadata to find, extract, and analyze metadata^[9] pertaining to communications”; (2) “use such metadata to analyze communications”; (3) “upload or transfer some or all such metadata to other CIA electronic and data storage systems for authorized foreign intelligence purposes”; and (4) “disseminat[e] . . . metadata from communications acquired under Section 702 of the Act . . . in accordance with the applicable provisions of these procedures.” Id. (§ 4.a).

The FBI Minimization Procedures previously approved by the Court contain a similar provision for metadata queries. See, e.g., Docket No. [REDACTED] b(1) and b(3) [REDACTED] FBI Minimization Procedures at 16 (§ 3.D (“Retention - Queries of Electronic and Data Storage Systems

⁹ The procedures provide that “‘metadata’ is dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport, or meaning of the communication.” Amended CIA Minimization Procedures at 1 (§ 1.c).

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

Containing Raw FISA-acquired Information”)). [b(1), b(3), and b(7)(E)]



[b(1) and b(3)]

Section 4 of the CIA minimization procedures has also been modified to clarify that for purposes of the procedures, “the term query does not include a user’s search or query of a CIA electronic and data storage system that contains raw FISA-acquired information, where the user does not receive the underlying raw FISA-acquired information in response to the search or otherwise have access to the raw FISA-acquired information that is searched.” Amended CIA Minimization Procedures at 3 (§ 4.b). This addition to Section 4 clarifies that a search that merely notifies the querying analyst of the existence of responsive Section 702 information – without actually providing access to the information itself – is not subject to the general querying restrictions of Section 4. Because this addition does not affect the circumstances under which CIA may acquire, retain, or disseminate U.S.-person information, it presents no concern under Section 1801(h).

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

Page 12

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

Oversight Functions and Vulnerability Assessments. The government has also added two new provisions to Section 6 of the CIA minimization procedures. The first provides that nothing in the procedures prohibits the performance of “lawful oversight functions” by CIA itself, or by DOJ, ODNI, or the “applicable Offices of the Inspectors General.” Amended CIA Minimization Procedures at 4 (§6.f). The new language merely makes explicit that the procedures should not be read to obstruct or hinder lawful and appropriate oversight functions. The Court has previously approved a similar provision in the Section 702 context. The previously-approved FBI minimization procedures, for instance, include a provision stating [redacted] b(1), b(3), and b(7)(E) [redacted]

Docket No. [redacted] b(1) and b(3) [redacted], FBI Minimization Procedures at 3 (§ I.F). The new CIA provision is broader, insofar as it expressly contemplates that certain agencies outside of CIA may perform oversight functions and in so doing could conceivably receive U.S. person information. The Court is satisfied, however, that limited disclosure of information to these recipients in order for them to discharge their oversight responsibility does not run afoul of Section 1801(h).

The second new component of Section 6 states that nothing in the procedures prevents CIA from conducting “vulnerability assessments using information acquired pursuant to Section 702 of the Act in order to ensure that CIA systems have not been compromised.” Amended CIA Minimization Procedures at 4 (§ 6.g). This language allows CIA to use information collected under Section 702 in efforts to prevent its information systems from being compromised by malware or other similar threats and to detect and remedy intrusions after they have occurred. The new language states that Section 702 information used for vulnerability assessments may be

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

Page 13

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

“retained for one year solely for that limited purpose,” and “may be disseminated only in accordance with the applicable provisions of these procedures.” Id. at 4-5 (§ 6.g). This provision changes nothing about the circumstances in which CIA may acquire or disseminate Section 702 information. Though the new provision broadens CIA’s authority to retain certain Section 702 information, including U.S. person information, the resulting change is modest in scope. Furthermore, the new provision is narrowly tailored to serve an important national security purpose; maintaining the integrity of CIA’s systems is essential to the agency’s fulfillment of its mission to produce, obtain, and disseminate foreign intelligence information. This amendment is consistent with Section 1801(h).

Waiver of Destruction Requirement. Finally, the government has made a minor change to Section 8 of the CIA minimization procedures. Section 8 generally requires the CIA to destroy any communication that is acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-U.S. person located outside the United States, but who was in fact, at the time of acquisition, a U.S. person or a person located in the United States. Amended CIA Minimization Procedures at 7 (§ 8). The Director of the CIA may waive the destruction requirement for such a communication by making a specific determination in writing that the communication contains significant foreign intelligence information or evidence of a crime. Id. New language further clarifies that such waiver determinations must be made “on a communication-by-communication” basis. Id. This further specification of the waiver process presents no issue under Section 1801(h).

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

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

2. *The FBI and NCTC Minimization Procedures.*¹⁰

Presumptions Regarding U.S. Person Status. The government has altered the language of the FBI minimization procedures regarding when it is appropriate **(1), b(3), b(7)(E)**

[REDACTED] Under the previously-approved procedures, **(1), b(3), and b(7)(E)**

[REDACTED] The procedures require the FBI to
(1), b(3), and b(7)(E)

[REDACTED]
See
(1) and b(3)
Docket No. [REDACTED] FBI Minimization Procedures at 2 (§ I.C). However, the previously-approved procedures permitted the FBI to **(1), b(3), and b(7)(E)** [REDACTED] See id. at 3 (§ I.C). The amended procedures adopt a uniform rule that allows the FBI **(1), b(3), and b(7)(E)** [REDACTED]

[REDACTED] Amended FBI Minimization Procedures at 2-3 (§ I.D).

This change brings the FBI minimization procedures into line with **(1), b(3), and b(7)(E)**

¹⁰ The FBI minimization procedures previously submitted by the government and approved by the Court consist of a copy of the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search, modified in a number of respects by a three-page cover document. See, e.g., Docket No. **(1) and b(3)** Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amendment Certifications, Exh. D (filed Apr. 22, 2011). Although the amended FBI minimization procedures are substantively similar in many respects to the previously-approved procedures, the amended procedures consist of a single, self-contained document that does not resort to cross-referencing. This formatting change reduces the risk of confusion and mistake and serves to bring the procedures into conformity with the FISC rules, which now restrict cross-referencing in procedures submitted to the Court for review. See FISC Rule 12 (adopted Nov. 1, 2010).

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

Page 15

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

b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

[REDACTED] b(1) and b(3) [REDACTED] Oct. 31, 2011 b(1),
b(3), and b(7)(E)

[REDACTED]. In the context of acquisitions that are directed at
non-U.S. persons located outside the United States, the Court concludes that this change to the
FBI minimization procedures, b(1), b(3), and b(7)(E)

comports with the definition of minimization procedures set forth at Section 1801(h).

b(1), b(3), and b(7)(E) The government has added language providing that
notwithstanding the remainder of the procedures, (1), b(3), and b(7)(E)

[REDACTED]
[REDACTED] Amended FBI Minimization Procedures
at 3 (§ I.G). Like the similar provision of the amended CIA minimization procedures that is
discussed above, this new provision of the FBI procedures is narrowly tailored to serve its
purpose. See id. at 3-4 (§I.G) b(1), b(3), and b(7)(E)

[REDACTED] The Court similarly finds that this change to the FBI
procedures is consistent with the requirements of Section 1801(h).¹¹

b(7)(E) The government has modified the previously-

¹¹ The government has also broadened Section I.G to include “lawful oversight” of the FBI by DOJ, ODNI, and “applicable Offices of the Inspectors General,” in addition to oversight by the FBI itself. See Amended FBI Minimization Procedures at 3 (§ I.G). Like the similar amendment to the CIA minimization procedures discussed above, this change presents no issue under Section 1801(h).

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

Page 16

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

approved provision regarding FBI queries of information acquired under Section 702. **b(7)(E)**

[REDACTED] Amended FBI Minimization Procedures at 11

(§ III.D. **b(7)(E)**)

[REDACTED] See id. Like the similar change to the CIA minimization procedures discussed above, this change presents no issue under Section 1801(h).

b(1), b(3), and b(7)(E) The government has deleted the provisions of the FBI minimization procedures limiting the acquisition and use of '**b(1), b(3), and b(7)(E)**' See **b(1) and b(3)** Docket No. [REDACTED] FBI Minimization Procedures at 8-9 (§ 2.C); id. at 13-14 (§ III.C.2). In

the context of telephone and Internet communications, the term **b(1), b(3), and b(7)(E)**

[REDACTED] See id. at 8-9 (§ 2.C). The Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search limit the circumstances in which such communications can be retained and used for investigative or analytical purposes. See Docket No. **b(1) and b(3)** Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search at 13-14 (§ III.C.2) (as approved by the FISC on May 18, 2012). Although the same restrictions appear in prior versions of the FBI's Section 702 minimization procedures, they have no practical effect because

b(1), b(3), and b(7)(E) See Docket No. [REDACTED]

FBI Minimization Procedures, Cover Document at 1. In light of that definition (which is retained

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

Page 17

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

in the amended procedures¹²), there are no b(1), b(3), and b(7)(E) for the FBI to minimize.

Because the deletion of the provisions regarding b(1), b(3), and b(7)(E) does not alter the manner in which the FBI acquires, retains, or disseminates Section 702 information, this change is not problematic under Section 1801(h).¹³

b(1), b(3), and b(7)(E) The government has added a new provision to the FBI minimization procedures requiring the FBI to b(1), b(3), and b(7)(E)

See Amended FBI Minimization Procedures at 9-10 (§ III.C.2). This change obviously presents no issue under Section 1801(h).

b(1), b(3), and b(7)(E) The government has made a minor change to the b(1), provision set forth in the final paragraph of Section III.A of the amended FBI minimization procedures. This provision, b(1), b(3), and b(7)(E)

generally requires the FBI to remove from its systems any communication that is acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-U.S. person located outside the United States but who is located inside the United States at the time of acquisition or is subsequently determined to be a U.S. person. See Amended FBI Minimization Procedures at 6 (§ III.A). The Director or Deputy Director of the FBI may

¹² See Amended FBI Minimization Procedures at 2 (§ I.B.3) b(1), b(3), and b(7)(E)
b(1), b(3), and b(7)(E)

¹³ The Court reaches this conclusion with the understanding the FBI does not acquire, either directly or through NSA, so-called “about” communications – i.e., communications that are not to or from a tasked facility but merely contain a reference to a tasked facility. Certain “about” communications are acquired by NSA through its upstream collection of Internet communications, the fruits of which are not shared with FBI or CIA in unminimized form. See Nov. 30 Op., *supra*, at 7 n.3.

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

Page 18

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

b(1), b(3), and b(7)(E) by making a specific determination in writing th b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

[REDACTED] Id. The amended provision contains new language further clarifying that b(1), b(3), and b(7)(E) s must be made b(1), b(3), and b(7)(E) basis. b(1), b(3), and b(7)(E)

[REDACTED] this amendment to the FBI procedures does not alter the requirements of the b(1), b(3), and [REDACTED] and therefore presents no issue under Section 1801(h).

b(1), b(3), b(7)(E) The amended FBI minimization procedures retain a previously-approved provision requiring that FBI b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

Amended FBI Minimization Procedures at 19 (§ III.G.1.a). However, new language provides that an AD (or his superior) can b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED] Id. The amended provision further states that b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED] Id. This change limits the FBI's discretion to b(1), Section 702 information and, therefore, presents no concern under Section 1801(h).

b(1), b(3), b(7)(E) The amended FBI minimization procedures retain the

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

Page 19

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

previously-approved requirements for [b(1), b(3), b(7)(E)], with one minor change. See Amended FBI Minimization Procedures at 12-16 (§ III.E). The previously-approved minimization procedures require that, when the FBI determines that [b(1), b(3), b(7)(E)] has been identified, the FBI shall [b(1), b(3), and b(7)(E)]

Docket No. [b(1) and b(3)], FBI Minimization Procedures at 18 (§ III.E.1.c) & 20 (§ III.E.2.c). The amended FBI Minimization Procedures require the FBI to [b(1), b(3), and b(7)(E)]

[b(1), b(3), and b(7)(E)] See Amended FBI Minimization Procedures at 12-13 (§ III.E.1.c) & 14 (§ III.E.2.c). The Court recently approved identical changes to the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search. See Docket Numbers [b(1) and b(3)] May 18, 2012 Mem. Op. and Order (“May 18 Opinion”) at 18-19. The Court sees no reason to reach a different result here, in the context of collection that is directed at non-U.S. persons located outside the United States and, therefore, less likely to [b(1), b(3), b(7)(E)]

Dissemination. The dissemination provisions of the FBI minimization procedures reflect a number of changes from the previously-approved procedures. Three of these changes conform the Section 702 minimization procedures to the dissemination provisions of the recently-revised Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search:

- The amended FBI minimization procedures [b(1), b(3), and b(7)(E)]

b(1), b(3), and b(7)(E)

' Amended FBI Minimization Procedures at 21 (§ IV.A) (emphasis added).

- With regard to foreign governments, the amended FBI minimization procedures explicitly b(1), b(3), and b(7)(E)

. See Amended FBI Minimization Procedures at 22-24 (§ IV.C).

- The amended FBI minimization procedures b(1), b(3), and b(7)(E)

The previously-approved procedures state that the FBI b(1), b(3), and b(7)(E)

" See Docket No. b(1) and b(3) FBI Minimization Procedures at 27 (§ IV.A) (emphasis added).¹⁴ In contrast, the amended procedures b(1), b(3), and b(7)(E)

Amended FBI Minimization Procedures at 21 (§ IV.A) (emphasis added). As discussed in the May 18 Opinion, b(1), b(3), and b(7)(E)

See May 18 Op. at 14-15.¹⁵

¹⁴ Section IV.A of the previously-approved FBI minimization procedures further provides that b(1), b(3), and b(7)(E)

(Emphasis added.) This language is stricken by the amendments to the FBI procedures and rendered superfluous by b(1), b(3), and b(7)(E)

¹⁵ The amendments to the FBI procedures also replace certain references to b(1), b(3), and b(7)(E) Compare, e. g., Docket No. [REDACTED] FBI Minimization Procedures at 30-31 (§ IV.D), with Amended FBI Minimization Procedures at 24 (§ IV.D). The government advises that this change in terminology is not (continued...)

For the reasons set forth in the May 18 Opinion approving the same modifications to the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search, the Court concludes that these changes to the amended FBI minimization procedures for Section 702 acquisitions also are consistent with the requirements of Section 1801(h). In reaching this conclusion, the Court relies upon the same Executive Branch representations on which it relied in the May 18 Opinion.

The amended FBI minimization procedures contain a new provision permitting the FBI, in the event Section 702 information **b(1), b(3), and b(7)(E)**

[REDACTED]

[REDACTED] Amended FBI Minimization

Procedures at 26 (§ IV.H). This provision closely tracks language that the Court has approved as a supplemental minimization procedure in numerous orders granting authority to conduct electronic surveillance and physical search in cases **b(1), b(3), and b(7)(E)**

[REDACTED] See, e.g., Docket No. **b(1) and b(3)** Primary Order and Warrant at 10.

The Court sees no issue under Section 1801(h) with the inclusion of such a provision in the Section 702 minimization procedures.

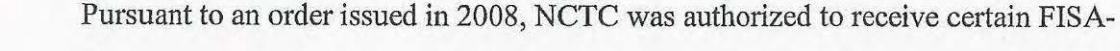
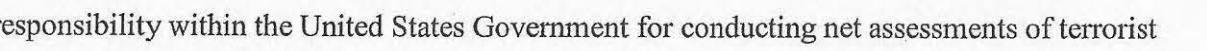
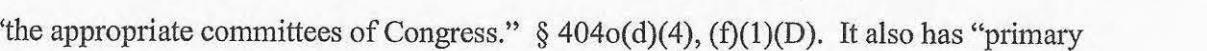
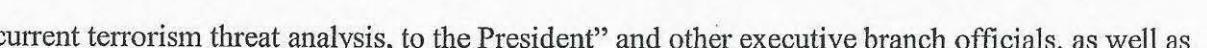
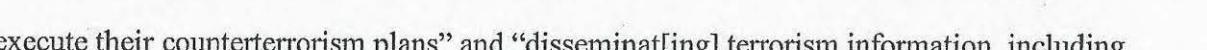
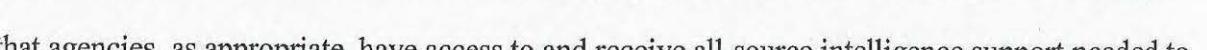
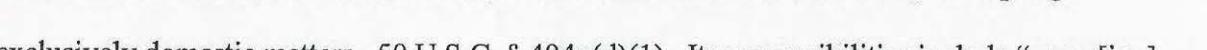
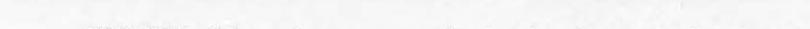
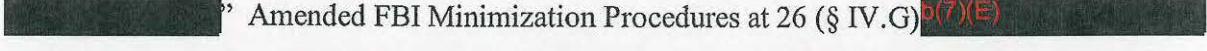
Finally, the amended FBI minimization procedures **b(7)(E)**

[REDACTED] **b(1), b(3), and b(7)(E)**

¹⁵(...continued)
intended to have any substantive effect. See May 18 Op. at 13 n.23.

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

b(1), b(3), and b(7)(E)



NCTC is “the primary organization in the United States Government for analyzing and integrating all intelligence . . . pertaining to terrorism and counterterrorism,” excepting exclusively domestic matters. 50 U.S.C. § 404o(d)(1). Its responsibilities include “ensur[ing] that agencies, as appropriate, have access to and receive all-source intelligence support needed to execute their counterterrorism plans” and “disseminat[ing] terrorism information, including current terrorism threat analysis, to the President” and other executive branch officials, as well as “the appropriate committees of Congress.” § 404o(d)(4), (f)(1)(D). It also has “primary responsibility within the United States Government for conducting net assessments of terrorist threats.” § 404o(f)(1)(G).

Pursuant to an order issued in 2008, NCTC was authorized to receive certain FISA-

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

Page 23

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

derived information from terrorism cases that FBI had uploaded to its [b(1), b(3), and b(7)(E)] does not contain raw FISA information. Rather, it contains FBI investigative reports and other work product, some of which contain FISA information. As a result, FISA-derived information regarding U.S. persons that NCTC personnel can access [b(1), b(3), and b(7)(E)] has already been subject to minimization by the FBI. The Court approved procedures in 2008 that permit the FBI to [b(1), b(3), and b(7)(E)]

[REDACTED]
[REDACTED]
[REDACTED]
Docket No. [b(1) and b(3)] Oct. 8, 2008 Mem. Op. at 3-6. The Court found that [FBI b(1), b(3), and b(7)(E)]

[REDACTED]. Id. at 3.

[b(1), b(3), and b(7)(E)]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
See Docket No. [b(1) and b(3)] [b(1), b(3), and b(7)(E)]

¹⁶ [b(1), b(3), and b(7)(E)]

(continued...)

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

The new Section IV.G of the amended Section 702 FBI minimization procedures and the new NCTC minimization procedures are consistent with the requirements of Section 1801(h). In light of NCTC's important role in analyzing and processing intelligence regarding terrorism and counterterrorism, providing it with access to terrorism- and counterterrorism-related information in FBI general indices is consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, as required by Section 1801(h)(1). Given the non-U.S. person, overseas focus of Section 702 collection, the information at issue ~~b(1), b(3), and b(7)(E)~~ [REDACTED] to contain U.S. person information that is not foreign intelligence information as defined in Section 1801(e)(1), which is the principal concern of Section 1801(h)(2). Finally, the FBI will have applied its own minimization procedures to the information at issue here before it is shared with NCTC, and those procedures allow the dissemination of evidence of a crime for law enforcement purposes. See Amended FBI Minimization Procedures at 22-24 (§ IV.B & C). Accordingly, the Court is satisfied that the FBI and NCTC minimization procedures, taken together, permit the dissemination of evidence of a crime for law enforcement purposes, as required by Section 1801(h)(3).

3. *The NSA Minimization Procedures.*

The NSA minimization procedures have been altered in a number of respects. Before addressing the changes, some background discussion is warranted.

¹⁶(...continued)
~~b(1), b(3), and b(7)(E)~~
[REDACTED]
The amended FBI procedures at issue here do not permit the sharing of unminimized Section 702 information with NCTC.

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

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

a. *The Scope of NSA's Upstream Collection.*

Last year, following the submission of Certifications ~~b(1) and b(3)~~ for renewal, the government made a series of submissions to the Court disclosing that it had materially misrepresented the scope of NSA's "upstream collection" under Section 702 (and prior authorities including the Protect America Act). The term "upstream collection" refers to the acquisition of Internet communications as they transit the "internet backbone" facilities ~~b(1) and b(3)~~ as opposed to the collection of communications directly from Internet service providers like ~~b(1) and b(3)~~. See Docket Nos. ~~b(1) and b(3)~~ Oct. 3, 2011 Memorandum Opinion ("Oct. 3 Op.") at 5 n.3. Since 2006, the government had represented that NSA's upstream collection only acquired discrete communications to or from a facility tasked for acquisition and communications that referenced the tasked facility (so-called "about" communications). See *id.* at 15-16. With regard to the latter category, the government had repeatedly assured the Court that NSA only acquired ~~b(1)~~ specific categories of "about" communications. *Id.*

The government's 2011 submissions made clear, however, that NSA's upstream collection was much broader than the government had previously represented. For the first time, the government explained that NSA's upstream collection results in the acquisition of "Internet transactions" instead of discrete communications to, from or about a tasked selector. See *id.* at 15. Internet transactions, the government would ultimately acknowledge, could and often do contain multiple discrete communications, including wholly domestic non-target communications and other non-target communications to, from, or concerning U.S. persons. *Id.*

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

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

While the government was able to show that the percentage of wholly domestic non-target communications and other non-target communications to, from, or concerning U.S. persons being acquired was small relative to the total volume of Internet communications acquired by the NSA pursuant to section 702, the acquisition of such communications nonetheless presented a significant issue for the Court in reviewing the procedures. In fact, it appeared that NSA was annually acquiring tens of thousands of Internet transactions containing at least one wholly domestic communication; that many of these wholly domestic communications were not to, from, or about a targeted facility; and that NSA was also likely annually acquiring tens of thousands of additional Internet transactions containing one or more non-target communications to or from U.S. persons or persons in the United States. Id. at 33, 37.

In the October 3 Opinion, the Court approved in large part Certifications b(1) and b(3) [REDACTED] and the accompanying targeting and minimization procedures. The Court concluded, however, that one aspect of the proposed collection – NSA’s upstream collection of Internet transactions containing multiple communications, or “MCTs” – was, in some respects, deficient on statutory and constitutional grounds. The Court concluded that although NSA’s targeting procedures met the statutory requirements, the NSA minimization procedures, as the government proposed to apply them to MCTs, did not satisfy the statutory definition of “minimization procedures” with respect to retention. Oct. 3 Op. at 59-63. As applied to the upstream collection of Internet transactions, the Court found that the procedures were not reasonably designed to minimize the retention of U.S. person information consistent with the government’s national security needs. Id. at 62-63. The Court explained that the net effect of the

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

Page 27

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

procedures would have been that thousands of wholly domestic communications, and thousands of other discrete communications that are not to or from a targeted selector but that are to, from, or concerning United States persons, would be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, were unlikely to contain foreign intelligence information. Id. at 60-61. For the same reason, the Court concluded that NSA's procedures, as the government proposed to apply them to MCTs, failed to satisfy the requirements of the Fourth Amendment. Id. at 78-79. The Court noted that the government might be able to remedy the deficiencies that it had identified, either by tailoring its upstream acquisition or by adopting more stringent post-acquisition safeguards. Id. at 61-62, 79.

By operation of the statute, the government was permitted to continue the problematic portion of its collection for 30 days while taking steps to remedy the deficiencies identified in the October 3 order and opinion. See 50 U.S.C. § 1881a(i)(3)(B). In late October of 2011, the government timely submitted amended NSA minimization procedures that included additional provisions regarding NSA's upstream collection. The amended procedures, which took effect on October 31, 2011 ("Oct. 31, 2011 NSA Minimization Procedures"), require NSA to restrict access to the portions of its ongoing upstream collection that are most likely to contain wholly domestic communications and non-target information that is subject to statutory or Fourth Amendment protection. See Nov. 30 Op. at 7-9. Segregated Internet transactions can be moved to NSA's general repositories only after having been determined by a specially trained analyst not to contain a wholly domestic communication. Id. at 8. Any transaction containing a wholly domestic communication (whether segregated or not) would be purged upon recognition. Id. at

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

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

8, 9. Any transaction moved from segregation to NSA's general repositories would be permanently marked as having previously been segregated. Id. at 8. On the non-segregated side, any discrete communication within an Internet transaction that an analyst wishes to use is subject to additional checks. Id. at 8-10. NSA is not permitted to use any discrete, non-target communication that is determined to be to or from a U.S. person or a person who appears to be in the United States, other than to protect against an immediate threat to human life. Id. at 9. Finally, all upstream acquisitions are retained for a default maximum period of two, rather than five, years. Id. at 10-11.

The Court concluded in the November 30 Opinion that the October 31, 2011 NSA Minimization Procedures adequately remedied the deficiencies that had been identified in the October 3 opinion. Id. at 14-15. Accordingly, NSA was able to continue its upstream collection of Internet transactions (including MCTs) without interruption, but pursuant to amended procedures that are consistent with statutory and constitutional requirements.

However, issues remained with respect to the past upstream collection residing in NSA's databases. Because NSA's upstream collection almost certainly included at least some acquisitions constituting "electronic surveillance" within the meaning of 50 U.S.C. § 1801(f), any overcollection resulting from the government's misrepresentation of the scope of that collection implicates 50 U.S.C. § 1809(a)(2). Section 1809(a)(2) makes it a crime to "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. The Court therefore directed the government to make a written submission addressing

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

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

the applicability of Section 1809(a), which the government did on November 22, 2011. See

Docket No. [REDACTED] b(1) and b(3) Oct. 13, 2011 Briefing Order, and

Government's Response to the Court's Briefing Order of Oct. 13, 2011 (arguing that Section 1809(a)(2) does not apply).

Beginning late in 2011, the government began taking steps that had the effect of mitigating any Section 1809(a)(2) problem, including the risk that information subject to the statutory criminal prohibition might be used or disclosed in an application filed before this Court. The government informed the Court in October 2011 that although the amended NSA procedures do not by their terms apply to information acquired before October 31, NSA would apply portions of the procedures to the past upstream collection, including certain limitations on the use or disclosure of such information. See Nov. 30 Opinion at 20-21. Although it was not technically feasible for NSA to segregate the past upstream collection in the same way it is now segregating the incoming upstream acquisitions, the government explained that it would apply the remaining components of the amended procedures approved by the Court to the previously-collected data, including (1) the prohibition on using discrete, non-target communications determined to be to or from a U.S. person or a person in the United States, and (2) the two-year age-off requirement. See id. at 21.

Thereafter, in April 2012, the government orally informed the Court that NSA had made a "corporate decision" to purge all data in its repositories that can be identified as having been acquired through upstream collection before the October 31, 2011 effective date of the amended NSA minimization procedures approved by the Court in the November 30 Opinion. NSA's

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

Page 30

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

effort to purge that information, to the extent it is reasonably feasible to do so, is now complete.

See Aug. 24 Submission at 9-10.¹⁷

Finally, NSA has adopted measures to deal with the possibility that it has issued reports based on upstream collection that was unauthorized. NSA has identified ^{b(1)} and ^{b(3)} reports that were issued from the inception of its collection under Section 702 to October 31, 2011, that rely at least in part on information derived from NSA's upstream acquisitions from that period. See Sept. 12, 2012 Supplement to the Government's Ex Parte Submission of Reauthorization Certifications at 2 ("Sept. 12 Submission"). The government advises that, of the ^{b(1)} and ^{b(3)} reports, ^{b(1)} have been confirmed to be based entirely upon communications that are to, from or about persons properly targeted under Section 702 and therefore present no issue under Section 1809(a)(2). See id. The government is unable to make similar assurances, however, regarding the remaining ^{b(1)} reports. Accordingly, NSA will direct the recipients of those ^{b(1)} reports (both within NSA and outside the agency) not to further use or disseminate information contained therein without first obtaining NSA's express approval. Id. at 3-4. Upon receipt of such a request, NSA will review the relevant report to determine whether continued use thereof is

¹⁷ The government has informed the Court that NSA stores some of the past upstream collection in repositories in which it may no longer be identifiable as such. ^{b(1) and b(3)}

[REDACTED]. See Aug. 24 Submission at 14-16. Assuming that NSA cannot with reasonable effort identify information in its repositories as the fruit of an unauthorized electronic surveillance, such information falls outside the scope of Section 1809(a)(2), which by its terms applies only when there is knowledge or "reason to know that the information was obtained through electronic surveillance not authorized" by statute.

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

Page 31

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

appropriate. Id. at 4.¹⁸ Finally, the government has informed the Court that it will not use any report that cites to upstream collection acquired prior to October 31, 2011 in an application to this Court absent express notice to, and approval of, the Court. Aug. 24 Submission at 24.

Taken together, the remedial steps taken by the government since October 2011 greatly reduce the risk that NSA will run afoul of Section 1809(a)(2) in its handling of the past upstream acquisitions made under color of Section 702. NSA's self-imposed prohibition on using non-target communications to or from a U.S. person or a person in the United States helped to ensure that the fruits of unauthorized electronic surveillance were not used or disclosed while it was working to purge the pre-October 31, 2011 upstream collection. And NSA's subsequent purge of that collection from its repositories and the above-described measures it has taken with respect to derivative reports further reduce the risk of a problem under Section 1809(a)(2). Finally, the amended NSA minimization procedures provide that in the event, despite NSA's effort to purge the prior upstream collection, the agency discovers an Internet transaction acquired before October 31, 2011, such transaction must be purged upon recognition. See Amended NSA Minimization Procedures at 8 § 3(c)(3). In light of the foregoing, it appears to the Court that the outstanding issues raised by NSA's upstream collection of Internet transactions have been resolved, subject to the discussion of changes to the minimization procedures that appears

¹⁸ For instance, NSA may determine that the report is fully supported by cited communications other than the ones obtained through upstream communication. Sept. 12 Submission at 4. In other instances, NSA may revise the report so that it no longer relies upon upstream communications and reissue it. Id. If such steps are not feasible because the report cannot be supported without the upstream communication, NSA will cancel the report. Id.

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

Page 32

below.¹⁹

b. Changes to the NSA Minimization Procedures.

“Processing” versus “handling” information. In a number of places in the amended NSA minimization procedures, the government has replaced the term “processed” with the word “handled.” See Amended NSA Minimization Procedures at 9 (§ 5(1)) & 12 (§§ 6(c)(1) & 6(c)(2)). Both the previously-approved NSA minimization procedures and the amended procedures define the terms “processed” or “processing” to mean “any step necessary to convert a communication into an intelligible form intended for human inspection.” Id. at 2 (§ 2(h)). The previously-approved procedures did not uniformly use the terms in a manner consistent with that narrow definition. This clarifying change remedies that inconsistency by using the distinct term “handled” or “handling” to refer to the treatment of communications after they have been rendered intelligible for human inspection. This non-substantive change reduces the potential for confusion and mistake and raises no issue under Section 1801(h).

Oversight Functions. Like the amended CIA and FBI minimization procedures discussed above, the amended NSA minimization procedures contain language stating that the procedures do not restrict the exercise of “lawful oversight” of NSA by NSA itself, DOJ, ODNI, or “the applicable Offices of Inspectors General.” Amended NSA Minimization Procedures at 1 (§ 1). For the same reasons, the Court finds that this provision is consistent with Section 1801(h).

¹⁹ Under the circumstances, the Court finds it unnecessary to further address the arguments advanced by the government in its November 22, 2011 response to the Court’s October 13, 2011 briefing order regarding Section 1809(a), particularly those regarding the scope of prior Section 702 authorizations.

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

Vulnerability or Network Assessments. The amended NSA minimization procedures also state that the procedures do not restrict NSA's performance of "vulnerability or network assessments using information acquired pursuant to Section 702 . . . in order to ensure that NSA systems are not or have not been compromised." Amended NSA Minimization Procedures at 1 (§ 1). ~~b(1), b(3), and b(7)(E)~~

[REDACTED], this "vulnerability or network assessments" language also raises no concern under Section 1801(h). The language allows NSA to use information collected under Section 702 in efforts to prevent its information systems from being compromised by malware or other similar threats and to detect and remedy intrusions after they have occurred. Maintaining the integrity of NSA's systems is essential to the agency's fulfillment of its national security mission, including the acquisition, production, and dissemination of foreign intelligence information. The new language is narrowly crafted to serve that purpose, stating that Section 702 information used for vulnerability or network assessments may be "retained for one year solely for that limited purpose," and "may be disseminated only in accordance with the applicable provisions of these procedures." *Id.* at 1 (§ 1).

Upstream Collection. The government has made several changes to Section 3(b) of the NSA minimization procedures, which, among other things, addresses NSA's handling of Internet transactions acquired through its upstream collection. Section (3)(b)(4)(a)²⁰ generally requires NSA to use technical means to segregate and restrict access to the two categories of MCTs that

²⁰ The government has renumbered portions of Section 3 so that the substance of Section 3(b)(5) of the previously-approved procedures now appears in Section 3(b)(4).

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

Page 34

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

are most likely to contain non-target information concerning U.S. persons or persons in the United States. See Nov. 30, 2012 Mem. Op. at 11-12. The amended procedures include new language stating that notwithstanding this general segregation requirement, “NSA may process Internet transactions . . . in order to render such transactions intelligible to analysts.” See Amended NSA Minimization Procedures at 4 (§ 3(b)(4)(a)(1)). The Court’s understanding is that this new language permits NSA to render Internet transactions intelligible to humans before segregating them in accordance with Section 3(b)(4)(a). With the understanding that the procedures continue to preclude access to Internet transactions by intelligence analysts until after segregation (and even then, only in accordance with the remainder of the procedures), the Court is satisfied that this amendment is consistent with Section 1801(h).

The previously approved procedures required NSA to “destroy[] upon recognition” any Internet transaction containing a discrete wholly domestic communications (*i.e.*, a communication as to which the sender and all intended recipients are reasonably believed to be in the United States). See Oct. 31, 2011 NSA Minimization Procedures at 4 § 3(b)(5)(a)(1)(a); see also Nov. 30, 2011 Mem. Op. at 9. The amended procedures state that Internet transactions recognized as containing a discrete wholly domestic communication must “be handled in accordance with Section 5 below.” Amended NSA Minimization Procedures at 4-5 (§§ 3(b)(4)(a)(2)(a), 3(b)(4)(b)(1)). Section 5 requires as a general rule that “a communication identified as a domestic communication (and if applicable the Internet transaction in which it is contained) will be promptly destroyed upon recognition.” Id. at 8 (§ 5). As explained below, however, Section 5 allows the Director of NSA to waive the destruction of a particular

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

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

communication under certain circumstances. Id. at 8-9 (§ 5). Accordingly, the effect of this amendment to Section 3(b) is to convert what was an absolute destruction requirement into a qualified destruction requirement. Nevertheless, as discussed below, the circumstances in which a Director's waiver may be granted are narrowly defined, so that the Court is satisfied that this amendment to the NSA minimization procedures is consistent with Section 1801(h).

Another change to Section 3(b) of the NSA minimization procedures involves metadata. The procedures approved by the Court in the November 30, 2011 Memorandum Opinion contain a provision allowing NSA to copy metadata from Internet transactions that are not subject to segregation pursuant to Section 3(b) without first complying with the other rules for handling non-segregated transactions – *i.e.*, without ruling out that the metadata pertained to a discrete wholly domestic communication or to a discrete non-target communication to or from a U.S. person or a person inside the United States. See Nov. 30, 2011 Mem. Op. at 15-20. Metadata copied pursuant to this provision must be handled in accordance with the other provisions of the procedures. Id. at 16. Furthermore, in the event that NSA later identifies an Internet transaction as containing a wholly domestic communication, any metadata that has been extracted from that transaction must be destroyed. Id.

The amended procedures retain this provision, but now expressly limit it to Internet transactions acquired on or after October 31, 2011. Amended NSA Minimization Procedures at 6 (§ 3(b)(4)(b)(4)). This date change accounts for the fact that, as discussed above, NSA's upstream acquisitions before that date have been subject to an earlier set of minimization procedures that did not provide for the extraction and use of metadata by NSA. See Nov. 30,

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

Page 36

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

2011 Mem. Op. at 20-21. The addition of the date makes clear that although the amended NSA minimization procedures now generally apply to Section 702 information acquired by NSA under all certifications, this metadata provision continues to apply only to information acquired under the 2011 and 2012 certifications. Because this amendment serves only to preserve the status quo with respect to metadata, it presents no issue under Section 1801(h).

Destruction of Raw Data. The government has amended Section 3(c) of the NSA minimization procedures, which limits the retention of raw Section 702 information acquired by NSA. Like the previously-approved procedures, the amended procedures provide a default retention period of two years for upstream Internet communications and a default retention period of five years for all other communications. See Amended NSA Minimization Procedures at 7 (§ 3(c)). The government has added language to Section 3(c) to make clearer that these retention limits are subject to separate provisions of the procedures, which may allow a particular communication to be retained longer – e.g., because it contains U.S. person-identifying information that is necessary to understand foreign intelligence information or assess its importance. See id. at 7 (§ 3(c)); id. at 10-11 (§ 6). New language also makes clear that the determination that a communication qualifies for retention beyond the default “age off” period must be made by NSA on a communication-by-communication basis and, in the case of Internet transactions, is subject to the special rules set forth in Section 3(b) of the procedures. Id. at 7 (§ 3(c)). These clarifying changes raise no issue under Section 1801(h).

The final change to Section 3(c) is new language requiring NSA to destroy upon recognition “[a]ny Internet transaction acquired through NSA’s upstream collection techniques

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

Page 37

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

prior to October 31, 2011.” Amended NSA Minimization Procedures at 8 (§ 3(c)(3)). As discussed above, NSA has deleted “all data objects identified as acquired through NSA’s upstream Internet collection techniques on or before October 31, 2011.” See Aug. 24 Submission at 9. This new language formalizes NSA’s undertaking to destroy any additional information that is heretofore identified as having been acquired through its prior upstream Internet collection and presents no issue under Section 1801(h).

Waiver of Destruction Requirement. The previously-approved NSA minimization procedures generally require that NSA destroy upon recognition any communication that is defined as a domestic communication. Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5). Domestic communications include: (1) any communication that does not have at least one communicant outside the United States, see id. at 2 (§ 2(e)); (2) any communication acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communication was acquired, id. at 7 (§ 3(d)(2)); and (3) any communication acquired by targeting a person who at the time of targeting was believed to be a non-U.S. person but was in fact a U.S. person, id. The destruction requirement can be waived, however, if the Director or Acting Director of the NSA “specifically determines in writing” that:

- (1) the communication is “reasonably believed to contain significant foreign intelligence information,” in which case it can be “provided to the FBI (including United States person identities) for possible dissemination in accordance with its minimization procedures”;
- (2) the communication is “reasonably believed to contain evidence of a crime,” in which case it can be disseminated to appropriate federal law enforcement authorities and retained for a reasonable period of time to permit appropriate

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

access by law enforcement agencies;

(3) the communication is reasonably believed to contain information necessary to be retained for cryptanalytic, traffic analytic, or signal exploitation purposes, or information necessary to understand or assess a security vulnerability, in which case it can be obtained for a period sufficient to permit exploitation; or

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

See id. The previously-approved procedures further provide that notwithstanding these requirements: (1) “if a domestic communication indicates that a target has entered the United States, NSA may advise FBI of that fact”; and (2) NSA may retain and provide to FBI and CIA certain information deemed necessary “for collection avoidance purposes.” Id. at 9 (§ 5).

~~b(1), b(3), and b(7)(E)~~

[REDACTED], the government has amended Section 5 to further clarify that waivers may only be made on a “communication-by-communication basis.” See Amended NSA Minimization Procedures at 8 (§ 5). This change does not alter the requirements of the waiver provision and raises no concern under Section 1801(h).²¹

²¹ In October 2011, the government reported a compliance incident involving NSA’s application of Section 5. The incident was the subject of a more detailed follow-up submission made on August 28, 2012 (“Aug. 28 Submission”). As previously approved by the Court, Section 5 states that a waiver may occur only when “the Director (or Acting Director) specifically determines, in writing,” that one of the four enumerated criteria is met with respect to “[a] communication.” See, e.g., Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5). In accordance with this language, the government represented to the Court in 2008 that the waiver provision would be applied on a “case-by-case basis” rather than categorically. Docket No. ~~b(1) and b(3)~~ Aug. 27, 2008 Hrg. Tr. at 36-37. The Court relied on this representation in approving Section 5. Docket No. ~~b(1) and b(3)~~ Sept. 4, 2008 Mem. Op. at 25 n.24.

In March 2011, however, the Acting Director of NSA made an “advance waiver

(continued...)

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

Another change to Section 5 is the addition of new language that limits the types of domestic communications that may be the subject of a destruction waiver. As amended, the provision requires the Director (or Acting Director) to specifically determine in writing not only that one of the four enumerated conditions is satisfied, but also that “the sender or intended recipient of the domestic communication had been properly targeted under Section 702 of the Act.” See Amended NSA Minimization Procedures at 8 (§ 5). The change has the practical effect of limiting the reach of the waiver provision to domestic communications acquired with the reasonable but mistaken belief that the target is a non-U.S. person located outside the United States. This narrowing amendment is consistent with the requirements of Section 1801(h).

A third change to Section 5 of the NSA minimization procedures broadens the effect of a waiver made on the ground that the communication at issue contains significant foreign intelligence information. While the previously-approved language of Section 5(1) states that a

²¹(...continued)

determination” pursuant to which NSA personnel could thereafter deem “certain terrorism-related communications that met specific criteria . . . to contain ‘significant foreign intelligence’ and hence . . . subject to a destruction waiver.” Aug. 28 Submission at 2. This advance waiver determination was relied upon seven times by NSA personnel until September 2011, when it was rescinded as inconsistent with the requirements of Section 5. Id. It was later determined, however, that in six of those instances no waiver was required. Id. After reporting the incident to the Court, DOJ and NSA undertook a review of NSA’s practice under Section 5 of the procedures. That review revealed that NSA has used the waiver provision on 16 other occasions and that each of those other waivers was consistent with the requirements of Section 5. Id. at 3. Furthermore, NSA, working together with DOJ, has undertaken a number of steps to improve coordination of guidance involving NSA’s FISA authorities (including Section 702) and is continuing to strengthen its internal compliance infrastructure. Id. at 3-6. In light of the corrective measures taken by the government following the “advance waiver determination” incident, the Court is satisfied that the incident does not preclude a finding that NSA’s minimization procedures satisfy the requirements of Section 1801(h).

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

Page 40

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

communication retained on that basis can be “provided to the FBI . . . for possible dissemination in accordance with its minimization procedures,” Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5(1)), the amended provision states that such a communication “may be retained, handled, and disseminated in accordance with these procedures,” Amended NSA Minimization Procedures at 9 (§ 5(1)). The result of this change is that NSA may retain, use, and disseminate such a communication as if it constitutes a “foreign communication.” See Amended NSA Minimization Procedures at 10-12 (§§ 6-7) (setting forth rules for retention and dissemination of foreign communications). Read in isolation, this amendment appears to give NSA substantially more leeway to retain, use, and disseminate a domestic communication that is the subject of the waiver on “significant foreign intelligence” grounds. As discussed in the preceding paragraph, however, the waiver provision, as amended, now may be applied only to those domestic communications acquired with a reasonable, but mistaken, belief that the target is a non-U.S. person located outside the United States. The Court has previously recognized that Section 702 authorizes the government to acquire such communications. See Docket No. [REDACTED] b(1) and b(3) Sept. 4, 2008 Mem. Op. at 25-26. Moreover, if a communication retained on this basis contains U.S.-person identifying information, that information must be deleted before the communication can be disseminated outside NSA unless one of eight specific exceptions applies. See Amended NSA Minimization Procedures at 11-12 (§ 6(b)). Under the circumstances, the Court is satisfied that this amendment to Section 5(1) of the NSA minimization procedures is consistent with Section 1801(h).

Another change to the NSA minimization procedures provides that in the event a

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

Page 41

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

domestic communication subject to a waiver by the Director or Acting Director is contained within an Internet transaction, NSA may retain the entire transaction. See Amended Minimization Procedures at 9 (§ 5). This change addresses NSA's inability to disaggregate Internet transactions that it has acquired under Section 702 without destabilizing its systems. See b(1) and b(3) Docket Nos. [REDACTED] Government's Response to the Court's Briefing Order of May 9, 2011 (filed June 1, 2012) at 22. The change permits NSA to retain not just the particular portion of an Internet transaction that is deemed to qualify for a waiver, but also other unrelated portions of the transaction within which it was acquired, which may include non-target U.S. person information with no foreign intelligence value. For several reasons, the Court is satisfied that this change is consistent with the requirements of Section 1801(h). First, NSA has only applied the waiver provision 16 times since Section 702 collection commenced in 2008. See Aug. 28 Submission at 2. Furthermore, as discussed above and in the November 30 Opinion, NSA's minimization procedures include special handling requirements for Internet transactions, including protections for non-target U.S. person information, that will apply to any transaction that is retained by NSA following a Section 5 waiver. Finally, the procedures require NSA to delete U.S.-person identifying information from a communication before disseminating it outside the agency, unless one of eight specific exceptions applies. See Amended NSA Minimization Procedures at 11-12 (§ 6(b)).

The final change to Section 5 involves what NSA may do, absent a Director's waiver, in the event that a domestic communication indicates that a target has entered the United States. The previously-approved procedures allow NSA to advise the FBI of the fact of the target's entry

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

Page 42

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

into the United States and to retain and provide to FBI and CIA technical information about the communication for “collection avoidance purposes.” Oct. 31, 2011 NSA Minimization Procedures at 9 (§ 5). The amended procedures permit NSA not only to inform the FBI of the fact of the target’s entry into the United States and share with the FBI and CIA the same technical “collection avoidance” information, but also to provide to the FBI “any information concerning the target’s location that is contained in the communication.” Amended NSA Minimization Procedures at 10 (§ 5). In addition, the amended provision states that NSA “may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL).” *Id.* This change to Section 5 allows NSA to share limited information with the FBI and serves to better facilitate the transition from Section 702 coverage of the target to other forms of surveillance or investigation that are permitted within the United States. The Court is satisfied that this amendment to the procedures is consistent with Section 1801(h).

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

The final question before the Court is whether the targeting and minimization procedures included as part of the August 24 Submission are consistent with the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A). Largely for the same reasons that the Court has concluded that the amended procedures meet the requirements of Section 1881a(d)-(e), the Court is also satisfied that the amended procedures are reasonable under the Fourth Amendment. The basic framework of protections formed by the previously-approved procedures remains intact. Many of the amendments made by the government add to those protections or merely serve to clarify what is

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

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

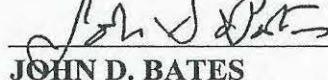
required of the government. The remaining changes do not individually or collectively alter the Court's prior conclusion that the targeting and minimization procedures are consistent with the Fourth Amendment.

IV. CONCLUSION

For the foregoing reasons, the Court finds that the certifications and amendments submitted in the above-captioned dockets pursuant to Section 1881a(g) contain all the required elements and that the targeting and minimization procedures adopted in accordance with Section 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment.

Orders approving the certifications, the amendments, and the use of the accompanying procedures are being entered contemporaneously herewith.

ENTERED this 20th day of September 2012, in Docket Nos. b(1) and b(3)



JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

b(6), b(7)(C)

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

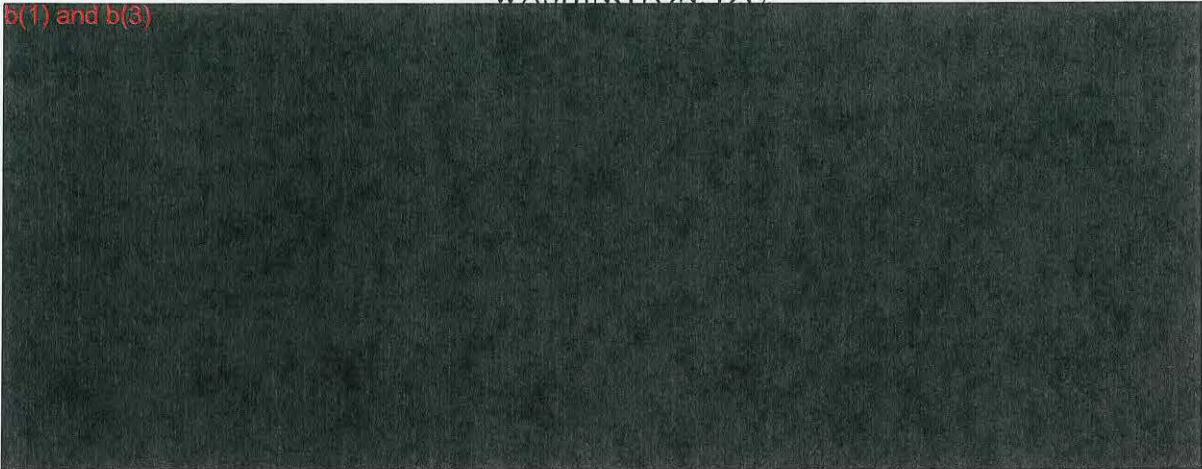
~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

b(1) and b(3)



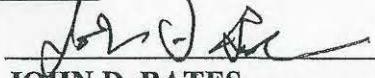
ORDER

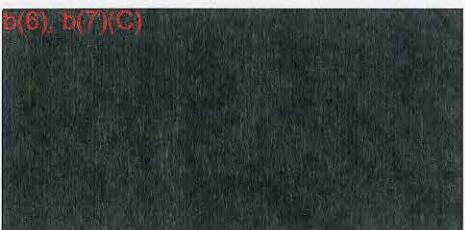
For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications referenced above contain all the required elements and that the targeting procedures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

09-20-2012 P05:56

ENTERED this 20th day of September 2012, at _____ Eastern Time, in
Docket Nos. 


JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

b(6), b(7)(C)


~~SECRET~~

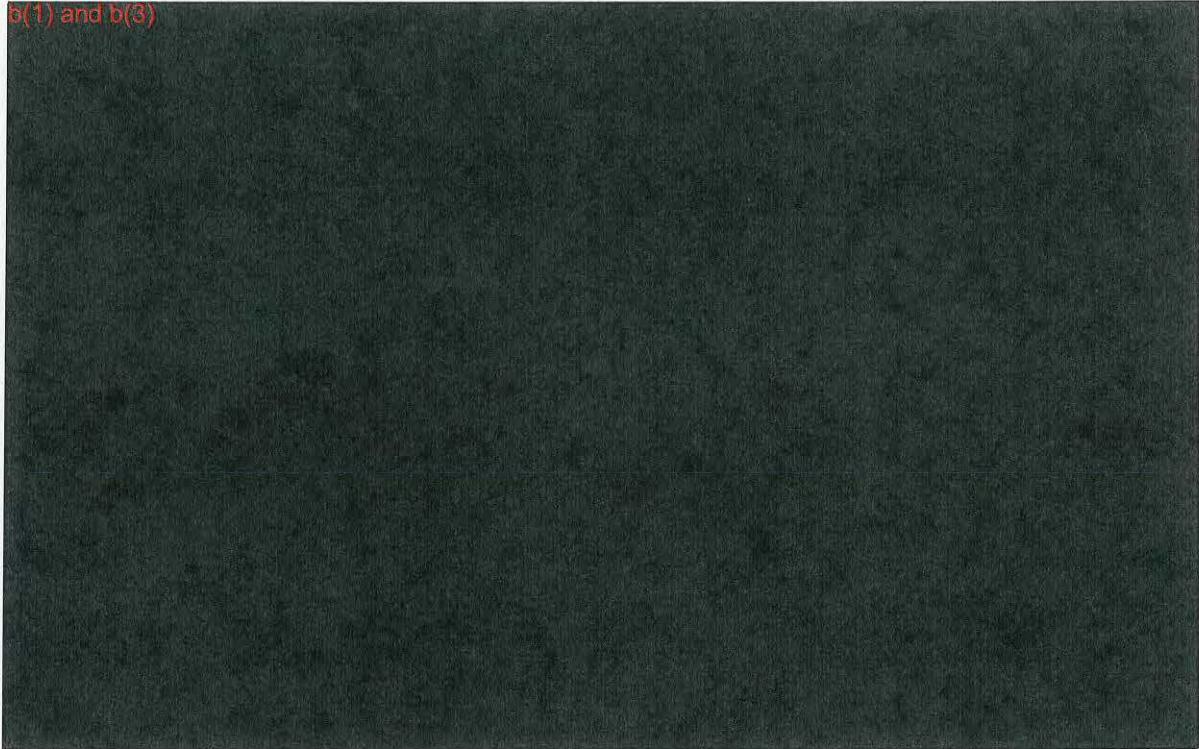
~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

b(1) and b(3)



ORDER

For the reasons stated in the Memorandum Opinion 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 on August 23, 2012, contain all the required elements and that the targeting procedures and minimization procedures approved for use in connection with those amended certifications are consistent with the requirements of 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

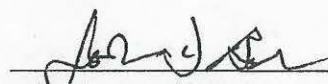
~~SECRET~~

~~SECRET~~

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

09-20-2012 P05:56

ENTERED this 28th day of September 2012, at _____ Eastern Time, in
Docket Nos. [REDACTED]


JOHN D. BATES

Judge, United States Foreign
Intelligence Surveillance Court

b(6), b(7)(C)

~~SECRET~~

Page 2