Central Intelligence Agency Minimization Procedures ~~(S)~~

7. At Tab 3 to this Notice, the Government respectfully submits a substitute first page to the CIA minimization procedures for the purpose of including the omitted word "communications" between the words "unminimized the" in the first line of the first paragraph. (U)

Respectfully submitted,

(b)(6) [redacted]

National Security Division
United States Department of Justice

Section 3 - Acquisition and Processing - General (U)

(a) Acquisition (U)

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

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

(1) Personnel shall exercise reasonable judgment in determining whether information acquired must be minimized and shall destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Inadvertently acquired communications of or concerning a United States person may be retained no longer than five years in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications. ~~(S//SI)~~

(2) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, and 6 of these procedures. ~~(C)~~

(3) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S)~~

(4) As a communication is reviewed, a determination shall be made as to whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5 and 6 of these procedures. ~~(S//SI)~~

(5) Magnetic tapes or other storage media containing communications acquired pursuant to Section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, shall not include United States person

EXHIBIT D

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

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

With respect to any unminimized communications acquired pursuant to section 702 of the Act, the FBI will apply its standard minimization procedures as described in the Standard Minimization Procedures for Electronic Surveillance of a non-U.S. Person Agent of a Foreign Power (approved September 17, 1997) and its Standard Minimization Procedures for Physical Search of a non-U.S. Person Agent of a Foreign Power (approved January 20, 1995) ("non-U.S. Person Standard Minimization Procedures"), as amended by the Amendment to the FBI's Standard Minimization Procedures for Electronic Surveillance and Physical Search (approved September 29, 2006), with the following modifications: (S)

a. References to "non-United States person agent of a foreign power" shall be understood to refer to non-United States persons reasonably believed to be located outside the United States. (U)

b. In determining whether an individual is a non-United States person, the following presumptions apply: (S//NF)

   1. If an individual is known or believed to be located outside the United States, he or she should be presumed to be a non-United States person unless the individual is identified as a United States person or circumstances give rise to the reasonable belief that the individual is a Unites States person. ~~(S//NF)~~

   2 (b)(1); (b)(3); (b)(7)(E) [redacted]

c. Any communication acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States but is in fact located inside the United States at the time such communication is acquired or is subsequently determined to be a United States person shall be removed from FBI systems upon recognition, unless the Director of the FBI determines that such communication is reasonably believed to contain significant foreign intelligence information, evidence of a crime that has been, is being, or is

EXHIBIT E

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

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

1. As used herein, the terms "Attorney General," "foreign power," "agent of a foreign power," "United States person," "person," "foreign intelligence information," "international terrorism," and "sabotage" have the meanings specified in sections 101 and 701 of the Act. (U)

2. Information about a United States person may be retained within CIA and disseminated to authorized recipients outside of CIA if the identity of the United States person and all personally identifiable information are deleted. A generic term may be substituted which does not identify the United States person in the context of the message. If the information cannot be sanitized in such a fashion because the identity is necessary, or it is reasonably believed that it may become necessary, to understand or assess the information, that identity may be retained or disseminated outside of CIA along with the information if:

   a. The information is foreign intelligence information. Such information includes, but is not limited to, information falling within one or more of the following categories:

      (1) the information indicates that the United States person has acted or may be acting as an agent of a foreign power, including information indicating that a United States person was in contact with a foreign power under facts and circumstances indicating that he intends to collaborate with a foreign power or become an agent of a foreign power;

      (2) the information indicates that a United States person may be a target of intelligence activities of a foreign power;

      (3) the information indicates that a United States person has engaged or may be engaging in the unauthorized disclosure of properly classified national security information; or

~~CL BY: 2293198~~
~~CL REASON: 1.4(c)~~
~~DECL ON: 20330730~~
~~DRV FROM: COL S-06~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE DNI/AG CERTIFICATION [redacted].	Docket Number 702(i)-08-01

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the "certification submitted in accordance with [50 U.S.C. § 1881a(g)] contains all the required elements and that the targeting and minimization procedures adopted in accordance with [50 U.S.C. § 1881a(d)-(e)] are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States."

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

ENTERED this 4th day of September, 2008, in Docket No. 702(i)-08-01.

Mary A. McLaughlin

MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE DNI/AG CERTIFICATION [redacted]	)	Docket Number 702(i)-08-01

MEMORANDUM OPINION

This matter is before the Court on the "Government's Ex Parte Submission of Replacement Certification and Related Procedures and Request for an Order Approving Such Certification and Procedures," filed on August 5, 2008 ("Ex Parte Submission"). For the reasons stated below, the government's request for approval is granted.

I. BACKGROUND

A. Section 702 of the Foreign Intelligence Surveillance Act

The government filed the Ex Parte Submission pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which was enacted as part of the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (Jul. 10, 2008) ("FAA"), and is now codified at 50 U.S.C. § 1881a. Subsection (a) of Section 702 permits the government to authorize, "for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). The implementation of any authorization under Section 702 must conform to the

limitations enumerated in subsection (b), which provides that "[a]n acquisition authorized under subsection (a)":

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

50 U.S.C. § 1881a(b).

Absent exigent circumstances, before implementing any authorization under Section 702, the Attorney General and the Director of National Intelligence ("DNI") must provide the Foreign Intelligence Surveillance Court ("FISC") with a written certification, accompanied by targeting and minimization procedures, and must obtain the Court's approval of the certification and the procedures. Id. §§ 1881a(a), (g), and (i). In the certification, the Attorney General and DNI must attest that:

> (1) there are procedures in place that are "reasonably designed" to "ensure that an acquisition authorized under subsection (a) 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";

(2) "the minimization procedures to be used with respect to such an acquisition . . . meet the definition of minimization procedures under [50 U.S.C. § 1801(h) or § 1821(4)], as appropriate" and either "have been approved, have been submitted for approval, or will be submitted with the certification for approval by the [FISC]";

(3) the Attorney General and DNI have adopted "guidelines . . . to ensure compliance with the limitations in subsection (b) [of Section 702] and to ensure that an application for a court order is filed as required by [FISA]";

(4) the targeting procedures, minimization procedures, and guidelines adopted by the government "are consistent with the Fourth Amendment";

(5) "a significant purpose of the acquisition is to obtain foreign intelligence information";

(6) "the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communications service provider"; and

(7) "the acquisition complies with the limitations in subsection (b)."

50 U.S.C. § 1881a(g)(2)(A).

The certification must be accompanied by targeting and minimization procedures adopted pursuant to Section 702(d) and (e), respectively, and it must "be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is . . . appointed by the President, by and with the advice and consent of the Senate," or " the head of an element of the intelligence community." 50 U.S.C. §§ 1881a(g)(2)(B) and (g)(2)(C). Additionally, Section 702, as applicable here, requires that the certification include "an effective date for the authorization that is at least 30 days after the submission of the written certification to the court." Id. § 1881a(g)(2)(D)(i).

B. Judicial Review

The FAA provides the FISC with jurisdiction to review the certification, the targeting and minimization procedures, and any amendments to those procedures. 50 U.S.C. § 1881a(i)(1)(A). That review, however, is limited. The FISC's role with respect to the certification is merely to "determine whether [it] contains all the required elements." Id. § 1881a(i)(2)(A). The Court reviews the targeting procedures to "assess whether the procedures are reasonably designed to – (i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (ii) 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." Id. § 1881a(i)(2)(B). As for the minimization procedures, the Court must "assess whether such procedures meet the definition of minimization procedures under [50 U.S.C. § 1801(h) or § 1821(4)], as appropriate." Id. § 1881a(i)(2)(C).

Section 702 requires the FISC to enter an order approving the certification and the use of the targeting and minimization procedures if the Court finds that the certification contains all the required elements, and that the targeting and minimization procedures are consistent with the requirements of 50 U.S.C. §§ 1881a(d)(1) and (e)(2) and with the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A). Should the Court conclude that it cannot make those findings, it must direct the government either to correct any deficiency or to refrain from implementing the authorization for which the certification was submitted. Id. § 1881a(i)(3)(B). Any order entered under Section 702 must be accompanied by "a written statement of reasons for the order." Id. § 1881a(i)(3)(C). The FISC must complete its review and issue an order not later than 30 days after the government's

submission of its certification and procedures, unless the Court "extends that time as necessary for good cause in a manner consistent with national security." Id. § 1881a(i)(1)(B), (j)(2).

C. The Government's Ex Parte Submission

The government's Ex Parte Submission includes "DNI/AG 702(g) Certification [redacted]" which was executed by the Attorney General and the DNI on [redacted] 2008, and which authorizes the targeting of certain non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information (the "Certification"). Accompanying the Certification are the supporting affidavits of the Directors of the National Security Agency ("NSA"), the Central Intelligence Agency ("CIA"), and the Federal Bureau of Investigation ("FBI"). Also included in the government's Ex Parte Submission are two sets of targeting procedures (one set to be used by the NSA and the other by the FBI), and three sets of minimization procedures (one set each for the NSA, the FBI, and the CIA).

Following the Court's preliminary review of the Ex Parte Submission, the FISC staff met with counsel for the government to communicate the Court's questions regarding the proposed targeting and minimization procedures. Thereafter, on August 26, 2008, the government submitted its "Preliminary Responses to Certain Questions Posed by the Court" ("Govt. Responses"). On August 27, the Court held a hearing during which the government answered additional questions and provided additional information about the scope and meaning of the proposed procedures. Following the hearing, the government made two supplemental submissions addressing, among other things, an issue of law it raised with the Court shortly before the hearing. The government has also submitted a copy of the guidelines adopted by the Attorney General and the DNI for ensuring

compliance with the limitations set forth in 50 U.S.C. § 1881a(b).[1] This Memorandum Opinion relies on the entire record before the Court, including each of the above-referenced submissions and information received at the August 27 hearing.

II. ANALYSIS

A. The Certifications Contain All the Required Elements.

The Court is required to review the Certification "to determine whether [it] contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). After examining the Certification, the Court finds that:

> (1) it has been made under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), Certification ("Cert.") at 4-5;
>
> (2) it contains each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A) and enumerated at pages 2-3 supra, Cert. at 1-2;
>
> (3) as required by 50 U.S.C. § 1881a(g)(2)(B), it is accompanied by the applicable targeting procedures[2] and minimization procedures;[3]

---

[1] The Ex Parte Submission and accompanying materials provided by the government consist largely of classified information. At the government's request, the Court has conducted its review ex parte and in camera. See 50 U.S.C. § 1881a(k)(2).

[2] See Procedures Used by the NSA for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended ("NSA Targeting Procedures") (attached to the Certification as Exhibit A); Procedures Used by the FBI for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended ("FBI Targeting Procedures") (attached as Exhibit C).

[3] See Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended ("NSA

(continued...)

(4) it is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);[4] and

(5) it includes an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D). Cert. at 3.[5]

Accordingly, the Court finds that the Certification "contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A).

B. The Targeting Procedures and the Minimization Procedures Are Consistent With the Applicable Statutory Requirements

With respect to the targeting procedures and minimization procedures, the Court is required to assess whether they conform to the applicable statutory requirements. 50 U.S.C. § 1881a(i)(3)(A).

1. The Targeting Procedures Satisfy the Requirements of Section 1881a(d)(1).

The government has submitted two sets of targeting procedures, one for use by the NSA and one for use by the FBI. Each set of procedures is discussed in turn.

---

[3](...continued)
Minimization Procedures") (attached as Exhibit B); Minimization Procedures Used by the FBI in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended ("FBI Minimization Procedures") (attached as Exhibit D); Minimization Procedures Used by the CIA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended ("CIA Minimization Procedures") (attached as Exhibit E).

[4] See Affidavit of Lt. Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached at Tab 1); Affidavit of Robert S. Mueller, III, Director, FBI (attached at Tab 2); Affidavit of Michael V. Hayden, Director, CIA (attached at Tab 3).

[5] The statement described in 50 U.S.C. § 1881a(g)(E) is not required in this case because there has been no "exigent circumstances" determination under Section 1881a(c)(2).

a. Overview of the NSA Targeting Procedures

NSA seeks to acquire foreign intelligence information from communications that are to, from, or about a targeted person. NSA Targeting Procedures at 2; Transcript of Proceedings on August 27, 2008 ("Trans.") at 19-22. It does so by tasking for acquisition a telephone number or electronic communications account (generically referred to as "selectors") believed to be used by a targeted person. NSA Targeting Procedures at 3; Trans. at 24.

(i) Pre-Targeting Determination

NSA is required to determine "whether a person is a non-United States person[6] reasonably believed to be outside the United States" before that person is targeted for acquisition. NSA Targeting Procedures at 1. NSA makes this determination "in light of the totality of the circumstances based on the information available with respect to that person, including [redacted]

[redacted]

For every such determination, NSA analysts must [redacted]

[redacted]

[6] "United States person" (hereinafter "U.S. person") is defined as

> a citizen of the United States, an alien lawfully admitted for permanent residence . . ., an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)].

50 U.S.C. §§ 1801(i) and 1881(a).

[redacted]

NSA analysts examine the same categories of information, in the manner described above, in assessing whether the proposed target is a non-U.S. person. NSA Targeting Procedures at 1. In addition, prior to each tasking, NSA [redacted] in order to "ascertain whether NSA has

---

[7] Although the government "reserve[d] the right to supplement and/or modify these responses" at the August 27, 2008 hearing, Govt. Responses at 1, nothing at the hearing detracted from the responses cited herein.

[8] [redacted]

reason to believe" that the proposed selector is being used by a U.S. person. Id. at 4. This step is taken to avoid targeting United States persons. See id.

NSA may avail itself of the following presumption regarding the nationality of a proposed target:

[redacted]

Id. NSA invokes the presumption only after analysts have exercised "due diligence" in attempting to ascertain the person's location under the NSA Targeting Procedures. Trans. at 5-6. Moreover, even in cases where "the actual location of the target may be unknown, [redacted]

[redacted]

(ii) Post-Targeting Analysis

NSA is also required to conduct post-targeting analysis "to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States" and to "enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States." NSA Targeting Procedures at 6. In the event that NSA concludes that a target is

within the United States, or "that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person," it will "terminate the acquisition without delay" and report the incident to the Department of Justice and the Office of the DNI. Id. at 9. [redacted]

[redacted]

This post-targeting analysis includes "routinely" comparing each selector [redacted] for indications that a tasked selector may be used inside the United States. Id. at 6-7; Govt. Responses at 7. NSA reviews the results of these comparisons [redacted] Govt. Responses at 7.

The post-targeting analysis also includes examination of the content of communications obtained through surveillance of a tasked selector for indications that a targeted person is now in, or may enter, the United States. NSA Targeting Procedures at 6-7. There is no set schedule for this form of analysis, and its timing can depend on the intelligence priorities attached to a particular target. Govt. Responses at 7-8; Trans. at 8. At the outermost limit, the analyst responsible for a particular tasking is required to conduct an annual review of the target, though in practice such reviews usually occur more frequently. Trans. at 8, 46.[9]

[9] See also 50 U.S.C. § 1881a(l)(3)(A) (requiring annual review of acquisition "to determine whether there is reason to believe that foreign intelligence information has been or will be obtained").

(iii) Documentation and Oversight

At the time of targeting, analysts are required to "document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the United States." NSA Targeting Procedures at 8.[10] This documentation facilitates later oversight of how the procedures are implemented. Internally, NSA oversight personnel "conduct periodic spot checks of targeting decisions." NSA Targeting Procedures at 8. In addition, personnel from the Department of Justice and the Office of the DNI conduct reviews of NSA's implementation of its targeting procedures "at least once every sixty days." Id. NSA is also obligated within seven days to report to the Department of Justice and the Office of the DNI "any incidents of noncompliance" resulting in "the intentional targeting of a person reasonably believed to be located in the United States or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States." Id. at 8-9. NSA similarly will report any incident of intentionally targeting a U.S. person. Govt. Responses at 8. "Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases." NSA Targeting Procedures at 9.

---

[10] There is no requirement to record the basis for the reasonable belief that the target is not a U.S. person. However, the cited sources regarding the target's location, in conjunction with a [redacted] will often provide the grounds for reasonably presuming or concluding that the target is not a U.S. person. See Govt. Responses at 8.

(iv) Emergency Departure

The NSA Targeting Procedures contain the following emergency provision:

> If, in order to protect against an immediate threat to national security, the NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and [the DNI], NSA may take such action and will report that activity promptly to [the Department of Justice and the Office of the DNI]. Under such circumstances, the Government will continue to adhere to all of the statutory limitations set forth in subsection 702(b) of [FISA].

Id. at 10 (emphasis added). The government expects that this departure provision will be invoked only under "very extreme circumstances," Trans. at 17-18, and in fact is not likely to be used at all. Id. at 19.[11] If it should be used, the government anticipates that such use would involve a relaxation of documentation requirements if [redacted] is unavailable at the time of the emergency, or a modification of the schedule for oversight reviews in the event that personnel must be redeployed to respond to the emergency. Id. at 18.

b. The NSA Targeting Procedures Comply With 50 U.S.C. § 1881a(d)(1) and Are Reasonably Designed to Prevent the Targeting of U.S. Persons.

Section 1881a(d)(1) requires:

> targeting procedures that are reasonably designed to –
>
> > (A) ensure that any acquisition . . . is limited to targeting persons reasonably believed to be outside of the United States; and

---

[11] A similar provision was included in the NSA procedures previously adopted for acquisitions under the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 15, 2007). See In re DNI/AG 105B Certifications [redacted] Memorandum Opinion and Order entered January 15, 2008, at 22. That provision has never been implemented. Trans. at 18.

> (B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.

50 U.S.C. § 1881a(d)(1).

Section 1881a(d)(1) does not, by its terms, require that the targeting procedures seek to prevent the targeting of United States persons, as distinct from persons located in the United States. Nonetheless, another provision of the statute states that, pursuant to Section 1881a,[12] the government "may not intentionally target any person known at the time of acquisition to be located in the United States," and also "may not intentionally target a United States person reasonably believed to be located outside the United States." See 50 U.S.C. § 1881a(b)(1) and (b)(3) (emphasis added). Moreover, as discussed above, see pages 8-11 supra, the targeting procedures adopted under Section 1881a(d) require government analysts to assess whether a proposed target reasonably appears to be a U.S. person, as part of the same process whereby they ascertain whether a proposed target reasonably appears to be located outside the United States. Because the limiting of acquisitions to non-U.S. person targets is important to the Court's Fourth Amendment analysis, see pages 33-34, 37-38 infra, the Court will also assess how the NSA Targeting Procedures apply to determinations of U.S. person.

In assessing the NSA Targeting Procedures, it is useful to consider separately the acquisition of communications that are to or from a tasked selector ("to/from communications"), and the

---

[12] Other sections of FISA provide separate means of authorizing electronic surveillance and physical search of targets in the United States, see 50 U.S.C. §§ 1804-1805, 1823-1824, and of targeting U.S. persons outside the United States. See id. §§ 1881b-1881c.

acquisition of communications that contain a reference to a tasked selector ("about communications").

(i) To/From Communications

For communications that are to or from a tasked selector, targeting procedures will satisfy both prongs of Section 1881a(d)(1) if they are reasonably designed to ensure that the users of tasked selectors are reasonably believed to be outside the United States. For purposes of Section 1881a(d)(1)(A), the persons targeted by acquisition of to/from communications are the users of the tasked selectors: their communications are intentionally selected for acquisition, whereas the communications of other persons are incidentally obtained only when they are communicating with the users of tasked selectors. And because a user of a tasked selector is a party to every to/from communication acquired by NSA, a reasonable belief that the users of tasked selectors are outside the United States will ensure that NSA does not intentionally acquire any to/from communication "as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1)(B).

The Court finds that the NSA Targeting Procedures are reasonably designed to ensure that the users of tasked selectors are reasonably believed to be outside the United States. Analysts are required in every case to consider [redacted] in assessing the target's location. They are also trained to review [redacted] Prior to targeting, an NSA analyst must form a reasonable belief that the user of a proposed selector is outside the United States. The basis for that belief is reviewed by a second analyst prior to tasking.

After targeting, additional analysis is conducted to ascertain whether the user may later be present in the United States. [redacted] Moreover, analysts' implementation of these procedures is subject to regular review and evaluation by NSA, the Department of Justice, and the Office of the DNI.

Finally, the provision permitting NSA to depart from these procedures temporarily to respond to an emergency is, as explained by the government, sufficiently narrow in scope that it does not undermine the Court's general assessment of reasonableness.

NSA's record of implementation of comparable procedures for acquisitions under the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 15, 2007) ("PAA"), supports this conclusion. With over [redacted] targeting decisions made, Trans. at 43, only [redacted] instances of improper targeting had been identified through May 9, 2008. Id. at 13. Most instances of non-compliance have involved inadequate documentation or delayed reporting, rather than improper targeting decisions. Id. at 11, 13-14.

The Court further finds, as a predicate of its Fourth Amendment analysis, see pages 32-41 infra, that the NSA Targeting Procedures are also reasonably designed to ensure that the users of tasked selectors, i.e., the targets of acquisition for to/from communications, are reasonably believed to be non-U.S. persons. NSA analysts perform the same steps in assessing the U.S. person status of the prospective target as they do in assessing location, as well as an additional pre-tasking step to ascertain whether the proposed selector is known to be used by a U.S. person. Moreover, as explained by the government, the presumption of non-U.S. person status that NSA may make based

on the overseas location of the target, see page 10 supra, logically follows from the proposition, previously accepted by the FISC, "that the vast majority of persons who are located overseas are not United States persons and that most of their communications are with other, non-United States persons, who are also located overseas." In re Directives, Docket No. 105B(g): 07-01, Memorandum Opinion entered April 25, 2008, at 87 (footnote omitted), aff'd, Docket No. 08-01 (FISA Ct. Rev. Aug. 22, 2008).[13]

(ii) About Communications

For tasked electronic communications accounts, the NSA also acquires communications that contain a reference to the name of the tasked account.[14] The government asserts that, for purposes

---

[13] The minimization procedures contain similar presumptions regarding non-U.S. person status, see NSA Minimization Procedures at 2; FBI Minimization Procedures at 1, which the Court finds reasonable on the understanding that they will be applied in the manner described for the presumption in the NSA Targeting Procedures.

[14] These about communications fall into [redacted] categories first described to the FISC in prior proceedings. Trans. at 40-41. Those categories are as follows (for ease of reference, the tasked account is called "tasked@email.com"):

[redacted]

of Section 1881a(d)(1)(A), the person being "targeted" by such an acquisition is the user of the tasked account, not other persons who are parties to the acquired communication.[15] Govt. Responses at 3; Trans. at 24. The Court accepts this conclusion. It is natural to regard the user of the tasked account as the "target" of the acquisition, because the government's purpose in acquiring about communications is to obtain information about that user. Trans. at 24.[16] The communication is not acquired because the government has any interest in the parties to the communication, other than their potential relationship to the user of the tasked account; indeed, the government may have

---

See In re DNI/AG 105B Certifications Memorandum Opinion and Order entered January 15, 2008, at 17 n.18.

[15] In some cases the user of the tasked account may also be a party to an acquired about communication; for example, Trans. at 20.

[16] For purposes of FISA surveillances conducted under 50 U.S.C. §§ 1804-1805, the "target" of the surveillance "'is the individual or entity . . . about whom or from whom information is sought.'" In re Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, at 73 (1978)). There is no reason to think that a different meaning should apply here.

no knowledge of those parties prior to acquisition. See id. at 19-20. And parties to an acquired about communication do not become targets of acquisition unless and until they are separately vetted under the NSA Targeting Procedures and a selector used by them is separately tasked. Id. at 26-27. Of course, anyone assessed to be a U.S. person or to be inside the United States cannot be targeted at all. See pages 8-11 supra.

Having concluded that this mode of acquisition targets the users of tasked selectors, and that the NSA Targeting Procedures are reasonably designed to ensure that the users of tasked selectors are reasonably believed to be outside the United States, see pages 15-16 supra, the Court finds that the NSA Targeting Procedures satisfy Section 1881a(d)(1)(A). Similarly, based on the discussion at pages 16-17 supra, the Court finds that the NSA Targeting Procedures are reasonably designed to prevent the targeting of U.S. persons in the acquisition of about communications.

A separate analysis is required of whether, in conformance with Section 1881a(d)(1)(B), the NSA Targeting Procedures are reasonably designed to prevent the intentional acquisition of about communications "as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." For each acquisition of an about communication, NSA relies on [redacted] means of ensuring that at least one party to the communication is outside the United States: "NSA will [redacted] employ an Internet Protocol filter to ensure" that at least one party to a communication is outside the United States [redacted] NSA Targeting Procedures at 2.

The Court finds that these measures are reasonably designed to prevent the intentional acquisition of communications as to which all parties are in the United States.[17]

c. The FBI Targeting Procedures

In addition to NSA, the FBI may also conduct acquisitions under the certification, in conformance with the FBI Targeting Procedures. The FBI will apply its procedures "in acquiring foreign intelligence information, in the form of [redacted]" by targeting electronic communications accounts "designated by the [NSA]." FBI Targeting Procedures at 1. Prior to requesting the FBI to [redacted] for an account, NSA will have followed its own targeting procedures in determining that the user of the account "is a person reasonably believed to be located outside of the United States and is not a United States person." Id. Thus, the FBI Targeting Procedures apply in addition to the NSA Targeting Procedures, whenever [redacted] are acquired.

Because the FBI is only involved in the acquisition of to/from communications, Trans. at 32, the FBI Targeting Procedures will satisfy Section 1881a(d)(1) if they are reasonably designed to ensure that the users of tasked selectors are reasonably believed to be outside of the United States. See page 15 supra. Because the Court has found that the NSA Targeting Procedures meet this

---

[17] The government has represented that these measures have prevented the acquisition of wholly domestic communications under the PAA. Trans. at 28; Govt. Responses at 5. With regard to Internet Protocol (IP) filters, the Court understands that [redacted] Trans. at 28-29. Although it is theoretically possible that a wholly domestic communication could be acquired as a result of [redacted] NSA is not aware of this actually happening. Id. at 29-31.

standard, see pages 15-16 supra, and also are reasonably designed to prevent the targeting of U.S. persons, see pages 16-17 supra, it should readily follow that the FBI Targeting Procedures, which provide additional assurance that users of tasked accounts are non-U.S. persons located outside the United States,[18] also pass muster. The Court has reviewed the FBI Targeting Procedures and found that they satisfy these criteria also.

2. The Government's Minimization Procedures Satisfy 50 U.S.C. § 1881a(e)(1).

Section 1881a(e)(1) requires the government to "adopt minimization procedures that meet the definition of minimization procedures" under 50 U.S.C. § 1801(h) or §1821(4), "as appropriate." Those definitions are substantively identical for purposes of this case,[19] and define "minimization procedures" 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

---

[18] [redacted]

[19] They differ only in referring to electronic surveillance (§ 1801(h)) or physical search (§ 1821(4)), and to the procedure for emergency approval for those respective modes of collection in a context that does not apply to this case.

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;[20]

(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).

---

[20] "Foreign intelligence information" is defined as

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

50 U.S.C. §§ 1801(e) and 1881(a).

In this case, there are three sets of minimization procedures that have been adopted by the Attorney General: a set of procedures for each of the two agencies that will conduct acquisitions, the NSA and the FBI, and a third set of procedures for the CIA, which may receive from those agencies the raw data from acquisitions. NSA Minimization Procedures at 8; FBI Minimization Procedures at 2. Each of these sets of procedures closely resembles minimization procedures that have been found by judges of this Court to meet the definition of minimization procedures under section 1801(h) in the context of cases that have a significantly greater likelihood of acquiring communications to, from, or about United States persons. See, e.g., Docket Nos [redacted] (In re Various Known and Unknown Agents of [redacted] (In re [redacted] (b)(1); (b)(3); (b)(7)(A); (b)(7)(E) [redacted] and [redacted] (In re [redacted] (b)(1); (b)(3); (b)(7)(A) [redacted]).

The targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that U.S. person information will be obtained. See page 17 supra. Yet, the protection to U.S. persons afforded by the proposed minimization procedures nearly replicates the protection afforded such persons in cases involving search or surveillance intentionally targeting U.S. persons. Procedures that have been found to be reasonably designed for the purpose of surveillance targeting U.S. persons should be reasonable for the acquisition of communications targeting non-U.S. persons abroad. The Court's review of the minimization procedures confirms that they are reasonable in the context of this case.

Although the procedures proposed by the government are not identical to these previously approved procedures, the differences, as discussed below, do not undermine a finding that they meet

the definition of minimization procedures under the statute. Therefore, for the reasons stated below, the Court finds that each set of minimization procedures is reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, of private U.S. person information, consistent with the foreign intelligence needs of the government, and otherwise conforms to the statutory definition.

a. Cross-cutting Issues

Some issues worthy of discussion are presented by more than one agency's minimization procedures.[21]

(i) Special Retention Provisions

All three sets of minimization procedures permit the head of the agency, under certain circumstances, to authorize retention of information from communications acquired when the government reasonably believed that the target was a non-U.S. person outside the United States, when in fact the target was a U.S. person or was inside the United States.[22] For example, the CIA Minimization Procedures state:

> Any communication . . . acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside

---

[21] The NSA and FBI minimization procedures include presumptions of non-U.S. person status based on a person's location outside the United States. NSA Minimization Procedures at 2; FBI Minimization Procedures at 1. The Court understands that those presumptions apply in the same manner as the analogous presumption in the NSA Targeting Procedures, which is discussed above. See page 10 supra. On that understanding, the Court finds that the minimization presumptions comport with the statutory definitions.

[22] For purposes of applying the NSA Minimization Procedures, such communications are treated as "domestic communications." NSA Minimization Procedures at 4.

> the United States but is in fact located inside the United States at the time such communication is acquired or was in fact a United States person at the time of targeting shall be destroyed unless the Director of the [CIA] determines in writing that such communication is reasonably believed to contain: significant foreign intelligence information; evidence of a crime that has been, is being, or is about to be committed; or information retained for cryptanalytic, traffic analytic, or signal exploitation purposes.

CIA Minimization Procedures at 6.[23] In addition to these categories of information, the Director of NSA may also authorize retention upon a finding that "the communication contains information pertaining to a threat of serious harm to life or property" or "information necessary to understand or assess a communications security vulnerability." NSA Minimization Procedures at 5-6.

For ease of reference, the Court will refer to these provisions collectively as "special retention provisions."[24] For the following reasons, the Court finds that the special retention provisions are reasonable and consistent with the statutory definition of minimization procedures.

First, the Court concludes that the government is authorized to acquire communications when it has a reasonable, but mistaken, belief that the target is a non-U.S. person located outside the United States. The Certification authorizes "the targeting of non-United States persons reasonably believed to be located outside the United States" in accordance with the targeting procedures. Cert. at 3; see also 50 U.S.C. § 1881a(a) ("the Attorney General and the [DNI] may

---

[23] Corresponding provisions are in the FBI Minimization Procedures at 1-2 and the NSA Minimization Procedures at 5-6.

[24] Although the agencies' special retention provisions use somewhat different language to describe the form of approval, the government has explained that, for all three agencies, the agency head will make such determinations in writing on a case-by-case basis. Govt. Responses at 11; Trans. at 36-37.

authorize jointly . . . the targeting of persons reasonably believed to be outside the United States"). There may be cases where, after properly applying the targeting procedures, the government reasonably believes at the time it acquires a communication that the target is a non-U.S. person outside the United States, when in fact the target is a U.S. person and/or is in the United States. The acquisition of such communications is properly authorized under Section 1881a, notwithstanding the fact that the government is prohibited from intentionally targeting U.S. persons or any persons inside the United States, or intentionally acquiring a communication when it is known that all parties thereto are inside the United States.[25]

The Court also finds that 50 U.S.C. § 1806(i) does not require the destruction of information from such communications. Section 1806(i) provides that, in the case of

> the unintentional acquisition . . . of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

---

[25] The government may not: (1) "intentionally target" any person "known at the time of acquisition to be located in the United States;" "intentionally target a United States person," even if such person is "reasonably believed to be located outside the United States;" or (3) "intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(b)(1), (3), and (4) (emphasis added). "Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases." NSA Targeting Procedures at 9.

50 U.S.C. § 1806(i) (emphasis added).[26] The government argues that, by its terms, Section 1806(i) applies only to a communication that is unintentionally acquired,[27] not to a communication that is intentionally acquired under a mistaken belief about the location or non-U.S. person status of the target or the location of the parties to the communication. See Government's filing of August 28, 2008. The Court finds this analysis of Section 1806(i) persuasive, and on this basis concludes that Section 1806(i) does not require the destruction of the types of communications that are addressed by the special retention provisions.[28]

Having concluded that such communications are within the scope of authorized acquisition, and that Section 1806(i) does not apply to such communications, the only remaining question is whether the special retention provisions comport with the statutory definition of minimization procedures. The Court concludes that they do. Once an agency head has made a case-specific, written determination that certain information falls within one of the categories specified in the

---

[26] Prior to the FAA, this subsection had only applied to radio communications. See FAA § 106, 122 Stat. 2462 (replacing "radio communication" with "communication" in this subsection).

[27] A communication would be unintentionally acquired, for purposes of Section 1806(i), if, for example, the acquisition resulted from a technical malfunction or an inadvertent mis-identification of a selector.

[28] In approving other minimization and targeting provisions that refer to "inadvertently" acquired communications, the Court relies on the government's representations that those provisions will be implemented in accordance with the explanations provided in the government's Notice of Clarification and Correction, filed September 2, 2008. So understood, those provisions of the minimization procedures do not implicate Section 1806(i).

special retention provisions, continued retention and appropriate dissemination of such information do not conflict with the requirements of Sections 1801(h) and 1821(4).[29]

(ii) Technical and Linguistic Assistance from Foreign Governments

The NSA and CIA minimization procedures provide for the sharing of raw data with foreign governments for "technical and linguistic assistance." NSA Minimization Procedures at 8-10 (permitting such sharing [redacted]; CIA Minimization Procedures at 4-5 (permitting such sharing with foreign governments generally).[30] Access to this raw information is restricted to foreign government personnel involved in rendering the necessary assistance to NSA or CIA, and the foreign government may not permanently retain or otherwise make use of information so received. NSA Minimization Procedures at 9-10; CIA Minimization Procedures at 4-5. Given these tight restrictions, the FISC

---

[29] Specifically, evidence of a crime may be retained and disseminated for law enforcement purposes under Sections 1801(h)(3) and 1821(4)(C). "[S]ignificant foreign intelligence information" may be retained and, as appropriate, disseminated under Sections 1801(h)(1)-(2) and 1821(4)(A)-(B). "[I]nformation retained for cryptanalytic, traffic analytic, or signal exploitation purposes" – which NSA refers to as "technical data base" information, see NSA Minimization Procedures at 2 – may not, once fully processed, be identified as foreign intelligence information, but the Court is satisfied that retention of information for such purposes, and subject to other minimization requirements, is permissible as "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1) and 1821(4)(A). Finally, in the context of acquisitions under this Certification, "information pertaining to a threat of serious harm to life or property" and "information necessary to understand or assess a communications security vulnerability" can reasonably be regarded as information to be retained under the above-quoted provisions of Sections 1801(h)(1) and 1821(4)(A).

[30] Previously, the FISC has authorized disseminations of raw FISA information to foreign governments on a more limited basis. See, e.g., Docket No. [redacted] Order [redacted].

finds that such information-sharing comports with the requirements of Sections 1801(h) and 1821(4).

b. NSA Minimization Procedures

The NSA Minimization Procedures in this matter are substantially similar to other sets of minimization procedures employed by NSA in the conduct of electronic surveillance in other contexts. The procedures proposed herein borrow from four sets of procedures: (1) the NSA Standard Minimization Procedures adopted by the Attorney General for use in nearly all NSA requests for electronic surveillance sought pursuant to Section 1804 and authorized by judges of this Court in accordance with Section 1805 ("SMP"); (2) the procedures adopted by this Court in In re Electronic Surveillance and Physical Search of International Terrorist Groups, Their Agents, and Related Targets, Order, No. [redacted] (May 2002), as extended and modified by orders of this Court, most recently on December 6, 2007 ("Raw Take Motion"); (3) the procedures proposed by the government and approved by several judges of this Court in several dockets captioned, In re Various Known and Unknown Agents of [redacted] most recently in Docket [redacted] "Domestic Selector Procedures"); and (4) the procedures adopted by the government for use in acquisitions authorized pursuant to the PAA ("PAA Procedures").[31]

[31] Unlike the other sets of minimization procedures, the PAA Procedures have never been presented to a judge of the FISC for a determination as to whether they meet the definition of minimization procedures in Section 1801(h). However, a judge of this Court considered the minimization procedures as a factor that supported finding that certain directives issued in accordance with DNI/AG Certifications satisfied the reasonableness requirement of the Fourth (continued...)

Prior to now, any deviation from the SMP was made by asking the Court to adopt the SMP with specified modifications. Thus, to assess such minimization procedures, a judge needed to review the SMP as well as the proposed modification. The NSA Minimization Procedures in this matter, however, are drafted as a stand alone set of procedures, complete unto themselves. Notwithstanding the changed verbiage, the NSA Minimization Procedures at issue here are substantially the same as the Domestic Selector Procedures and the PAA Procedures.[32] The most significant difference involves the special retention provisions discussed at pages 24-28 supra.

Other differences appear to be of less moment. The NSA Minimization Procedures at issue here adopt the previously approved five-year period of retention for "inadvertently acquired information," i.e., information acquired "notwithstanding reasonable steps taken to minimize the acquisition of information not relevant to the authorized purpose of the acquisition." Government's submission of September 2, 2008, at 4 (internal quotations omitted).[33] The NSA Minimization Procedures at issue here, however, extend the period of time for which NSA may retain technical

---

[31](...continued)
Amendment. In re Directives, Docket No. 105B(g): 07-01, Memorandum Opinion entered April 25, 2008, at 88-89, 94.

[32] For example, it is the Court's understanding that Section 3(b)(1) of the NSA Minimization Procedures at issue here is meant to convey the same meaning as Section 3(c)(2) of the SMP, as modified in the Domestic Selector Procedures and the PAA Procedures to permit retention for five years.

[33] See NSA Minimization Procedures at 3 ("Inadvertently acquired communications of or concerning a United States person may be retained no longer than five years . . . ."); see also note 28 supra.

data base information from one year to five years.[34] For the reasons presented by the government, both in its written submissions and in the hearing, and consistent with the findings of other judges of the FISC, the Court finds an outside retention period of five years, even for the technical data, to be reasonable.

c. FBI Minimization Procedures

The FBI Minimization Procedures are the standard FBI minimization procedures for a non-U.S. person agent of a foreign power, subject to certain modifications. They shall be implemented in accordance with a recent FBI policy directive, FBI Minimization Procedures at 2, and in the same manner in which that policy directive applies in cases where the FBI [redacted]. Govt. Responses at 10. In many orders authorizing [redacted] the FISC has found that those standard FBI minimization procedures, implemented in conformance with that policy directive, comply with the applicable statutory definition. Nothing in the case-specific modifications to those procedures presents any additional concern.

[34] The NSA Minimization Procedures also include an additional category of technical information that may be retained for this period - information necessary to understand or assess a communications security vulnerability. NSA Minimization Procedures at 5-6.

d. CIA Minimization Procedures

The CIA Minimization Procedures are also similar in many respects to procedures previously approved by the FISC.[35] They include a new category of U.S. person information expressly authorized for retention and dissemination: information that "concerns a U.S. Government official acting in an official capacity." CIA Minimization Procedures at 2. The Court finds that this category is reasonable and complies with the statutory definition, on the understanding that CIA will disseminate this category of information, and other information disseminated pursuant to Paragraph 2 of the CIA Minimization Procedures, in a manner consistent with Section 1801(h)(2) – i.e., that nonpublicly available information that is foreign intelligence information as defined at Section 1801(e)(2) "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."

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

The Court is also charged with assessing whether the targeting procedures and minimization procedures "are consistent . . . with the fourth amendment to the Constitution of the United States." 50 U.S.C. § 1881a(i)(3)(A)-(B). The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no

---

[35] See, e.g., In Re Various Known and Unknown Agents of [redacted] Docket No. [redacted] CIA Minimization Procedures (Exhibit D to Application) (including substantively identical provisions for retention of certain categories of information (¶ 3); handling of privileged communications (¶ 4a); and dissemination of intelligence reporting to foreign governments (¶ 4c).

> Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. There is no question that the government's acquisition of private telephone calls can constitute a "search" or "seizure" within the meaning of the Fourth Amendment. See, e.g., Katz v. United States, 389 U.S. 347, 353 (1967). Although the scope of Fourth Amendment protection for email communications is not settled,[36] the Court will assume that, at least under some circumstances, the acquisition of electronic communications other than telephone calls can also result in such a "search" or "seizure."

The Court concludes that the Fourth Amendment does not require the government to obtain a warrant for acquisitions under the procedures at issue, and that the procedures are reasonable and consistent with the Fourth Amendment.

1. The Government Is Not Required to Obtain a Warrant for Acquisitions Pursuant to the Procedures in Question.

The applicable targeting procedures are reasonably designed to confine acquisitions to targeting persons reasonably believed to be outside the United States. See pages 15-21 supra. They also are reasonably designed to avoid targeting U.S. persons. See pages 16-17, 20-21 supra.

---

[36] See David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions § 7:28 (2007).

Because there is no reason to think that these procedures will be implemented in bad faith,[37] the acquisitions can generally be expected to target non-U.S. persons located outside the United States.

Under these circumstances, it can be questioned whether the Warrant Clause of the Fourth Amendment has any application at all, insofar as the targets of acquisitions under the procedures are non-U.S. persons located overseas.[38] However, to the extent that the Warrant Clause might otherwise apply, the Court concludes that acquisitions under these procedures fall within an exception to the warrant requirement recognized by the Foreign Intelligence Surveillance Court of Review in In re Directives, Docket No. 08-01, Opinion at 28 (FISA Ct. Rev. Aug. 22, 2008) (hereinafter "In re Directives"). That case, like this one, involved the warrantless acquisition of communications targeting persons reasonably believed to be outside the United States. In re Directives at 3. Unlike this case, In re Directives involved acquisitions that targeted U.S. persons reasonably believed to be outside the United States. See id. at 25-26 (discussing requirements for targeting U.S. persons). In that case, the Court of Review found that an exception to the warrant requirement applied to "surveillance undertaken for national security purposes and directed at a

---

[37] Cf. In re Directives, Docket No. 08-01, Opinion at 28 (FISA Ct. Rev. Aug. 22, 2008) ("Once we have determined that protections sufficient to meet the Fourth Amendment's reasonableness requirement are in place, there is no justification for assuming, in the absence of evidence to that effect, that those prophylactic procedures have been implemented in bad faith.").

[38] See United States v. Verdugo-Urqidez, 494 U.S. 259, 274-75 (1990) (observing that a warrant "would be a dead letter outside the United States" and holding that "the Fourth Amendment ha[d] no application" where respondent "was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico"); id. at 278 ("the Fourth Amendment's warrant requirement should not apply in Mexico as it does in this country") (Kennedy, J., concurring); id. at 279 ("I do not believe the Warrant Clause has any application to searches of noncitizens' homes in foreign jurisdictions because American magistrates have no power to authorize such searches.") (Stevens, J., concurring in the judgment).

foreign power or an agent of a foreign power reasonably believed to be located outside the United States." Id. at 15-16.[39]

The acquisitions at issue here fall within the exception recognized by the Court of Review. They target persons reasonably believed to be located outside the United States, see pages 15-21 supra, who will have been assessed by NSA to possess and/or to be likely to communicate foreign intelligence information concerning a foreign power authorized for acquisition under the Certification. Cert. at 2-3; NSA Targeting Procedures at 4; Govt. Responses at 1-3; Alexander Affidavit at 3.[40] And the acquisitions are conducted for national security purposes, i.e., with a "significant purpose . . . to obtain foreign intelligence information." Cert. at 2.

Moreover, the Court of Review's reasons for recognizing and applying a foreign intelligence exception in In re Directives apply with equal force here. First, the government's purpose in conducting the acquisitions in this case "goes well beyond any garden-variety law enforcement

---

[39] In so doing, the Court of Review analogized to cases in which the Supreme Court "excused compliance with the Warrant Clause when the purpose behind the governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose." Id. at 15 (citing, among other cases, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

[40] [redacted]

objective. It involves the acquisition from overseas foreign agents of foreign intelligence to help protect national security," a circumstance "in which the government's interest is particularly intense." In re Directives at 16.

Second, the Court of Review relied on the

> high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake. . . . Compulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government's ability to collect information in a timely manner. In some cases, that delay might well allow the window in which [redacted] or information is available to slam shut before a warrant can be secured.

Id. at 18. This case similarly involves targets who are attempting to conceal their communications, thereby presenting the same concerns that weigh against requiring the government to obtain a warrant.[41] Moreover, the government tasked over [redacted] overseas selectors for acquisition under the PAA, Trans. at 43, and it is reasonably anticipated that the government will seek to task [redacted] selectors under Section 1881a certifications. Subjecting [redacted] number of targets to a warrant process inevitably would result in delays and, at least occasionally, in failures to obtain perishable foreign intelligence information, to the detriment of the national security.

For these reasons, the Court concludes that the government is not obligated to obtain a warrant before conducting acquisitions under the procedures in question.

---

[41] Compare In re Directives at 18 (discussing [redacted]) with Trans. at 23 (noting challenge of [redacted]).

2. Acquisitions Conducted Under the Procedures in Question Are Reasonable Under the Fourth Amendment.

The Court of Review opinion in In re Directives also provides the analytical framework for analyzing reasonableness under the Fourth Amendment. A reviewing court must consider "the nature of the government intrusion and how the government intrusion is implemented. The more important the government's interest, the greater the intrusion that may be constitutionally tolerated." In re Directives at 19-20 (citations omitted). The court must

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

Id. at 20 (citations omitted).[42] In conducting this balancing test, the court must consider the totality of the circumstances, In re Directives at 19; Samson v. California, 547 U.S. 843, 848 (2006), rather than rigidly apply a set of pre-determined factors. In re Directives at 20-21; Ohio v. Robinette, 519 U.S. 33, 39 (1996).

The government's national security interest in conducting these acquisitions "is of the highest order of magnitude." Id. at 20.[43] On the other side of the balance, the targeting procedures reasonably confine acquisitions to targets who are non-U.S. persons outside the United States. Such persons are not protected by the Fourth Amendment. United States v. Verdugo-Urqidez, 494 U.S.

---

[42] Accord In re Sealed Case, 310 F.3d at 742 (describing "a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens").

[43] Accord Haig v. Agee, 453 U.S. 280, 307 (1981) (there is no governmental interest more compelling than the security of the nation).

259, 274-75 (1990). As a result, the acquisitions will intrude on interests protected by the Fourth Amendment only to the extent that (1) despite the operation of the targeting procedures, U.S. persons, or persons actually in the United States, are mistakenly targeted; or (2) U.S. persons, or persons located in the United States, are parties to communications to or from tasked selectors (or, in certain circumstances, communications that contain a reference to a tasked selector).[44] These circumstances present a real and non-trivial likelihood of intrusion on Fourth Amendment-protected interests, but they do not, by themselves, render the procedures unreasonable under the Fourth Amendment.[45] Indeed, the extent of such intrusion will be less in this context than in cases involving the intentional targeting of persons protected by the Fourth Amendment or otherwise lacking comparable targeting procedures.

Weighing the government's national security interest in conducting the acquisitions against the degree of intrusion on Fourth Amendment-protected interests, the Court finds that the procedures are reasonable under the Fourth Amendment. In addition to the targeting procedures, which limit the extent of Fourth Amendment intrusion as described above, the Court relies on the following protections in reaching this assessment.

Foreign Intelligence Assessments: Prior to conducting acquisitions for a new target, NSA assesses whether the person to be targeted "possesses and/or is likely to communicate foreign

---

[44] It is reasonable to presume that most persons in communication with a non-U.S. person target located overseas are themselves likely to be non-U.S. persons located overseas. See page 17 supra.

[45] See In re Directives, at 28 ("the fact that there is some potential for error is not a sufficient reason to invalidate the surveillances"), 30 ("incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful").

intelligence information" concerning a foreign power authorized under the Certification. NSA Targeting Procedures at 4; Cert. at 3; Alexander Affidavit at 3. In making these assessments, NSA considers several factors, [redacted]

In In re Directives, the Court of Review examined similar factors[46] and found that they were "in conformity with the particularity showing contemplated by [the Fourth Amendment reasonableness analysis in] Sealed Case." In re Directives at 24. The corresponding provisions of the NSA Targeting Procedures at issue here likewise direct the government's acquisitions toward communications that are likely to yield the foreign intelligence information sought,[47] and thereby

---

[46] A comparison of the factors identified in the NSA Targeting Procedures with those at issue in In re Directives, see FISC Docket No. 105B(g): 07-01, Classified Appendix submitted February 20, 2008, at pages [redacted] reveals that the two sets of factors are substantively identical, except for the references to the pertinent foreign powers and the inclusion of an additional factor in the NSA Targeting Procedures regarding [redacted] NSA Targeting Procedures at 6.

[47] It is fairly obvious why communications to and from targets identified under these procedures would be expected to contain foreign intelligence information. The Court has received (continued...)

afford a degree of particularity that is reasonable under the Fourth Amendment. Cf. In re Directives at 21 (rejecting suggestion that, to satisfy the Fourth Amendment, the government's procedures "must contain protections equivalent to the three principal warrant requirements: prior judicial review, probable cause, and particularity").

Minimization Procedures: As previously stated, see pages 21-32 supra, the minimization procedures used by the NSA, FBI, and CIA are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination," of U.S. person information, "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1). These procedures constitute a safeguard against improper use of information about U.S. persons that is inadvertently or incidentally acquired, and therefore contribute to the Court's overall assessment that the targeting and minimization procedures are consistent with the Fourth Amendment. See In re Directives at 29-30.

The Court recognizes that there are differences between the procedures at issue here and those at issue in In re Directives. Most prominently, in In re Directives, the government followed procedures adopted under section 2.5 of Executive Order No. 12,333, requiring the Attorney General to find probable cause to believe that a U.S. person to be targeted for acquisition was an agent or an employee of a foreign power, and limiting the duration of an authorization for a U.S. person target to 90 days. In re Directives at 25-26. In this case, the government's procedures

---

[47](...continued)
testimony that acquiring about communications enables the government to discover additional accounts used by targets, and to identify previously unknown persons who are associated with targets and may be involved in or possess information regarding targets' activities. See Trans. at 20-21.

provide for no comparable probable cause determination, presumably because U.S. persons cannot be intentionally targeted at all.

A probable cause determination by a high-level official is not an indispensable component of reasonableness in the circumstances of targeting non-U.S. persons overseas for foreign intelligence purposes. See United States v. Bin Laden, 126 F. Supp.2d 264, 281 (S.D.N.Y. 2000) (under Supreme Court decision in Verdugo, government not required to obtain a warrant or section 2.5 approval in order to conduct surveillance of non-U.S. persons' phone communications in Kenya). Where, as here, the government has "'special needs, beyond the normal need for law enforcement,'" even suspicionless searches can be reasonable under the Fourth Amendment. In re Sealed Case, 310 F.3d at 745 (quoting Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)). In this case, the NSA's assessment under its targeting procedures of the likelihood of obtaining foreign intelligence information provides a reasonable factual predicate for conducting the acquisitions, in view of the gravity of the government's national security interests and the other safeguards embodied in the targeting and minimization procedures.

III. CONCLUSION

Based on the foregoing statement of reasons and in reliance on the entire record in this matter, the Court finds, in the language of Section 1881a(i)(3)(A), that the certification "submitted in accordance with [Section 1881a(g)] contains 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 to the Constitution of the United

States." A separate order approving the certification and the use of the procedures pursuant to Section 1881a(i)(3)(A) is being entered contemporaneously herewith.

ENTERED this 4th day of September, 2008, in Docket No. 702(i)-08-01.

Mary A. McLaughlin

MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

~~SECRET//COMINT//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE ELECTRONIC SURVEILLANCE, PHYSICAL SEARCH, AND OTHER ACQUISITIONS TARGETING INTERNATIONAL TERRORIST GROUPS, THEIR AGENTS, AND RELATED TARGETS. (S)	:	Docket Numbers: [redacted]

GOVERNMENT'S SUBMISSION OF AMENDMENTS TO STANDARD MINIMIZATION PROCEDURES FOR FBI ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

AND

SUBMISSION OF REVISED MINIMIZATION PROCEDURES FOR THE NATIONAL COUNTERTERRORISM CENTER

AND

MOTION FOR AMENDED ORDERS PERMITTING USE OF AMENDED MINIMIZATION PROCEDURES

By this motion, the United States of America, through the undersigned Department of Justice (DOJ) attorney, seeks to amend previous Orders and Warrants

~~SECRET//COMINT//NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: 15 April 2037

("Orders") of this Court, as described below, to incorporate amendments, adopted by the Attorney General, to the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act (FBI SMPs), on file with this Court.[1] The amendments would permit the FBI to provide to the National Counterterrorism Center (NCTC) unminimized, or "raw," data acquired through electronic surveillance, physical search, or other acquisitions[2] authorized by this Court pursuant to the Foreign Intelligence Surveillance

---

[1] This motion seeks to amend the FBI SMPs and to replace NCTC's current minimization procedures. The scope of information FBI will share with NCTC will be the same that this Court has authorized FBI to share with the National Security Agency (NSA) and Central Intelligence Agency (CIA) in docket number [redacted]. Herein, the Government's May 10, 2002 motion in docket number [redacted] is referred to as the "Raw Take Motion." This Court's July 22, 2002 Order, as made permanent by this Court's May 19, 2004 Order and as modified, is referred to as the "Raw Take Order." The Government's Motion to make the Raw Take Order permanent, filed May 14, 2002, is referred to as the "2004 Raw Take Motion," and the Court's May 19, 2004 Order granting that motion is referred to as the "2004 Raw Take Order." ~~(S)~~

The NCTC-related amendment to the FBI SMPs replaces the current Section IV.G, which permits FBI to allow NCTC to access the Automated Case Support (ACS) data system. Section IV.E of the FBI SMPs permits FBI to provide raw FISA-acquired data to NSA and CIA as provided in docket number [redacted]. The Attorney General amendments and this motion do not seek to modify Section IV.E or docket number [redacted] except as specifically set forth herein. ~~(S//NF)~~

The Government does not seek to incorporate the amendment discussed herein, or the NCTC minimization procedures, into the Raw Take Order. Rather, the Government seeks to replace the existing FBI SMPs provision governing sharing FISA-acquired information with NCTC, and to replace NCTC's existing minimization procedures governing FISA-acquired information received from FBI. While the analysis set forth herein relies largely on this Court's opinions and orders in docket number [redacted] matters governing FBI's sharing information with NCTC have previously been docketed under docket number [redacted] captioned above. ~~(S)~~

[2] As indicated above, "FISA" and "FISA-acquired" herein do not refer to Section 702 of FISA (50 U.S.C. § 1881a). The FBI SMPs, by their terms, apply to Titles I and III of FISA (50 U.S.C. §§ 1801-1812 1821-1829). Currently, when FBI receives authorization to acquire information pursuant to Sections 704 or 705(b) of FISA (50 U.S.C. §§ 1881c, 1881d(b)), this Court orders FBI to apply the FBI SMPs to such information. Accordingly, to the extent that such authorities are governed by the FBI SMPs, the

Act, 50 U.S.C. §§ 1801-1812, 1821-1829, 1881c, 1881d(b) (FISA or the Act) (FISA-acquired information), in cases targeting: (1) foreign powers as defined at 50 U.S.C. § 1801(a)(4); (2) agents of such foreign powers; and (3) other targets when the electronic surveillance, physical search, or other acquisitions targeting such targets is reasonably expected to yield foreign intelligence information related to international terrorism (hereinafter collectively, "terrorism-related cases"). The proposed amendments also make changes to the FBI SMP provisions regarding [redacted] the retention provisions regarding attorney-client communications, non-pertinent and sensitive categories of communications, and extension of retention time limits. A clean copy of the FBI SMPs as revised is attached as Exhibit A. A copy with the changes described herein highlighted is attached as Exhibit B. ~~(S)~~

NCTC will be required to apply to raw FISA-acquired data provided by FBI the Revised NCTC Standard Minimization Procedures (NCTC SMPs), which are submitted

---

amendments to the FBI SMPs discussed herein will be incorporated into the minimization procedures governing information FBI acquires or has acquired pursuant to Sections 704 and 705(b). Therefore, the proposed revised NCTC SMPs would apply to raw information FBI provides to NCTC that FBI has acquired pursuant to Title I, Title III, Section 704, or Section 705(b) of FISA. As with the rest of the FBI SMPs, references to "electronic surveillance" and "physical search" in the amendments to the FBI SMPs include any other acquisitions conducted by FBI pursuant to Sections 704 and 705(b) that are governed by the FBI SMPs. ~~(S)~~

This motion does not seek authorization for any agency other than FBI to share information with NCTC. ~~(S)~~

with this motion as Exhibit C.[3] The Attorney General has approved the FBI SMP amendments and the NCTC SMPs, which satisfy FISA's definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) and 1821(4). ~~(S)~~

The amendment to the FBI SMPs permitting FBI to provide to NCTC data in terrorism-related cases would apply retroactively to January 1, 2001.[4] The other amendments to the FBI SMPs, discussed below, would apply retroactively in the same manner as the FBI SMPs generally. *See* Opinion and Order, *In re Electronic Surveillance and Physical Search of Foreign Powers and Agents of Foreign Powers* and *In re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Under the Foreign Intelligence Surveillance Act*, Docket Nos. Multiple and [redacted] (Oct. 31, 2008).

---

[3] The minimization procedures currently governing NCTC access to FBI systems, which were filed on October 2, 2008, will be superseded by the Revised NCTC SMPs submitted with this motion. The Revised NCTC SMPs are referred to as the NCTC SMPs herein. The October 2, 2008 procedures are referred to as the ACS Procedures herein. ~~(S)~~

[4] The amendment permitting raw sharing with NCTC would be incorporated into the FBI SMPs that became effective on November 1, 2008, and would apply to all Orders and Warrants that incorporate those Procedures. In addition, that amendment would permit FBI to share with NCTC raw FISA-acquired information collected on or after January 1, 2001, the same date to which the Raw Take Order applies retroactively. As discussed below, NCTC's counterterrorism mission would benefit from this retroactive application because of the foreign intelligence information it will receive. In addition, retroactive application will maintain consistency among NSA's, CIA's, and NCTC's access to such information. Of course, while the amendment would be incorporated into all Orders and Warrants, it would only permit sharing in the categories of cases listed in the amendment. ~~(S)~~

The FBI SMPs themselves apply retroactively, except for Section IV.E (incorporating the Raw Take Order, which contains unique limitations on applicability). *See* Opinion and Order, *In re Electronic Surveillance and Physical Search of Foreign Powers and Agents of Foreign Powers* and *In re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Under the Foreign Intelligence Surveillance Act*, Docket Nos. Multiple and [redacted] (Oct. 31, 2008) ("FBI SMP Order"), at 7, 10-11, 13. The Government accordingly requests that the modifications to the FBI SMPs other than the NCTC sharing provision, and other than the addition of Section IV.E.1, be applied retroactively as well. ~~(S)~~

The Government is not seeking retroactive application of the newly inserted subsection 1 to FBI SMPs Section IV.E, which implements the Raw Take Motion. The modification merely recites FBI's notice obligations to NSA and CIA set forth at 12 to 13 of the Raw Take Motion, discussed below, and expands the scope of the required notice from cases involving communicants who are indicted for a crime to those involving communicants who are charged with a crime. ~~(S)~~

The amendments separately modify Sections IV.A and IV.C of the FBI SMPs, governing dissemination of information. First, in both the domestic and foreign dissemination provisions, they explicitly permit FBI to disseminate information that is necessary to understand foreign intelligence information or to assess its importance. Second, they allow FBI to disseminate foreign intelligence information, or information necessary to understand or assess the importance of foreign intelligence information, to officials and agencies with a national security mission that requires access to foreign intelligence information. Third, they permit FBI to disseminate, for law enforcement purposes, evidence of a crime that is not foreign intelligence information to foreign law enforcement agencies. ~~(S)~~

In addition, the proposal modifies Section IV.E to include an FBI notification requirement under the Raw Take Order. The amendment modifying Section III.C.3 proposes to remove the requirement that FBI notify the Court of non-pertinent

categories of communications in individual FISA applications. Section III.C.3 as amended would continue to require that FBI, in determining whether FISA-acquired information meets the FBI SMP retention standard, pay particular care when applying the SMPs to certain sensitive communications that fall within the categories delineated in that section. The amendments to Sections III.E.1, III.E.2, III.G.1.a, and III.G.1.b address [redacted] and time limits for retention of raw FISA-acquired information. ~~(S)~~

FBI and NCTC have confirmed the facts set forth in this motion. (U)

1. Introduction. (U)

The Attorney General has adopted amendments to the FBI SMPs that permit FBI to provide to NCTC—the Government's primary organization for counterterrorism analysis, coordination, and planning—raw data acquired by the FBI pursuant to FISA in terrorism-related cases. The amendment is necessary to allow NCTC timely access to and use of information vital to its mission and to the United States Government's counterterrorism efforts. The Attorney General has also adopted revised NCTC SMPs governing NCTC's receipt, retention, and dissemination of FISA-acquired information. ~~(S)~~

In addition, the Attorney General has amended the FBI SMPs to clarify the general scope of FBI's authority to disseminate information, and to specifically permit

FBI to disseminate to foreign officials and agencies information that is necessary to understand or assess the importance of foreign intelligence information, or is evidence of a crime. ~~(S)~~

II. Amending the FBI SMPs to Permit Sharing of Raw Data with NCTC will Contribute to National Security, and the NCTC SMPs Satisfy the Act's Requirements. ~~(S)~~

As the Government's leading organization for the integration and analysis of all terrorism- and counterterrorism-related information, NCTC has a compelling need for the information included in the raw systems. While NCTC can currently access terrorism-related FISA-acquired information in FBI's ACS data system, that access is limited to data that the FBI has reviewed, determined to meet the standard set forth in the FBI SMPs, and summarized in a document that has been uploaded to ACS. The amendment to the FBI SMPs described herein will permit FBI to provide to NCTC raw information acquired pursuant to FISA in terrorism-related cases. The NCTC SMPs will subject NCTC's retention and dissemination of FISA-acquired information to limitations similar to those governing FBI, NSA, and CIA. As set forth below, the FBI and NCTC procedures comport with FISA, including FISA's definition of "minimization procedures" in 50 U.S.C. §§ 1801(h) and 1821(4). ~~(S)~~

A. Amendment to the FBI SMPs. (U)

Section IV.G (Access by the National Counterterrorism Center to the FBI's Automated Case Support Database) is replaced in its entirety with the following:

Disclosure to the National Counterterrorism Center (NCTC) of Information Acquired in Cases Related to Terrorism or Counterterrorism. ~~(S)~~

1. In addition to other disclosures permitted in these procedures, the FBI may provide to NCTC:

a. raw FISA-acquired information acquired on or after January 1, 2001 by FBI through electronic surveillance or physical search authorized under the Foreign Intelligence Surveillance Act targeting: (i) foreign powers defined at 50 U.S.C. § 1801(a)(4); (ii) agents of such foreign powers; and (iii) other targets where the surveillance or search is reasonably expected to yield foreign intelligence information related to international terrorism; and

b. information in FBI general indices, including the Automated Case Support (ACS) system and any successor system, provided that such access is limited to case classifications that are likely to contain information related to terrorism or counterterrorism.

NCTC's receipt of information described in (a) and (b) above is contingent upon NCTC's application of NCTC minimization procedures approved by the Foreign Intelligence Surveillance Court with respect to such information. ~~(S)~~

2. Nothing in this Section shall prohibit or otherwise limit FBI's authority under other provisions of these procedures to disseminate to NCTC information acquired pursuant to the Act and to which governing minimization procedures have been applied. ~~(S)~~

3. Nothing in this Section shall preclude FBI from requiring NCTC to apply procedures in addition to Court-authorized minimization procedures, provided that such additional procedures do not relieve NCTC of the

obligation to apply any part of the Court-approved NCTC minimization procedures. ~~(S)~~

4. For every surveillance or search from which FBI discloses raw information to NCTC, FBI shall also provide to NCTC:

   a. the identity of the target(s);

   b. a statement of whether each target was identified as a U.S. person, a non-U.S. person, or a presumed U.S. person in the relevant Court pleadings or orders;

   c. a statement of what special or particularized minimization procedures, if any, were provided for in such pleadings or orders; and

   d. where applicable, a statement that the target, or any other person whose communications with an attorney are likely to be acquired through surveillance or search of the target, is known by FBI monitors or other personnel with access to such FISA-acquired search or surveillance to be charged with a crime in the United States.

~~(S)~~

The notification requirements in subparagraph 4 of this paragraph track closely FBI's obligation, set forth at pages 12 to 13 of the Raw Take Motion, to provide information to CIA and NSA to facilitate their minimization of raw FISA-acquired information. As previously reported to this Court in notices dated November 5, 2010, and November 15, 2011, regarding docket number [redacted] FBI had not been in compliance with two of these requirements, in that FBI did not advise NSA or CIA (a) of categories of non-pertinent communications and/or special or particularized minimization procedures for specific orders, or (b) that a target of an order, or any other

person whose communications with an attorney are likely to be acquired pursuant to an order, was known by FBI to be under indictment.[5] As described in those notices, FBI had routinely advised NSA and CIA of the other two categories of information – (1) the identity of the target(s) of the surveillance or search from which raw data is being provided and (2) a statement of whether each target was identified as a U.S. person, a non-U.S. person, or a presumed U.S. person in the relevant court pleadings or orders. ~~(S)~~

The Office of Intelligence (OI) and FBI worked together to develop a process to aid FBI's compliance with these notification requirements. As described in the November 15, 2011, notice, beginning on October 24, 2011, FBI began providing NSA and CIA with the information described above, with the exception of categories of non-pertinent communications. FBI would provide these same categories of information to NCTC if the Court approves this motion. In addition, as described herein, the proposed amendments to the FBI SMPs would require the FBI to provide special or particularized minimization procedures to CIA, NSA, and NCTC, but not categories of non-pertinent communications.[6] ~~(S)~~

---

[5] *See* Letter from Kevin J. O'Connor, Chief, Oversight Section, Office of Intelligence, National Security Division, U.S. Department of Justice, to the Honorable John D. Bates, United States Foreign Intelligence Surveillance Court, dated Nov. 15, 2011. (U)

[6] Special or particularized minimization procedures may relate to acquisition, retention, and/or dissemination of FISA-acquired information. Because FBI is the agency conducting the acquisition in

As described in the November 15, 2011 notice, FBI and OI worked with the Office of the Director of National Intelligence (ODNI) to provide NSA and CIA with electronic access to the above-described categories of information. For as long as the Raw Take Motion has been implemented, the electronic feed from FBI to NSA and CIA of raw information acquired pursuant to FISA has included, and continues to include, the target's identity and United States person status. In addition, ODNI established a secure "Sharepoint" site that will store information regarding particularized minimization procedures and criminal charges for individual targets. Personnel at NSA and CIA currently have access to this site, and NCTC will be granted access to the site if the Court approves this motion.[7] As noted in the November 15, 2011, notice, FBI has populated the Sharepoint site with information regarding applications approved by the Court beginning on October 24, 2011, and to which the Raw Take Order applies. FBI has also populated the site with information provided by DOJ regarding previous indictments relevant to the cases covered by the Raw Take Order. This historical information only references federal indictments as provided by DOJ to FBI. As noted

---

these matters, FBI generally will not be advising NSA, CIA, or NCTC of special or particularized minimization procedures relating to acquisition. ~~(S)~~

[7] As noted in the November 15, 2011, notice, based on the design and testing of the Sharepoint site, the Government fully expects it to provide an effective means of compliance with FBI's reporting obligations described above. The Government may modify or replace that means of compliance as necessary to ensure efficiency and efficacy. In addition, the electronic feed to NCTC will include the identity and U.S. person status information referenced above. ~~(S)~~

above, under the proposed amendment to the FBI SMPs, FBI will be required to provide notice to NSA, CIA, and NCTC if the target, or any other person whose communications with an attorney are likely to be acquired through surveillance or search of the target, is known by FBI monitors or other personnel with access to such FISA-acquired search or surveillance to be charged with a crime in the United States. ~~(S)~~

Section IV.E of the FBI SMPs, which memorializes the Raw Take Order, will be amended to incorporate provisions tracking sections 2 (which will appear at Section IV.E.2) and 4 (which will appear at Section IV.E.1) of Section IV.G. As noted above, the Government does not seek retroactive application of the new Section IV.E.1. ~~(S)~~

B. NCTC SMPs. ~~(S)~~

The NCTC SMPs generally consist of provisions adapted from the FBI SMPs and procedures governing CIA's and NSA's minimization of information received pursuant to the Raw Take Order (CIA and NSA Raw Take Procedures, or "RTPs")[8] or Section 702 of FISA. They contemplate that NCTC will ingest into NCTC systems raw information acquired by FBI pursuant to the Act in terrorism-related cases and apply minimization procedures, as CIA and NSA currently do under the Raw Take Order.[9] ~~(S)~~

---

[8] The Raw Take Order modified NSA's standard minimization procedures for communications NSA acquires pursuant to Title I of FISA (NSA SMPs) to apply to raw information NSA receives from FBI pursuant to the Raw Take Order. *See* Raw Take Motion at 15-23. Those modified procedures constitute NSA's RTPs. ~~(S//SI)~~

[9] Pursuant to this Court's previous authorization in docket number [redacted], NCTC personnel currently may access terrorism-related case classifications in ACS. All FISA-acquired information in ACS

C. Permitting FBI to Provide Raw Data Acquired in Terrorism-Related Cases to NCTC will Enhance National Security. ~~(S)~~

1. NCTC's Critical Role in U.S. Counterterrorism Efforts ~~(S)~~

NCTC is the nation's primary organization for analyzing and integrating all terrorism- and counterterrorism-related intelligence possessed or acquired by the United States Government. 50 U.S.C. § 404o(d)(1). The Director of NCTC has broad authority and responsibility to "provide strategic operational plans for the civilian and military counterterrorism efforts of the United States Government and for the effective integration of counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States." *Id.* § 404o(f)(1)(B). The NCTC Director also is assigned "primary responsibility within the United States Government for conducting net assessments of terrorist threats." *Id.* § 404o(f)(1)(G). Accordingly, NCTC produces a wide range of analytic and threat information for the President, cabinet officers, senior policy-makers, military commanders, and other components of the government. Staffed by employees of multiple agencies, NCTC is able to draw on diverse backgrounds, disciplines, and experience. This unique environment enables NCTC to bring a broad, interdisciplinary perspective and innovative analysis to bear on information related to terrorism and counterterrorism. (U)

NCTC and FBI will agree to permit NCTC to ingest wholesale the same case classifications into NCTC systems without prior FBI review. ~~(S)~~

The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (Dec. 17, 2004) (IRTPA) amended the National Security Act of 1947, 50 U.S.C. § 401 *et seq.* (1947 Act) to mandate the creation of NCTC within the Office of the Director of National Intelligence (ODNI). 50 U.S.C. § 404o(a). The missions of NCTC, as set forth by Congress, include:

> (1) To serve as the primary organization in the United States Government for *analyzing and integrating all intelligence* possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism;
>
> (2) To conduct strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies;
>
> (3) To assign roles and responsibilities as part of its strategic operational planning duties to lead Departments or agencies, as appropriate, for counterterrorism activities that are consistent with applicable law and that support counterterrorism strategic operational plans, but shall not direct the execution of any resulting operations;
>
> (4) To ensure that agencies, as appropriate, *have access to and receive all-source intelligence support* needed to execute their counterterrorism plans or perform independent, alternative analysis;
>
> (5) To ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities; [and]
>
> (6) To serve as the *central and shared knowledge bank* on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support.

Id. § 404o(d) (emphasis added). In addition, the 1947 Act as amended requires that the Director of National Intelligence (DNI), of whose office NCTC is a component, "shall have access to all national intelligence and intelligence related to the national security which is collected by any Federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence."[10] *Id.* § 403-1(b). (U)

In addition, in the wake of the attempted terrorist attack on board Northwest Flight 253 on December 25, 2009, the President directed NCTC to "[e]stablish and resource appropriately a process to prioritize and to pursue thoroughly and exhaustively terrorism threat threads, to include the identification of appropriate follow-up action by the intelligence, law enforcement, and homeland security communities." Memorandum on the Attempted Terrorist Attack on December 25, 2009: Intelligence, Screening, and Watchlisting System Corrective Actions, Daily Comp. Pres. Doc. DCPD201000009 (Jan. 7, 2010). Through this direction, as well as through others given in the memorandum, the President intended to ensure that the reforms enacted

[10] In 2008, the Attorney General and DNI executed a Memorandum of Agreement (MOA) regarding NCTC's access, retention, use, and dissemination of "terrorism information contained within datasets identified as including non-terrorism information and information pertaining exclusively to domestic terrorism" pursuant to 50 U.S.C. § Section 404o(e). The NCTC SMPs, not the NCTC MOA, will govern NCTC's retention, use, and dissemination of raw FISA-acquired information received from FBI. ~~(S)~~

following the attacks of September 11, 2001, are "appropriately robust to address the evolving terrorist threat facing our Nation in the coming years." *Id.* (U)

As the ODNI component designated as the center for terrorism and counterterrorism analysis and integration, NCTC's mission requires it to pull together information from across government agencies. NCTC thus possesses substantial counterterrorism analytical resources and a mandate to receive and analyze counterterrorism from all legally permissible sources. Greater access to information enhances NCTC's all-source analysts' ability to produce counterterrorism foreign intelligence information. With NCTC's current access to ACS, NCTC analysts can only access FISA-acquired information after FBI personnel have not only reviewed it and determined that it meets the standard set forth in FBI SMPs § III.C. 1, but also summarized the information in a document and then uploaded that document to ACS.[11] ~~(S)~~

That access has been extremely valuable. The proposed ingestion of raw FISA-acquired information from terrorism-related cases, however, will enhance NCTC's abilities by permitting NCTC personnel to: (a) review such data in its original form, or a form closer to the original; (b) draw their own analytical judgments rather than

[11] Notably, it is not uncommon for the document uploaded to ACS to summarize, or even merely reference, particular FISA-acquired communications, while the communications themselves are not uploaded. ~~(S)~~

relying on those of FBI reviewers; (c) view data as soon as it enters NCTC's raw systems, rather than wait for it to be reviewed, identified as meeting applicable standards, analyzed, summarized, and uploaded by FBI personnel into ACS; and (d) apply NCTC's analytical tools in the context of all information in NCTC systems, including information received from a wide variety of federal and other agencies. As described below, two recent threats of international terrorism exemplify the benefit of NCTC access to FBI raw systems. ~~(S)~~

2. *NCTC's Use of ACS Access, and Previous Threats Illustrating the Value of Permitting FBI to Provide Raw Data to NCTC.* ~~(S)~~

The potential value of NCTC's receipt of raw FISA-acquired information is demonstrated by NCTC's use of its access to minimized FISA-acquired information in ACS. In addition, FBI's need to devote substantial analytical resources in two investigations—which involved Court-authorized electronic surveillance and physical search of multiple targets and facilities—presents an example of the benefit that providing raw FISA-acquired information to NCTC would yield. Receiving raw FISA-acquired information would thus enhance NCTC's abilities both to fulfill its own counterterrorism mission and to support FBI in times of urgent need. ~~(S)~~

a. NCTC's Use of ACS Access for its Central Counterterrorism Mission. ~~(S)~~

Since October 8, 2008, NCTC has been permitted to access terrorism- and counterterrorism-related case classifications in ACS, which includes FISA-acquired

information that FBI has determined reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime. ACS has provided NCTC personnel with access to information underlying FBI's formally disseminated reports. There have been numerous benefits from this access. ~~(S)~~

First, ACS access has given NCTC added insight into the meaning of disseminated FBI intelligence products. According to NCTC analysts, ACS provides "crucial context" for FBI intelligence reporting and has had a significant impact on NCTC's analytical priorities and reporting in the Presidential Daily Briefing (PDB) and the National Terrorism Bulletin (NTB). ~~(S)~~

Second, NCTC analysts have relied on details obtained from case files in ACS, combined with terrorism information from other sources, to develop analytic products of their own. Details gleaned from NCTC's continuous review of ACS case files have provided the basis for a number of long-term strategic products. NCTC has also used data from ACS case files as starting points for the synthesis of foreign intelligence from other U.S. Intelligence Community (USIC) agencies, providing the basis for finished NCTC intelligence products. ~~(S//NF)~~

Finally, NCTC has used information obtained from ACS in furtherance of its mission to provide terrorism analysis to senior policy makers in the U.S. Government.

As the designated mission manager for counterterrorism,[12] NCTC's director has the responsibility to disseminate "terrorism information, including current terrorism threat analysis" to senior members of the Executive Branch, including the President and Vice President.[13] NCTC analysts report that access to ACS has provided a significant source of information for several high-level NCTC intelligence products, including the PDB and the NTB. ~~(S)~~

Permitting NCTC to receive FBI-collected FISA-acquired data would enhance many of the benefits that NCTC currently derives from access to ACS. As noted above, receiving raw FISA-acquired information would expand NCTC analysts' ability to draw meaning from, and add context and value to, such information. This would aid NCTC in setting analytical priorities, facilitate alternative interpretations of significant foreign intelligence information, and identify significant foreign intelligence information that may have gone unnoticed or for which context was lacking. NCTC, in turn, could synthesize that information into more meaningful and timely intelligence products for senior policy makers in the U.S. Government and initiate the thorough and exhaustive pursuit of developing terrorism threat threads. NCTC's access to ACS has allowed NCTC personnel to review more information than FBI formally reports, and to review

---

[12] Director of National Intelligence, *Intelligence Community Directive 900: Mission Management* § D.1.b (Dec. 21, 2006). (U)

[13] 50 U.S.C. § 404o(f)(1)(D). (U)

information presented with less analysis and in a form closer to the original than a finished intelligence product. Access to raw FISA-acquired information would take this process a vital step further. It would provide to NCTC the original data underlying the minimized documents in ACS. Of course, it would also provide to NCTC raw data that has not been entered into ACS at all. NCTC could interpret or use either type of data differently than an FBI case agent, given NCTC's different mission, structure, unique access to information from a broad range of sources, and resources. ~~(S)~~

b. NCTC's Demonstrated Ability to Provide Support to FBI Counterterrorism Operations, which Receipt of Raw Data would Enhance. ~~(S)~~

NCTC's receipt of raw FISA-acquired data will not only improve NCTC's understanding of FBI intelligence reporting, but will also allow FBI to call upon the analytic expertise of NCTC to assist in the evaluation of raw FISA-acquired information. As this Court is aware, in [redacted] FBI conducted two simultaneous large, wide-ranging, and rapidly developing counterterrorism investigations, [redacted][14] These investigations involved Court-authorized electronic surveillance and physical search of multiple targets and facilities.

[redacted] (S//NF)

[14] [redacted]

FBI was not authorized to provide raw FISA-acquired information to NCTC in those investigations. To be sure, NCTC personnel detailed to FBI could access such information. Detailees, however, could not continue to access other NCTC systems, and thus could not avail themselves of the information or analytical tools in those systems. In contrast, permitting NCTC personnel to review raw FISA-acquired information in their capacity as NCTC personnel would allow these trained, specialized counterterrorism analysts both to accelerate the review of incoming raw information and to apply their analytical expertise and resources in determining the foreign intelligence value of that information. ~~(S//NF)~~

Although case file information from ACS was of great value to NCTC during [redacted] NCTC could not contribute to FBI's effort to rapidly review raw information. Moreover, NCTC was delayed in receiving foreign intelligence information regarding these terrorism threats and hence could not fully execute its statutory missions, as described above.[15] Permitting FBI to provide raw FISA-acquired information to NCTC, in contrast, would establish a cadre of analysts with training in FISA minimization procedures and computer systems used to process FISA-acquired information, as well as expertise in and current knowledge of

(b)(1); (b)(3); (b)(7(A); (b)(7)(E)

[15] Of course, if additional NCTC personnel were detailed to FBI, they would no longer function as NCTC employees. Thus, while they would gain access to raw FISA-acquired information in FBI systems, they would lose the ability to cross-reference that information with other data in NCTC systems and systems of other agencies to which NCTC has access. ~~(S)~~

international terrorist threats. These NCTC analysts could immediately provide a surge of support in counterterrorism investigations, without requiring FBI to rely on FBI or other-agency detailed personnel who may lack prior training in counterterrorism, FISA minimization procedures, or relevant computer systems, or who may not be as familiar as NCTC analysts with particular threats. ~~(S//NF)~~

In addition, NCTC has determined that permitting FBI to share raw FISA-acquired information acquired on or after January 1, 2001 will fulfill the national security purpose of the proposed sharing. First, as noted above, the Raw Take Order applies to information acquired on or after that date. Maintaining the same rule for CIA, NSA, and NCTC will prevent confusion and ensure that the agencies can share raw information freely in their joint analytical effort. Second, NCTC assesses that information relevant to al Qaeda's planning prior to the September 11, 2001 terrorist attacks is reasonably likely to exist in data acquired on or after January 1, 2001. Because the threat of al Qaeda and associated groups and individuals persists, and based on the analytical value of drawing connections among data points over time, receiving this information would greatly enhance NCTC's counterterrorism efforts. ~~(S)~~

In sum, NCTC's receipt of raw FISA-acquired information will greatly enhance NCTC's execution of its own missions to provide strategic counterterrorism analysis

and to conduct thorough and exhaustive pursuit of developing terrorism threat threads, and will enable it to surge expert resources to support FBI when urgent crises arise. ~~(S)~~

D. *The NCTC SMPs and Amendment to the FBI SMPs Satisfy FISA's Definition of Minimization Procedures.* ~~(S)~~

Collection of information pursuant to FISA may only be authorized if the Government's proposed minimization procedures satisfy the Act's requirements, and FISA-acquired information may only be used or disclosed consistent with Court-approved minimization procedures. 50 U.S.C. §§ 1805(a)(4), 1824(a)(4), 1806(a), 1825(a). FISA sets forth basic requirements for minimization procedures. First, specific procedures must be adopted by the Attorney General and be

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1), 1821(4)(A). (U)

In addition, minimization procedures must ensure that nonpublicly available information that 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." 50 U.S.C. §§ 1801(h)(2), 1821(4)(B). (U)

Finally, notwithstanding the requirements set forth in subsections (1) and (2), minimization procedures must also "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." *Id.* §§ 1801(h)(3), 1821(4)(C). (U)

1. NCTC's Receipt of Raw FISA-Acquired Information is Reasonable and Consistent with the Need of the United States to Produce and Disseminate Foreign Intelligence Information. ~~(S)~~

The proposed amendments will permit FBI to provide raw FISA-acquired information to NCTC, which in turn will be required to apply Court-approved minimization procedures to such information. This Court has previously approved such disclosures when the Government has demonstrated that they serve an important national security interest and that the ultimate recipient of raw information will be responsible for applying Court-approved minimization procedures to that information. Memorandum Opinion, *In Re Electronic Surveillance and Physical Search of Foreign Powers and Agents of Foreign Powers*, Docket No. [redacted] ("ACS Order") (FISA Ct. Oct. 8, 2008); Raw Take Order. Similar to the Raw Take Order, the proposed disclosure will substantially enhance the ability of NCTC both to assist FBI in assessing FISA-acquired

information and to fulfill NCTC's central analytical, planning, and pursuit functions, while protecting the privacy of United States persons consistent with the Act. ~~(S)~~

The Government's need to permit FBI to share raw data with NCTC, paired with the proposed NCTC SMPs, render the proposed sharing program consistent with FISA. The Act requires minimization procedures to "prohibit the dissemination[] of nonpublicly available information concerning United States persons," but only to the extent "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1). As discussed above, the information-sharing program proposed herein directly serves that need by allowing NCTC to review raw information critical to its central analytical role. Indeed, part of NCTC's unique mission is to compare a wide variety of data sets—to which other agencies may not have access—to identify pieces of information that other agencies may have overlooked, or the significance of which may not have been fully appreciated. ~~(S)~~

In addition, NCTC, as discussed above, is the Government's primary organization for counterterrorism analysis, integration, and planning, and possesses unique analytical abilities and perspectives. Its responsibilities span agency boundaries and encompass foreign and domestic threats arising from international terrorism. NCTC depends on, and is charged with facilitating, the sharing of terrorism- and

counterterrorism-related information across agencies. As further discussed above, NCTC's own counterterrorism analysis is substantially enhanced by its timely access to potential foreign intelligence information. Precisely because NCTC has access to multiple sources of international terrorism information, it is in an excellent position to assist FBI and other USIC agencies in understanding and assessing the importance of the information FBI collects pursuant to FISA in terrorism-related cases. Moreover, as set forth in detail below, NCTC's proposed minimization procedures meet the definition of minimization procedures in a manner similar to the procedures this Court has approved for CIA and NSA.[16] ~~(S)~~

As reflected in the Act's legislative history, Congress did not intend Section 1801(h)(1) to prevent the type of sharing that the amended FBI SMPs and NCTC SMPs would facilitate. Rather, Congress intended for "a significant degree of latitude [to] be given in counterintelligence and counterterrorism cases with respect to the retention of

---

[16] In the FBI and NCTC SMPs, some sharing of information is specifically labeled as "dissemination," while other sharing is referred to as a "disclosure." This distinction is intended to avoid confusion in implementation by agency personnel, who may not be attorneys or experts in FISA. Accordingly, in the proposed amended FBI SMPs, the title of Section IV has been changed from "Dissemination" to "Dissemination and Disclosure." Changes of "dissemination" to "disclosure" in the modified FBI SMPs submitted with this motion are not intended to modify FBI's authorization to share information, and the scope of NCTC's authorization under the proposed NCTC SMPs to share information is intended to track the FBI SMPs. Regardless of whether sharing of raw information between agencies, subject to the ultimate recipient's application of Court-approved minimization procedures, constitutes a "dissemination" of information, this Court has found that such sharing is consistent with the Act. ~~(S)~~

For the same reason, in the amended FBI SMPs, "Disclosure" replaces "Dissemination" in the titles and text of FBI SMPs Sections IV.D, IV.E, and IV.G. (U)

information and the dissemination of information *between and among counterintelligence components of the Government*." H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., pt. 1, at 59 (1978) (emphasis added).[17] Congress recognized that "bits and pieces of information . . . may together or over time take on significance" that is not immediately apparent, and stressed that "[n]othing in this definition is intended to forbid the retention or even limited dissemination of such bits and pieces before their full significance becomes apparent." *Id.* at 58. ~~(S)~~

Congress included Section 1801(h)(2) in the definition of minimization procedures to "protect individual United States persons from dissemination of information which identifies them in those areas in which the Government's need for their identity is the least established and where abuses are most likely to occur." *Id.* at 61. By contrast, the analysis and integration of terrorism and counterterrorism information is an area in which the Government's need to identify potential actors—both United States persons and non-United States persons—is well-established. Moreover, based on NCTC's mission, it is anticipated that the foreign intelligence information NCTC is most likely to identify, retain, and disseminate will meet the

---

[17] "[G]iven this degree of latitude," the report notes, it is "imperative that with respect to information concerning U.S. persons which is retained as necessary for counterintelligence or counterterrorism purposes, rigorous and strict controls be placed on the retrieval of such identifiable information and its dissemination or use for purposes other than counterintelligence or counterterrorism." *Id.* Of course, NCTC's receipt of raw data is expressly for a counterterrorism purpose. ~~(S)~~

definition set forth at 50 U.S.C. § 1801(e)(1), and thus will not implicate 50 U.S.C. § 1801(h)(2). In any event, NCTC's receipt of raw FISA-acquired information is fully consistent with the Congressional intent to allow robust analysis of such information, and the NCTC SMPs satisfy the Congressional mandate that U.S. person information that has no foreign intelligence value be protected. ~~(S)~~

2. The NCTC SMPs Protect the Privacy of Information Concerning Unconsenting United States Persons while Facilitating the Production and Dissemination of Counterterrorism Foreign Intelligence Information. ~~(S)~~

The NCTC SMPs are designed to permit the most effective use of foreign intelligence information while protecting the privacy of United States persons. Because NCTC, similar to FBI, is tasked in part with analyzing information acquired in the United States and relating to United States persons, many of the NCTC SMP provisions are based on analogous provisions in the FBI SMPs. Similar to CIA and NSA, however, NCTC does not have an operational law enforcement mission. Accordingly, the NCTC procedures treat privileged communications and crimes reporting in a manner similar to the CIA and NSA RTPs. In addition, the NCTC SMPs contain provisions that either reflect updates to other sets of procedures or are related to NCTC's particular mission and requirements. ~~(S//NF)~~

NCTC will not collect any information pursuant to FISA, so the initial paragraph of the NCTC SMPs states that NCTC will not engage in acquisition.[18] The following paragraph makes clear that the procedures do not apply to information that FBI disseminates to NCTC under the FBI SMPs, except for disseminations effected through NCTC's access to ACS.[19] Under "General Provisions," Sections A(1) and (2) recite the authority and scope of the procedures. Section A(3) incorporates the definitions in the Act, and sets forth definitions relevant to the procedures. "Information," defined in Section A(3)(a), includes all data and content acquired by FBI under Titles I or III or Section 704 or 705(b) of the Act, including "contents" as defined in the Act. The NCTC SMPs adopt the FBI SMP definitions of "metadata," "raw information," and "third-party information" (modified slightly)." *Compare* NCTC SMPs § A(3)(b), (e), (h) *with* FBI SMPs §§ III.A, II.C, III.D. The NCTC SMP definitions of "nonpublicly available information" and "United States person identity" are adapted from definitions in the NSA RTPs, modified to make clear that the reference to "context" in Section A(3)(i) does

---

[18] The Raw Take Motion distinguished CIA's and NSA's receipt of raw FISA-acquired information from Court-authorized "acquisition" of information for the purposes of the Act. *See* Raw Take Motion at 6-7 (CIA and NSA are "permitted to receive raw data from the FBI, but [are not] permitted to acquire information from Court-authorized electronic surveillance or physical search independently. Thus . . . at the acquisition stage, surveillances and searches would continue to be conducted solely by the FBI . . . ."). ~~(S//SI)~~

[19] As reflected in the referenced NCTC SMP paragraph, "dissemination" in this context refers to transmission or disclosure of information by FBI to NCTC after FBI determines such information is foreign intelligence information, necessary to understand foreign intelligence information, or necessary to assess the importance of foreign intelligence information in accordance with minimization procedures applicable to FBI. ~~(S)~~

not modify the "name, unique title, or address" of a United States person.[20] *Compare* NCTC SMPs § A(3)(d), (i), *with* NSA RTPs § 2(h), (f); *see* H.R. Conf. Rep. No. 95-1720, 95th Cong., 2d Sess., at 23 (1978); H.R. Rep 92-1283 at 57. The NCTC definition of "technical database" is adapted from the reference to technical databases in the CIA RTPs, *compare* NCTC SMPs § A(3)(g) *with* CIA RTPs § 3(b), and explicitly separates technical databases from all personnel engaged in intelligence analysis. The NCTC definition of "NCTC employee" is derived from the Raw Take Motion.[21] *Compare* NCTC SMPs § A(3)(c) *with* Raw Take Motion at 6 n.3. Finally, the definition of "review" of information was added to clarify when the age-off provisions set forth at Section B(2), discussed herein, are triggered. *See* NCTC SMPs § A(3)(j).[22] ~~(S)~~

---

[20] The definition of "United States person identity" is identical to the corresponding provision in the procedures governing NSA's and CIA's minimization of information acquired pursuant to Section 702 of FISA, submitted to this Court on April 20, 2011. ~~(S//SI//NF)~~

[21] The definition of "NCTC employee" encompasses detailees from other agencies, including FBI. FBI detailees to NCTC will apply the NCTC SMPs when accessing raw FISA-acquired data in NCTC systems. If they access raw FISA-acquired data in FBI systems, they will apply the FBI SMPs when accessing such data in FBI systems. ~~(S)~~

[22] NCTC advises that, when an e-mail message contains one or more attachments, the message itself is referred to as the "parent" document, while each attachment is referred to as a "child." Although NCTC possesses the technical ability to treat a child document as a separate communication from the parent, such a practice would generally make no more analytical sense than would separately reviewing different paragraphs of an individual message. Accordingly, NCTC in its data systems will process a parent document together with all associated child documents, and when any part of a message or attachment is "reviewed," NCTC will consider the parent and all associated children to have been reviewed. ~~(S)~~

The NCTC SMPs require the same presumptions set forth in the FBI SMPs regarding U.S. person status,[23] and contain essentially the same provisions for departures from the procedures. *Compare* NCTC SMPs § A(4), (5) *with* FBI SMPs § I.C, D. Similar to the CIA RTPs, the NCTC SMPs explicitly state that they do not prohibit certain actions. The provision regarding maintenance of technical databases is similar to the analogous CIA RTP provision. *Compare* NCTC SMPs § A(6)(a) *with* CIA RTPs § 3(b). Section A(6)(b) provides for the use of emergency backup systems, restricts access to such systems, and requires the application of the SMPs to data restored to analytical systems. Section A(6)(c) clarifies that the NCTC SMPs do nothing to impede NCTC's access to FISA-acquired information that FBI, NSA, or CIA could otherwise disseminate to NCTC. ~~(S//NF)~~

Section A(6)(d)(i) adopts the CIA RTP provision permitting retention, processing, or dissemination as specifically required by other legal authorities, but tailors this provision more narrowly than the CIA RTPs. *Compare* NCTC SMPs § A(6)(d)(i) *with* CIA RTPs § 3(d). The intent is to permit NCTC to deviate from the SMPs in response to direct and specific responsibilities, including but not limited to applicable Constitutional disclosure requirements and judicial orders. Executive Branch orders or

[redacted] (S)

directives will not trigger this provision, nor will general Congressional directives that are not specific to information NCTC receives pursuant to this motion. Section A(6)(ii) facilitates lawful oversight of NCTC's handling and use of FISA-acquired information. Section A(7) of the NCTC SMPs tracks the CIA RTP provision permitting crimes reporting, *see* CIA RTPs § 4(f), and Section A(8) is designed to facilitate compliance and oversight by explicitly requiring NCTC to identify in all records, systems, documents, and products FISA-acquired information that it received in raw form from FBI. Section A(9) requires NCTC to adhere to supplemental minimization procedures specific to particular Orders of this Court.[24] Section A(10) reserves the ability for FBI to require NCTC to comply with additional restrictions or obligations relating to the FISA-acquired information FBI provides, without incorporating such Executive Branch policy requirements into the procedures. ~~(S//NF)~~

The retention periods for raw data are the same for NCTC as for FBI, including the amendments to the FBI SMPs discussed below. *Compare* NCTC SMPs § B(2) *with* FBI SMPs § III.G. The NCTC SMPs also explicitly require raw FISA-acquired information to be identified as such, to be accessible only by trained NCTC employees, and to be maintained in a manner that permits marking or identification of information that

[24] This tracks a similar requirement in the Raw Take Order. *See* Raw Take Motion at 19-20. ~~(S)~~

satisfies the retention standard.[25] *See* NCTC SMPs § B(1). Section B(3) provides in general terms for the retention of information that meets the retention standard, which tracks the standard in FBI SMPs § III.C.1, in a manner that does not restrict access or provide for further marking, but that still requires the information to be identified as FBI-collected FISA-acquired information.[26] ~~(S)~~

The provisions governing NCTC's access to and queries of raw data, the requirement that queries be subject to review by DOJ's National Security Division (NSD), and the treatment of [redacted] information are the same as the corresponding FBI rules. *Compare* NCTC SMPs § C(1), (2), (4) *with* FBI SMPs § III.D, B.5, C.2. Section C(3), regarding metadata, tracks FBI SMPs § III.D, with the added requirement that FISA-acquired metadata received from FBI be identified as such, to facilitate compliance with minimization and other requirements. Also consistent with the FBI SMPs, the NCTC SMPs list categories of sensitive communications as to which reviewing personnel must pay special care. *Compare* NCTC SMPs § C(5)(a)-(g) *with* FBI SMPs §

---

[25] As noted above, for analytical purposes NCTC will process as a single communication a "parent" e-mail message and all attached "child" documents. Accordingly, if one document is marked for retention, the parent and associated children will all be retained together. ~~(S)~~

[26] The NCTC SMPs provide for retention and dissemination of information that is evidence of a crime, but not foreign intelligence information. NCTC may only retain or disseminate such information for a law enforcement purpose. As this Court is aware, NCTC is not a law enforcement agency. NCTC's authorization to retain and disseminate evidence of a crime that is not foreign intelligence information—for law enforcement purposes only—is intended to provide NCTC, like CIA and NSA, with the flexibility to handle such information as necessary to fulfill its crimes reporting obligations, and to respond to any unanticipated need to retain or disseminate such information, while remaining consistent with 50 U.S.C. § 1801(h)(3). ~~(S)~~

III.C.3.a-g.[27] As noted above, however, the NCTC procedures for handling attorney-client privileged communications are more similar to corresponding provisions in the CIA and NSA RTPs than the more detailed FBI SMP privilege provisions, which are designed in part to avoid exposing a criminal investigative and prosecuting team to such information.[28] *Compare* NCTC SMPs § C(6)(a), (b) *with* CIA RTPs § 4(a) *and* NSA RTPs § 4(b); *cf.* FBI SMPs § III.E. In addition, Section C(6)(c) of the NCTC SMPs is designed to facilitate compliance with, and oversight of, applicable privilege rules. ~~(S//SI//NF)~~

With the exceptions discussed below, the rules governing NCTC's dissemination and disclosure track other procedures previously approved by this Court.[29] Section D(1), which permits dissemination, is phrased similarly to CIA RTPs § 2, but applies the standard set forth in FBI SMPs § IV.A, including the amendment to FBI SMPs § IV.A proposed below.[30] It also explicitly states that NCTC may only disseminate FISA-

---

[27] This motion seeks to amend FBI SMPs § III.C.3. As set forth below, the amended section retains the provision regarding sensitive communications, but eliminates the requirements relating to categories of non-pertinent communications. ~~(S)~~

[28] While the CIA and NSA RTPs apply to communications of a person who is known to have been indicted for a crime in the United States, the NCTC SMPs apply to communications of a person who is known to have been charged—by complaint, indictment, or other instrument—in the United States. ~~(S//NF)~~

[29] The proposed NCTC SMPs incorporate the modifications made to Sections IV.A and IV.C of the FBI SMPs, which are discussed separately herein. ~~(S)~~

[30] FBI and NCTC may enter into an agreement regarding the coordination of disseminations of FISA-acquired information. Any such agreement is not intended to be incorporated into the FBI SMPs or NCTC SMPs. ~~(S)~~

acquired information as provided in the NCTC SMPs. Section D(2), providing for dissemination of information that is evidence of a crime, but is not foreign intelligence information, is derived from 50 U.S.C. § 1801(h)(3) and FBI SMPs § IV.B. Section D(3), regarding disseminations to foreign governments, tracks FBI SMPs § IV.C.1 and 2.[31] Section D(4) explicitly authorizes NCTC to disclose raw FISA-acquired information to FBI, which collected the information, and to CIA and NSA, which are eligible to receive the same information under the Raw Take Order. Any raw information NCTC shares under this provision must be clearly identified as raw FBI-collected FISA-acquired information, to ensure that the receiving agencies handle it properly. ~~(S//NF)~~

Section D(5) allows NCTC to obtain technical and linguistic assistance from federal agencies, and closely tracks[32] the corresponding FBI SMPs provision. *See* FBI SMPs § IV.D. Section D(6)(a) of the NCTC SMPs incorporates substantially the same caveat requirement for disseminations as the Raw Take Order. *See* Raw Take Motion at 20-21. Section D(6)(b) provides for disseminations by NCTC under circumstances in which the source, method, or legal authority through which information was collected

---

[31] It is not necessary for the NCTC SMPs to include a provision analogous to FBI SMPs § IV.C.3, regarding the use of information in foreign proceedings, because requests for such use will be processed through FBI. In addition, a provision analogous to FBI SMPs § IV.C.4, requiring the maintenance of records of foreign disseminations, would be superfluous because NCTC will be required to maintain records of all disseminations. *See* NCTC SMPs § F(4). ~~(S)~~

[32] The NCTC SMPs omit references to providing media, such as tapes or hard drives, to assisting agencies. ~~(S)~~

may not be disclosed for security or other reasons. It is intended to ensure that NCTC will be able to disseminate terrorism-related foreign intelligence information when necessary, but will be able to prevent the further use of that information—particularly in any proceeding—without the approval of the Attorney General. Of course, if NCTC disseminates information to any recipient for a law enforcement purpose, or without the total prohibition on further use, such information will bear the caveat required by Section D(6)(c) and 50 U.S.C. § 1806(b). Section D(6)(c) incorporates 50 U.S.C. § 1806(b), and Section D(6)(d) tracks the amendment to minimization procedures governing FBI, NSA, and CIA approved by this Court's December 6, 2007 Order in docket number [redacted]. ~~(S)~~

Section E governs NCTC's receipt of information residing in FBI general indices, currently consisting of ACS. *See* Submission Regarding Application of Existing Minimization Procedures to Certain Data Systems of the Federal Bureau of Investigation, *In Re Applications to the Foreign Intelligence Surveillance Court*, Docket No. [redacted] at 33-36 (filed June 16, 2006). Currently, pursuant to this Court's authorization, FBI permits NCTC users to access case classifications in ACS that are related to terrorism or counterterrorism. All FISA-acquired information in these ACS case classifications has either been assessed to be foreign intelligence information relating to terrorism or counterterrorism, or has been assessed to be evidence of a crime

that is not foreign intelligence information. Currently, NCTC's access to ACS is subject to the Court-authorized ACS Procedures, which require NCTC users to disregard FISA-acquired information in ACS that is evidence of a crime, but does not reasonably appear to be foreign intelligence information.[33] *See* ACS Procedures § E(4). ~~(S)~~

Similarly, Section E(1) of the NCTC SMPs submitted with this motion permits NCTC to consider as having been disseminated to NCTC all foreign intelligence information in these case classifications. Section E(2) prohibits NCTC from retaining or otherwise using information that is evidence of a crime, but not foreign intelligence information, except for a law enforcement purpose. These provisions preserve the legally required core of the existing minimization procedures governing NCTC's access to ACS, while leaving policy-based coordination requirements for intra-Executive Branch agreements. They impose essentially the same requirements as Section B(3) of the NCTC SMPs, which regulates NCTC's retention of information received from FBI in raw form. Unlike the ACS Procedures, the NCTC SMPs permit NCTC to retain or disseminate evidence of a crime that is not foreign intelligence information, but only for a law enforcement purpose. While NCTC does not anticipate engaging in such

[33] The ACS Procedures also contain provisions governing coordination between NCTC and FBI, and adopting internal NCTC procedures. The Government submits that such provisions are more appropriate to intra-Executive Branch memoranda and agreements than to Orders of this Court. ~~(S)~~

retention or dissemination, this allowance will provide flexibility if a relevant need arises, and satisfies a statutory requirement. *See* 50 U.S.C. § 1801(h)(3). ~~(S)~~

Sections E(3) and (4) anticipate that, in the future, NCTC may ingest data from ACS without first reviewing that data, and review the ingested information, including FISA-acquired information, in NCTC systems rather than in ACS itself. This would permit NCTC to assess such information using NCTC's analytical tools and in the context of other information in NCTC systems. Access to minimized FISA-acquired information in this manner would greatly enhance NCTC's ability to produce and disseminate foreign intelligence information. Because potentially large volumes of data—data that FBI has already assessed to meet applicable standards in the FBI SMPs—would be shared with NCTC, it would not be practicable or advisable for NCTC to review such information before it enters NCTC systems. After all, most of the information would have already been assessed to be foreign intelligence information, and NCTC would be searching through it for the rare piece of non-foreign intelligence evidence of a crime, in which NCTC has no interest. Still, NCTC may not retain information that is evidence of a crime but not foreign intelligence information for purposes other than law enforcement. The NCTC SMPs therefore require NCTC to destroy any such information promptly after discovering it and determining it not to be foreign intelligence information or necessary to understand or assess the importance of

foreign intelligence information, unless NCTC intends to use it for a law enforcement purpose. Thus, whether NCTC receives FISA-acquired information in raw form, through accessing ACS, or through ingesting data directly from ACS, it will not be permitted to retain information that is not foreign intelligence information, other than evidence of a crime retained for a law enforcement purpose. ~~(S)~~

Section F(1) is intended to ensure compliance with these procedures by training NCTC personnel on their requirements. *See* FBI SMPs § V.B. NCTC will be required to consult with NSD regarding this training, and NSD and NCTC intend for NSD to participate in NCTC training, particularly in the initial stages of NCTC's receipt of raw data. Section F(2) incorporates the general principles of FBI SMPs § III.B.2-4, and Section F(3) corresponds to FBI SMPs § III.A. Section F(4) tracks FBI SMPs § V.A, providing for broad NSD oversight, and adds a specific requirement for NCTC to maintain and make available for review copies of all disseminations of nonpublicly available information concerning non-consenting United States persons. Finally, Section F(5), similar to FBI SMPs § VI, requires NCTC to consult with NSD regarding significant questions regarding the interpretation of the NCTC SMPs. Moreover, in general, NCTC will consult closely with NSD as it develops systems, processes, and procedures for receiving, retaining, processing, and disseminating information in accordance with these procedures. ~~(S)~~

E. Initial Implementation Procedures. (U)

When the Government submitted the Revised FBI SMPs in 2008, this Court agreed with the Government's representation that "it would be 'impractical' to calculate time periods for destruction" under the new retention provisions based on expiration dates for cases that expired prior to the new procedures' effective date. FBI SMP Order at 6. Accordingly, the "Court accept[ed], as a reasonable means of transition to the new retention regime . . . the government's proposal that prior cases be deemed," for the purpose of calculating retention periods, to have expired on the effective date of the new procedures. *Id.* The Government respectfully submits that the same logic applies here, and requests that all data NCTC receives under the sharing regime described herein that FBI acquired pursuant to Orders that expired prior to the effective date of the NCTC SMPs be deemed, for purposes of calculating the retention period under NCTC SMPs § B(2), to have been acquired pursuant to an Order that expired on the effective date of the NCTC SMPs. ~~(S).~~

III. Amendments to Other FBI SMP Provisions. (U)

A. Section III.C.3 (Categories of Non-Pertinent and Sensitive Information). This section is amended to delete "Categories of Non-Pertinent and" from the title, and to replace the text preceding the enumerated list of sensitive categories with the following:

> Particular care should be taken when reviewing information that is sensitive information, as defined below. No sensitive information may be used in an analysis or report (such as an Electronic Communication (EC)) unless it is first determined that such information reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime. Information that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or necessary to assess the importance of foreign intelligence information may be retained, processed, and disseminated in accordance with these procedures even if it is sensitive information. Information that reasonably appears to be evidence of a crime may be retained, processed, and disseminated for law enforcement purposes in accordance with these procedures, even if it is sensitive information. Sensitive information consists of:

In addition, the text after the enumerated list is deleted, and "United States person" is added to subsection (g).

~~(S)~~

The amendment eliminates FBI's obligation to identify and report to the Court categories of non-pertinent information acquired pursuant to this Court's authorities. In effect, the current requirement does not impose any additional responsibility on FBI in its retention and use of such information. Currently, FBI can use such information for further investigation and analysis if it meets the standard in the SMPs for retention

and dissemination of information. The amendment removes a requirement that has no legal effect, and emphasizes the need to pay particular care to sensitive communications. ~~(S)~~

B. *Sections III.E.1.c and III.E.2.c (Retention of Attorney-Client Communications).* These sections are amended to reflect the following insertions and deletions: "A procedure to ensure that [redacted] (S)

While FBI generally can [redacted] (S)

C. *Section III.G.1.a (Time Limits for Retention).* This section is amended to reflect the following insertions and deletions:

> FISA-acquired information that has been retained but never reviewed shall be destroyed five years from the expiration date of the docket authorizing the collection unless specific authority is obtained from an Assistant Director of the FBI (AD)~~,~~ and NSD, ~~and the FISC~~ to retain the material, and the FISC approves a new retention period upon a finding that such modification is consistent with the applicable statutory definition of "minimization procedures.

Section III.G.1.b is similarly modified. ~~(S)~~

These amendments state the standard by which the Court evaluates whether an extension is warranted, and provide for an extension period to be set. (U)

D. *Section IV.A (Dissemination of Foreign Intelligence Information to Federal, State, Local and Tribal Officials and Agencies).* This section is amended to read as follows:

> The FBI may disseminate FISA-acquired information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information or assess its importance, in accordance with Sections IV.A.1 and IV.A.2 to federal, state, local and tribal officials with responsibilities relating to national security that require access to foreign intelligence information ~~directly related to the information proposed to be disseminated~~.

(U)

> *1. Need of the U.S. Government to Disseminate Foreign Intelligence Under the Proposed Standard. (U)*
>
> The first insertion is consistent with 50 U.S.C. § 1801(h)(1) and (2), and corrects an omission. The second insertion, which changes the scope of permissible recipients of disseminations, addresses FBI and NCTC's responsibilities under legal authorities and policies requiring the Intelligence Community to share foreign intelligence information

to the fullest extent permitted by law. The current FBI SMP standard, which limits dissemination to federal, state, local, and tribal officials and agencies with "responsibilities *directly related* to the information proposed to be disseminated" (emphasis added), is not consistent with the Government's need to obtain, produce, and disseminate foreign intelligence information. The current FBI SMP dissemination standard requires the FBI to determine in advance of the dissemination which potential recipients need the particular information. In practice, this standard undermines FBI's ability to fulfill its responsibility under Executive Orders 12333 and 13388 to share foreign intelligence information, including terrorism information, among agencies. The current FBI standard requires FBI to determine to whom it should "push" foreign intelligence information and perpetuates operationally-limiting "need-to-know" information sharing, which was criticized in the Final Report of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission Report"). The proposed standard, in contrast, would enable FBI to apply to FISA-acquired information more contemporary dissemination methods, which allow appropriately cleared consumers of foreign intelligence information to search for and "pull" FISA-acquired foreign intelligence information that they require to perform their official duties. ~~(S)~~

FBI and NCTC have submitted declarations describing in detail their need for the proposed dissemination rule. *See* Declaration of Eric Velez-Villar, Assistant Director, Directorate of Intelligence, FBI, dated March 19, 2012 ("FBI Declaration") (attached as Exhibit D); Declaration of Andrew Liepman, Principal Deputy Director, National Counterterrorism Center, dated March 21, 2012 ("NCTC Declaration") (attached as Exhibit E). ~~(S)~~

It is widely recognized that information sharing among U.S. intelligence and law enforcement agencies is critical to national security.[34] For example, Congress in IRTPA directed the President to "create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." Pub. L. 108-458, § 1016(b)(1)(A). The Foreign Intelligence Surveillance Court of Review noted in 2002 that "effective counterintelligence, we have learned, requires the wholehearted cooperation of all the government's personnel who can be brought to the task. A standard which punishes such cooperation could well be thought dangerous to national security." *In re Sealed Case*, 310 F.3d 717, 743 (FISA Ct. Rev. 2002); *see also* Exec. Order No. 13,388, 70 Fed. Reg. 62023 (2005) §§ 1(a), 2; 9/11 Commission Report at 399-400, 408, 416. The 9/11 Commission Report in particular noted in its discussions of "lost opportunities" to

[34] State, local, and tribal authorities (herein referred to as "non-federal" authorities) are essential to this effort. *See e.g.*, NCTC Declaration para. 8. (U)

detect the 9/11 plot that "no one was firmly in charge of managing the case *and able to draw relevant intelligence from anywhere in the government*, assign responsibilities across the agencies (foreign or domestic), track progress, and quickly bring obstacles up to the level where they could be resolved." 9/11 Commission Report at 400 (emphasis added). The 9/11 Commission emphasized the need for joint intelligence work and the "importance of integrated, all-source analysis," because no single agency "holds all the relevant information." *Id.* at 408. (U)

As detailed in the FBI Declaration, the current FBI standard for dissemination undermines its ability to make FISA-acquired information available for analysts and other users to "pull" as needed. Currently, an FBI analyst who wishes to disseminate FISA-acquired foreign intelligence information as widely as legally permitted must identify all potential recipients with responsibilities directly related to the specific information. This requires a sufficiently broad and detailed knowledge of the mission, roles, and responsibilities of "not only every IC agency, element, ad-hoc task force and, in some cases one or two individuals within an agency, but also that same understanding of all entities that *support* national security missions or *consume* foreign intelligence in fulfillment of their official duties. Further, the area of expertise expected of the information originator must extend not only to the authorities, missions and capabilities of the potential recipient agency, but also to a detailed and expansive

understanding of the information itself"—which indeed may not be possible in the absence of input from other subject matter experts within the IC. *See* FBI Declaration para. 15. ~~(S)~~

In contrast, under the "pull" method, analysts disseminating foreign intelligence information no longer need to try to identify all potential agencies or government officials who require that information. Rather, they can identify a few appropriately secure and access-controlled information repositories in which to place the information. This permits self-guided, cleared users to search for, find, and pull that information which is relevant to their official duties. Examples of such information repositories could include Intelink, NCTC CURRENT, or the Library of National Intelligence (LNI). Once reports are loaded into such repositories, they are discoverable and retrievable by authorized users, who query the repositories for national security-related documents relevant to their official duties. *See* FBI Declaration paras. 10, 16, 20; NCTC Declaration para. 39. ~~(S)~~

Access to some electronic repositories may be as broad as access to the Joint Worldwide Intelligence Communications System (JWICS), comparable to a Top Secret/Sensitive Compartmented Information version of the Internet, or the Secret Internet Protocol Router Network (SIPRNET), comparable to a Secret version of the Internet. Access to others may be limited based on agency or user profiles. Some

repositories can limit access to certain classes of documents based on user profiles, and others currently cannot. All, however, are only accessible by appropriately cleared personnel who have been given access based on their work duties in the field of national security. According to ODNI, such personnel are not limited to U.S. Intelligence Community employees.[35] ODNI concurs, however, that it is reasonable to conclude that the decision to give an agency or individual user access to JWICS, SIPRNET, LNI, or other similar system or repository is based on the agency's or user's need to access the information in those systems or repositories to fulfill a national security-related responsibility. Moreover, as set forth in the NCTC Declaration at para. 39, the searchable electronic repositories discussed herein (or the systems through which users access those repositories, such as an agency's system that is connected to

---

[35] Under certain circumstances, [redacted] may receive limited SIPRNET access. When such users access SIPRNET, their credentials identify them as [redacted] If a site or document has been identified by the owner or administrator as [redacted] users of SIPRNET are not permitted to access it. Similarly, if a site or document has been marked as releasable to one or more of the [redacted] listed above, [redacted] to which the site or document is releasable may access it on SIPRNET. The Department of Defense, which is responsible for SIPRNET, confirms that [redacted] no other [redacted] employees have access to SIPRNET. (S)

According to NSA's JWICS site, no non-United States users have access to JWICS—"JWICS operates at the TS/SI/TK/US-only level." ~~(C)~~

In general, the agency disseminating a particular report is responsible for marking it appropriately, and recipients of disseminations are responsible for handling them in accordance with the markings and caveats they bear. For example, if NCTC disseminated a report that was only cleared for recipients of agencies of the United States or jurisdictions within the United States, it would be marked "NOFORN." If NCTC disseminated a report that was releasable to [redacted] it would be marked as releasable to [redacted] If the reports were then placed onto a site on SIPRNET—or disseminated to any agency—access to, or handling of, those reports would be subject to the marking. ~~(S)~~

JWICS) generally are subject to access policies requiring that users only use the systems in fulfillment of their official duties. For example, the Intelink terms of use state that use of Intelink "is limited to official government business," and that use of Intelink services "for personal/non-official use (e.g., casual browsing ...)" is prohibited.[36] In addition, individuals' use of these systems is also generally subject to audit. *See* NCTC Declaration paras. 19, 39. Accordingly, while users of an electronic repository such as NCTC CURRENT could potentially view a wide variety of intelligence reporting, the requirement that users only access or use the systems in performance of their official duties necessarily requires users to only search the systems with queries reasonably designed to discover information relevant to their work responsibilities. ~~(S)~~

The practice of making foreign intelligence information available in such repositories is based upon the premise that a user, who has been granted a security clearance and access to secure systems containing national security information based on his or her mission needs, is in the best position to determine what information he or she needs to fulfill his or her responsibilities. An analyst at one agency can better find and pull needed information than can a reporting agency identify all analysts that might, based on their training, mission, and other resources, assist them. *See* 9/11

---

[36] *See* Intelink Services Terms of Use (last modified August 2011) [redacted] (S)

Commission Report at 417 (criticizing the assumption that "it is possible to know, in advance, who will need to use" information). Consistent with that premise, and with statutory information-sharing legislation such as the IRTPA provisions quoted above, ODNI and NCTC have provided means such as Intelink, LNI, and NCTC CURRENT to which agencies can contribute foreign intelligence information and from which users can locate and pull the information they need. As reflected in the NCTC Declaration, the "availability of foreign intelligence reporting from diverse sources and disciplines in a common repository offers the substantial added benefit of allowing users to enter a search, review the results of that search, and assess each piece of information in the context of the others." NCTC Declaration para. 40. ~~(S)~~

Significantly, other FISA-related minimization procedures do not impose the mission-based requirement found in the FBI SMPs. For example, the Court-approved CIA and NSA RTPs, which govern CIA's and NSA's treatment of FBI-collected data that CIA and NSA minimize, contain no mission-based restriction on dissemination. The CIA RTPs simply state that U.S. person information that meets the procedures' standard for retention and dissemination "may be retained within CIA and disseminated to authorized recipients outside of CIA." CIA RTPs § 2. The NSA RTPs permit NSA to

disseminate reports based on foreign[37] communications of or concerning United States persons "in accordance with other applicable law, regulation, and policy" if the United States person identities in such communications are deleted.[38] If an NSA report contains unredacted information that identifies a United States person, that report may only be disseminated to a recipient requiring that identity "for the performance of official duties," and if specific additional standards are met.[39] NSA RTPs §§ 6(b), 7. ~~(S//NF)~~

As a result of the unique dissemination requirement in the FBI SMPs, then, when FBI collects FISA-acquired information in matters relating to international terrorism and provides CIA and NSA that information pursuant to the Raw Take Order, CIA and NSA may identify the foreign intelligence information it contains and disseminate that foreign intelligence information, through Intelink and otherwise, to recipients to whom FBI could not itself disseminate under its own SMPs. ~~(S//NF)~~

---

[37] The NSA SMPs' and RTPs tightly limit NSA's dissemination of domestic communications, due to NSA's focus on foreign communications. NSA SMPs § 5(a). ~~(S//SI)~~

[38] To be sure, the Raw Take Motion stated that it "anticipated that CIA and NSA will disseminate foreign intelligence information from FBI FISA collection to the full range of Federal offices and agencies with responsibilities relating to international terrorism to which CIA and NSA now disseminate terrorism-related foreign intelligence from other sources." *See* Raw Take Motion at 21-22 (emphasis added). ~~(S//SI//NF)~~

[39] The additional standards relate, for example, to the foreign intelligence value of the identifying information, and not to the mission of the recipient. ~~(S)~~

Accordingly, as reflected in the authorities that created NCTC, and in the FBI and NCTC Declarations attached hereto, the Government assesses that permitting appropriately cleared personnel with national security responsibilities to conduct research in electronic repositories of foreign intelligence information is a highly effective way of disseminating such information from collectors to consumers. A rule that fails to permit this practice is not consistent with the Government's need to obtain, produce, and disseminate foreign intelligence information. The current rule requires the originator of information to make a product-by-product determination as to what officials require each report, rather than permitting dissemination through searchable repositories. The proposed amendment, in contrast, permits dissemination to repositories, so long as access to the repositories is limited to officials who need access to foreign intelligence information for national security mission-based reasons. Of course, the proposed rule also permits direct transmission of foreign intelligence information to officials with such a mission-based need. In short, although the current FBI SMP dissemination standard requires the FBI to engage in the sometimes impossible task of identifying in advance the full range of agencies and officials that require each particular dissemination of foreign intelligence information to fulfill their national security responsibilities, the proposed new language would still require FBI to determine that proposed recipients have a national security mission. For all practical

purposes, under the proposed standard, even if FBI does not determine in advance of the dissemination to an electronic repository which agencies and officials have responsibilities directly related to the information being disseminated, a user of one of these electronic repositories who designs his/her queries consistent with the electronic repository's terms of use would likely only discover and retrieve FISA-acquired information that was relevant to that user's work responsibilities. ~~(S)~~

2. *Sharing with State, Local, and Tribal Agencies and Officials Under the Revised Dissemination Standard. (U)*

Federal agencies charged with national security have recognized the critical role played by state, local and tribal ("SLT") officials as partners in protecting the United States. Key to the efficacy of that partnership is the sharing of information so that each entity may benefit from the others' unique knowledge and access to information so that threats may be stopped before they materialize.[40] In the terrorism context, the 9/11 Commission Report concluded that one of the most serious weaknesses leading to the attacks was a breakdown in information sharing among federal agencies and with state,

[40] In a recent hearing of the Subcommittee on Counterterrorism and Intelligence of the United States House of Representatives Committee on Homeland Security entitled, "Federal Government Intelligence Sharing with State, Local, and Tribal Law Enforcement: An Assessment 10 Years After 9/11," FBI Assistant Director, Directorate of Intelligence testified: "As threats are increasingly conceived and carried out entirely within our borders, our reliance upon our state, local, and tribal partners has never been more critical. It's almost certain that before an FBI agent comes fact-to-face with a threat actor, a state, local, or tribal police officer or deputy will most likely encounter them first. *They must know what we know in order to do their jobs.*" Oral testimony, Eric Velez-Villar, Assistant Director, Directorate of Intelligence, Federal Bureau of Investigation ("FBI Oral Testimony"), February 28, 2012 Hearing Transcript (Exhibit I), at 10 (emphasis added). (U)

local and tribal governments. 9/11 Commission Report at 400. Since that report was issued, the United States has endeavored to create a new information sharing, and partnership, paradigm in which state, local and tribal officials have the information they need to fulfill their critical partnership roles.[41] Critical to this approach are the Executive Branch's strict standards for restricting access to classified information and protections for privacy and civil liberties. Currently, there are only approximately 4,000 state, local and tribal officials who hold security clearances, which, as discussed below, are required for access to any classified information.[42] Oral Testimony, Scott McAllister, Deputy Under Secretary for State and Local Program Office, Office of Intelligence and

---

[41] IRTPA implemented many of the 9/11 Commission's recommendations, and prioritizes information-sharing, where appropriate, with state, local, and tribal entities—as well as the private sector—through the use of policy guidelines and technologies, while protecting privacy and civil liberties. IRTPA § 1016(b)(2)(A), (H). IRTPA directs the Information Sharing Environment (ISE) Program Manager (PM/ISE) to, *inter alia*, "address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments." *Id.* § 1016(f)(2)(B)(v). The President must report to Congress "the extent to which State, tribal, and local officials are participating in the ISE." *Id.* § 1016(g)(4)(F). The ISE was mandated by IRTPA. It was envisioned as "an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out [Section 1016, "Information Sharing"]." IRTPA § 1016(a)(2). IRTPA left open the possibility that the ISE would be expanded to include other intelligence information. *Id.* § 1016(e)(9), (g)(2)(G). In 2007, Congress added "weapons of mass destruction information" to the definition of "terrorism information." Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53 § 504 (Aug. 3, 2007) ("9/11 Act"). (U)

[42] This number was reported by DHS and presumably does not include, for example, military reservists or SLTs detailed to the FBI for service on JTTFs. (U)

The description of procedures relating to classified information, including how such information is shared with SLT officials, is provided to illustrate processes currently in place. While the Government will continue to protect classified information, specific procedures may change, as may the cited figures—for example, there is no authority that sets a specific number of SLT officials with security clearances. The fact that only 4,000 clearances have been granted, however, demonstrates the care and parsimony with which the federal government determines which SLT officials need, and warrant, access to classified national security information. (U)

Analysis, Department of Homeland Security ("DHS Oral Testimony), February 28, 2012 Hearing Transcript at 17. (U)

Recognizing the need to share information outside the federal government, and to properly safeguard that information, the President issued Executive Order 13549 ("Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities") on August 18, 2010. It set forth the following critical principles, among others:

- SLT personnel are only eligible for access to classified information if they are nominated by a federal agency. *Id.* §§ 1.3(a), 5(b).
- Agencies sponsoring SLT personnel and facilities for access to and storage of classified information must periodically ensure that there is a demonstrated, foreseeable need for such access. *Id.* § 4(d)(1).
- By default, SLT personnel will only be eligible for Secret clearances. *Id.* § 1.3(a).
- SLT facilities where classified information is stored or used are subject to federal inspection, accreditation, and compliance monitoring. *Id.* § 1.3(e).
- Access to information systems that store, process, or transmit classified information shall be enforced by the rules established by the agency that controls the system. Access must be consistent with controls that originators apply to information. *Id.* §§ 1.3(g), 5(h).
- All determinations of eligibility for access to classified information, and all security accreditations of facilities, predating the Order that do not meet the standards in the Order must be reconciled with those standards. *Id.* § 1.3(i).
- DHS is the Executive Agent for the program and has management and oversight responsibilities, including training. *Id.* §§ 2, 4; *see id.* § 4(c) (additional oversight by the Office of the Director of National Intelligence).

(U)

On March 1, 2012, the Secretary of Homeland Security issued a detailed Implementing Directive under the Executive Order. It recognized the need to share "actionable, timely, and relevant classified information" with SLT partners as "self-evident," as well as the need for consistency in procedures relating to sharing, accessing, and safeguarding classified information. *See* Implementing Directive, Classified National Security Information Program for State, Local, Tribal and Private Sector Entities, Department of Homeland Security (March 1, 2012) ("DHS Directive") (Exhibit F), Foreword and §§ 1-100, 1-101. In general, the directive permits federal agencies to sponsor SLT individuals for security clearances and access to classified information if the requirements of the DHS directive are met. Some key provisions of the directive include:

- The directive applies to all SLT personnel who have been sponsored for or granted a security clearance for access to classified information by a federal agency under the SLTPS program[43] and each federal agency that sponsors SLT personnel for such a clearance. It also applies to all SLT facilities that store classified information *Id.* § 1-102(a), (b).
- All information provided to SLT officials remains under control of the federal government. *Id.* § 1-105.
- All federal agencies sharing classified information with SLT entities must report to DHS regarding implementation of the program. *Id.* § 1-103(b).
- Each federal agency that sponsors an SLT individual for a security clearance is responsible for maintaining "security cognizance" over such individual unless that obligation is transferred to DHS. *Id.* § 1-104(a).

---

[43] Parts of the referenced program regulate sharing with private-sector ("PS") entities as well as SLT. (U)

- DHS is responsible for security cognizance of SLT-owned or –operated facilities that store classified information. *Id.* § 1-104(b).
- SLT personnel receiving classified information must safeguard that information, agree to certain procedures, complete security training, and agree to report security incidents. *Id.* § 1-103(c).
- Security clearances for SLT officials must be issued consistent with policies and procedures governing federal employee security clearances. SLT officials undergo the same investigative and adjudicative scrutiny as federal employees. *Id.* §§ 2-101(a), 2-103(b).
- SLT officials selected for security clearances must have a "demonstrated and foreseeable need" for access to classified information and "be in a position to capitalize on the value" of the classified information. *Id.* § 2-101(e).
- SLT law enforcement, public health, and first responder officials are only eligible for clearances if they are participating in a federally sponsored board, committee, task force, fusion center, or similar entity and the sponsoring federal agency determines there is a need for access to classified information.[44] *Id.* § 2-102(a)(1).
- Physical security requirements, including inspection, certification, and oversight by DHS or a sponsoring federal agency. *Id.* §§ 3-101 - 103; *see particularly* § 3-103(b)(4) (classified information technology systems).
- SLT officials are required to protect all classified information and are subject to dissemination rules. *Id.* §§ 4-101 – 108.

The principle means by which the government directly shares national security information with state, local, and tribal partners is through fusion centers,[45] which are

---

[44] Governors, mayors, and senior homeland security, law enforcement, fire, public health, and emergency officials are also eligible. *Id.* §§ 2-101(4), 2-102(a)(1)-(2). (U)

[45] In 2007, Congress was sufficiently concerned regarding the impact on national security of insufficient information sharing with non-federal entities that it included a title in the 9/11 Act under the heading, "Improving Intelligence and Information Sharing within the Federal Government and with State, Local, and Tribal Governments." 9/11 Act, Title V. Congress lauded the development of State, local, and regional Fusion Centers, and directed DHS to establish a DHS State, Local, and Regional Fusion Center Initiative to partner with and support fusion centers. *Id.* § 511; 9/11 Act § 511. In particular, DHS was directed to support efforts to include the fusion centers into the ISE. 9/11 Act § 511(b)(2). Congress considered the Fusion Center Initiative to be "key to Federal information sharing efforts" and took note of "the blossoming State and local intelligence community." H.R. Rep. No 110-259 § 511. Accordingly, it directed DHS to act "quickly, thoroughly, and cooperatively" to provide "maximum support" to the fusion centers. *Id.* (U)

"owned" by state or local authorities, and receive federal support.[46] *See* Statement for the Record, Federal Bureau of Investigation, February 28, 2012 Hearing ("FBI SFR") (Exhibit G), at 1-2; Statement for the Record, United States Department of Homeland Security, February 28, 2012 Hearing ("DHS SFR") (Exhibit H), at 4. Fusion centers contribute to federal national security efforts by providing critical information made available by the combination of SLT officials' knowledge, expertise, and information. The FBI, in turn, provides SLT officials at fusion centers with a national perspective on regional threats and trends to better inform decision-makers at all levels. The FBI assesses that the exchange of intelligence in fusion centers aids other intelligence and law enforcement organizations, including the JTTFs, in their investigative operations. *See* FBI SFR at 2. DHS has undertaken efforts to include fusion centers in the intelligence cycle. *See* DHS SFR at 4. FBI and DHS assess that well-informed SLT officers may be best positioned to detect early signs of terrorist activity. *See* FBI Oral Testimony, February 28, 2012 Hearing Transcript, at 10; DHS Oral Testimony, February 28, 2012 Hearing Transcript at 6. (U)

To be recognized and certified by the federal government, fusion centers are required to meet certain baseline capabilities. This includes implementing a privacy

[46] Information also is shared through FBI-run Joint Terrorism Task Forces (JTTFs), which are operational counterterrorism squads that incorporate non-FBI personnel who are detailed to the FBI; and Field Intelligence Groups (FIGs), which are FBI analytical units that are focal points for information-sharing. (U)

protection policy that "cover[s] all center activities and [is] at least as comprehensive as the requirements set forth in the [ISE Privacy Guidelines, 28 C.F.R. Part 23] and Department of Justice guidelines.[47] There are currently 79 fusion centers.[48] According to DHS, certain fusion centers and certain non-fusion center SLT officials in NY have restricted access to Secret-level federal information systems.[49] *Id.* at 17. ~~(S)~~

The U.S. Government's primary non-defense, Secret-level classified information network available to SLT officials is the Homeland Secure Data Network (HSDN). *See* DHS Directive § 3-103(b)(4)(c). HSDN is a secure communications infrastructure provided by DHS to fusion centers and limited other SLT officials or entities. *See generally* http://www.dhs.sgov.gov. The purpose of HSDN is to provide SLT officials with controlled access to certain sites available on SIPRNET. HSDN is essentially a web portal to certain sites on SIPRNET and also provides users with secure e-mail capability. According to information provided by DHS to DOJ in March 2012, DHS has provided

---

[47] *See* DHS/DOJ Fusion Process Technical Assistance Program and Services, Fusion Center Privacy Policy Development, Privacy, Civil Rights, and Civil Liberties Template (April 2010), *available at* http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181. (U)

[48] The DHS website lists 77 fusion centers. *See* Fusion Centers and Contact Information, http://www.dhs.gov/files/programs/gc_1301685827335.shtm (last updated Feb. 22, 2012). DHS advised the Department of Justice that as of March 2012, the number of recognized centers has reached 79. (U)

[49] According to DHS, it has not provided JWICS access to SLT officials at fusion centers. DHS has provided a JWICS connection to limited senior level leadership of the New York City Police Department (NYPD), but this access is limited to secure e-mail communications. ~~(S)~~

approximately 64 fusion centers with user workstations that are connected to HSDN,[50] and only limited personnel within one of these fusion centers would have access to HSDN. The HSDN terminals are housed in secure conditions at the fusion centers and other locations in New York. Any SLT officials with access to HSDN have received the appropriate security clearance and are bound by the rules regarding the handling of classified information, as detailed above and as provided by Executive Order 13549. ~~(S)~~

Significantly, HSDN does not provide SLT officials with full access to SIPRNET. Rather, it provides access to certain sites on SIPRNET. According to DHS, those sites include ones that DHS and the Department of Defense mutually agree to allow SLT officials access, as well as individual sites to which individual SLT officials may seek access from the federal agency that administers the site. For example, SLT officials may receive access to NCTC CURRENT-S, which contains disseminated foreign intelligence information acquired pursuant to FISA, as described in the NCTC Affidavit paras. 31, 38. ~~(S)~~

SLT officials who are assigned to fusion centers and who have received security clearances may thus access classified foreign intelligence information, potentially including disseminated FISA-acquired information, through HSDN. In addition, SLT

[50] According to information provided by DHS in March 2012, DHS has also provided HSDN terminals to NYPD and the New York City Fire Department. There are limited officials at these agencies who have security clearances and who have been authorized to have access to HSDN. ~~(S)~~

officials receive broadly disseminated intelligence products. For example, according to DHS, DHS issues a Daily Intelligence Bulletin that is e-mailed to SLT officials at fusion centers who have security clearances and authorized access to HSDN. The Daily Intelligence Bulletin is an analytical document compiled by DHS analysts that includes foreign intelligence information disseminated by other federal agencies; the Bulletin includes intelligence that is relevant to the SLT officials and may include FISA-derived information. For example, NCTC may disseminate to NCTC CURRENT-S FISA-derived foreign intelligence information that FBI disseminated to NCTC. DHS, in turn, has access to CURRENT-S and may choose to include that FISA-derived foreign intelligence information in its Daily Intelligence Bulletin if it has some relevance to SLT officials. ~~(S)~~

The restrictions of the current FBI dissemination standard would prevent the FBI from disseminating FISA-derived foreign intelligence information to NCTC CURRENT-S, a repository that is accessed by both federal and SLT officials, because the FBI does not know in advance of the dissemination the identity or responsibilities of every official who has access to the repository. The FBI thus cannot assess whether every potential reader has responsibilities to which a particular dissemination directly relates. Indeed, as discussed above in the context of dissemination to federal partners, a

recipient may not even know that a dissemination will be relevant to his or her responsibilities until discovering it and reading it. (U)

In addition, under the current FBI standard, FBI may not be able to issue to fusion centers across the country an analytical document containing finished intelligence, like the DHS Daily Intelligence Bulletin described above, because FBI would not be able to determine whether every cleared person at the fusion centers had responsibilities "directly" related to the information being disseminated. The fusion center personnel may, for example, have responsibilities related to homeland security, preventing WMD proliferation and cyber attacks, and combating terrorism but may not have responsibilities directly related to the particular FISA-derived information being disseminated. As outlined in the FBI Declaration at paragraphs 23-25, given the important role that SLT officials and entities play in combating terrorism, assisting in homeland security, preventing crippling cyber attacks on local or state government infrastructure, countering WMD proliferation, and otherwise maintaining public safety and security, it is critical that the FBI and NCTC be able to disseminate foreign intelligence information—which has been fully evaluated under applicable minimization procedures—either to secure, access-controlled electronic repositories or through other dissemination vehicles to enable properly cleared SLT officials to protect their regions and assist the federal government in its investigations. ~~(S)~~

Notably, as set forth in the FBI Declaration at paragraphs 24-25, while the need to disseminate to state, local, and tribal officials under the proposed standard will likely be more frequently and routinely applied to counterterrorism information, the FBI, based on its experience and expertise, may determine that dissemination under the proposed standard of particular information other than counterterrorism information may be necessary to national security. The FBI thus seeks the flexibility to do so when the need to engage in such dissemination—to state, local, and tribal officials with national security responsibilities and federal security clearances at the appropriate level—outweighs countervailing considerations. (U)

As noted above, SLT officials are critical national security partners. When sharing any classified information with SLT officials, the federal government takes great care to ensure that that information is handled with the same security and privacy controls it is accorded within the federal system. Executive Order 13549 and the DHS Directive mandate that SLT officials' eligibility for security clearances is limited and need-based. SLT personnel and facilities are subject to the same security requirements as federal personnel and facilities, and are subject to federal oversight. While some SLT officials may be involved in other sharing or access arrangements, *see, e.g.*, DHS Directive § 1-108(a), all classified information is subject to security restrictions. *See, e.g.*,

Executive Order 13526 §§ 4.1 (general restrictions), 4.2 (distribution controls), 5.4(d)(5) (preventing unnecessary access). (U)

E. Section IV.C (Dissemination of Foreign Intelligence Information Concerning United States Persons to Foreign Governments). This section is amended as follows: the title of the section will read "Dissemination to Foreign Governments." The following underlined text will be inserted into the first sentence: "The FBI may disseminate FISA-acquired information concerning United States persons, which reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime being disseminated for a law enforcement purpose, to foreign governments as follows". In addition, the following underlined text is inserted into Section IV.C.2: [redacted] (S)

The amendment tracks the first insertion to Section IV.A above, and consistent with 50 U.S.C. § 1801(h)(3) adds authority for FBI to disseminate evidence of a crime to foreign governments. This corrects an omission in the FBI SMPs. To facilitate the dissemination of evidence of a crime to foreign governments, the amendments permit FBI to [redacted] (S)

F. *Section IV.E (Disclosure Under Docket Number* [redacted]). In addition to the title change discussed above, this section is amended to add the following:

1. For every surveillance or search from which FBI discloses raw information to CIA or NSA, FBI shall also provide:

a. the identity of the target(s);

b. a statement of whether each target was identified as a U.S. person, a non-U.S. person, or a presumed U.S. person in the relevant Court pleadings or orders;

c. a statement of what special or particularized minimization procedures, if any, were provided for in such pleadings or orders; and

d. where applicable, a statement that the target, or any other person whose communications with an attorney are likely to be acquired through surveillance or search of the target, is known by FBI monitors or other personnel with access to such FISA-acquired search or surveillance to be charged with a crime in the United States.

~~(S)~~

2. Nothing in this Section shall prohibit or otherwise limit FBI's authority under other provisions of these procedures to disseminate to CIA or NSA information acquired pursuant to the Act and to which governing minimization procedures have been applied. ~~(S)~~

FBI's notice obligations to CIA and NSA under the Raw Take Order are currently set forth only in the Raw Take Motion. The amendment adds them to the FBI SMPs.

See United States Foreign Intelligence Surveillance Court Rules of Procedure, Rule 12.

~~(S)~~

G. Section VII (Review of Procedures). This section has been modified to reflect that the date by which the FBI SMPs will be reviewed remains five years from the date on which those procedures were initially adopted. ~~(S)~~

V. Conclusion. (U)

The Government respectfully submits that the FBI SMPs, with the amendments approved by the Attorney General, meet the definition of minimization procedures under 50 U.S.C. §§ 1801(h) and 1821(4). As set forth above, based on NCTC's articulated need, the Government requests that FBI be permitted to share raw FISA-acquired information acquired in terrorism-related cases on or after January 1, 2001. The remaining amendments to the FBI SMPs, except the insertions to Section IV.E, modify provisions that themselves apply retroactively, pursuant to this Court's Order, and the Government requests that those amendments apply with the same retroactivity. Accordingly, the Government respectfully requests that the Court issue the proposed Order attached hereto, which applies the amended procedures retroactively, to previously issued Orders and Warrants of this Court. The Government further submits that the NCTC SMPs meet the definition of minimization procedures cited above. ~~(S)~~

WHEREFORE, the United States of America, by counsel, files with this Court the attached amendment to the FBI Standard Minimization Procedures and respectfully moves to amend all Orders and Warrants issued by this Court governed by those Procedures. A proposed Order to that effect is attached hereto. The United States further files the attached Revised NCTC Standard Minimization Procedures. ~~(S)~~

Respectfully submitted,

Lisa O. Monaco
Assistant Attorney General

Tashina Gauhar
Deputy Assistant Attorney General

Kevin J. O'Connor
Chief, Oversight Section

VERIFICATION

I have reviewed the foregoing motion and the National Counterterrorism Center (NCTC) Standard Minimization Procedures described therein. NCTC will follow those minimization procedures with respect to information acquired by FBI pursuant to Court-authorized electronic surveillance, physical search, or other acquisition and provided to NCTC by FBI. ~~(S)~~

21 March 2012
Date

Andrew Liepman
Principal Deputy Director
National Counterterrorism Center

VERIFICATION

I have reviewed the foregoing motion and the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act described therein. The FBI will follow those minimization procedures applicable to the FBI, as described in the foregoing motion. (U)

4/16/12
Date

Mark F. Giuliano
Executive Assistant Director
National Security Branch
Federal Bureau of Investigation

I hereby approve the filing of this Motion regarding the sharing of FISA-acquired information between FBI and NCTC and the attached proposed Order with the United States Foreign Intelligence Surveillance Court. ~~(S)~~

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

Date: 4-20-12

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE ELECTRONIC SURVEILLANCE, PHYSICAL SEARCH, AND OTHER ACQUISITIONS TARGETING INTERNATIONAL TERRORIST GROUPS, THEIR AGENTS, AND RELATED TARGETS

Docket Numbers [redacted]

MEMORANDUM OPINION AND ORDER

In a submission made on April 23, 2012 ("April 23, 2012 Submission"), the government proposed new standard minimization procedures for the National Counterterrorism Center (NCTC) and various amendments to the standard minimization procedures used by the Federal Bureau of Investigation (FBI).[1] Both the NCTC procedures and the amendments to the FBI procedures were approved by the Attorney General on April 20, 2012.

The primary objective of these proposed procedures is to permit the FBI to provide to NCTC information relating to international terrorism in raw form, and to permit NCTC to review, retain, and disseminate such information, subject to procedures that comply with the requirements of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1885c. The government's proposal also encompasses a number of changes to the FBI's standard minimization procedures that do not directly bear on NCTC's receipt and use of such information.[2]

---

[1] See Docket Nos. [redacted] & [redacted] Government's Submission of Amendments to Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act, and Submission of Revised Minimization Procedures for the National Counterterrorism Center, and Motion for Amended Orders Permitting Use of Amended Minimization Procedures, filed on Apr. 23, 2012.

[2] The Court initially approved the current version of the FBI's standard minimization procedures in 2008. See Docket No. [redacted] Submission of Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search ("2008 FBI SMPs"), filed on Oct. 23, 2008; Opinion and Order ("FBI SMPs Opinion"), issued on Oct. 31, 2008. This initial approval was

(continued...)

For the reasons stated below, the Court finds that the minimization procedures proposed by the government satisfy the applicable requirements of FISA.

I. The Applicable Statutory Requirements

The government intends the new procedures to apply to information obtained through certain electronic surveillances, authorized pursuant to 50 U.S.C. §§ 1801-1812, and physical searches, authorized pursuant to §§ 1821-1829, as well as to certain acquisitions of foreign intelligence information authorized pursuant to § 1881c. April 23, 2012 Submission at 2-3 & n.2.[3] FISA requires that information obtained through these forms of collection be handled in

---

[2](...continued)
granted in the context of a motion to amend all prior FBI search and surveillance orders so that the 2008 FBI SMPs would thereafter govern the handling of information previously acquired pursuant to those orders. See FBI SMPs Opinion, at 3-7. In that motion, the government proposed, and the Court accepted, that it was sensible to modify how certain provisions of the 2008 FBI SMPs would apply to information acquired before November 1, 2008, or pursuant to orders issued before November 1, 2008. See id. at 4-6, 10-11. To the extent warranted, some of these modifications are further discussed below. At the same time, the government presented a second motion that sought to exempt specified FBI data storage systems from certain marking and notice requirements embodied in the 2008 FBI SMPs. The Court granted this motion also. See id. at 7-9, 11-12 (exempting specified systems from the marking requirements of Section III.B.5 and Section III.C.1 and the electronic notification requirements of Section III.E.1.e and Section III.E.2.d). Since then, the Court has approved the use of the 2008 FBI SMPs, subject to the same exemptions, in many individual cases.

Because the government describes its current proposal as involving amendments to the 2008 FBI SMPs, see, e. g., April 23, 2012 Submission at 2-3, and those amendments do not affect the provisions of the 2008 FBI SMPs that are implicated by the above-described modifications and exemptions, the Court understands the government to intend these modifications and exemptions to remain in force. That approach is reasonable and in conformance with FISA's minimization requirements. The continued effect of these modifications and exemptions is specified infra at page 20.

[3] The government further intends to use the new procedures for information obtained pursuant to certain authorizations made by the Attorney General pursuant to Section 1881d(b). See April 23, 2012 Submission at 2-3 & n.2. The Court does not review minimization procedures under Section 1881d(b).

accordance with minimization procedures.[4] The statute defines "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;[5]

---

[4] See § 1805(a)(3), (c)(2)(A) (when authorizing electronic surveillance, Court must find that the minimization procedures satisfy the applicable statutory definition and direct that the procedures be followed); § 1824(a)(3), (c)(2)(A) (same for physical search); § 1881c(c)(1)(C) (when authorizing acquisition of foreign intelligence information pursuant to Section 1881c, Court must find that the "dissemination provisions" of the minimization procedures comply with the statutory definition of "minimization procedures" for electronic surveillance or physical search, "as appropriate").

[5] Section 1801(e) defines "foreign intelligence information" as

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

(continued...)

> (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) (electronic surveillance); § 1821(4) (physical search).[6]

The issue presented is whether the proposed amendments to the FBI procedures and the new NCTC procedures comply with this definition. In order to analyze this issue, the Court first will examine the proposed sharing of raw information with NCTC, subject to NCTC's applying a new set of standard minimization procedures. The Court will then examine the proposed revisions to the FBI's standard minimization procedures that do not relate directly to sharing raw information with NCTC, as well as the corresponding provisions of the new NCTC minimization procedures.

II. FBI's Sharing of Raw Information with NCTC

The proposed procedures would authorize the FBI to provide to NCTC

> raw FISA-acquired information acquired on or after January 1, 2001 by FBI through electronic surveillance or physical search[7] targeting: (i) foreign powers

---

[5](...continued)

> (B) the conduct of the foreign affairs of the United States.

[6] The definitions of "minimization procedures" for electronic surveillance and physical search are substantively identical (although the definition for physical search at § 1821(4)(A) refers to "the purposes . . . of the particular physical search"). For ease of reference, subsequent citations refer only to the definition for electronic surveillance at § 1801(h).

[7] It is the government's practice to propose use of the FBI's standard minimization procedures for electronic surveillance and physical search in certain applications for acquisition (continued...)

> as defined at 50 U.S.C. § 1801(a)(4) [groups engaged in international terrorism or activities in preparation therefor]; (ii) agents of such foreign powers; and (iii) other targets where the surveillance or search is reasonably expected to yield foreign intelligence information related to international terrorism.

Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the FISA ("Proposed FBI SMPs") § IV.G.1.a., at 33, attached as Exhibit A to the April 23, 2012 Submission. This proposal is similar to information-sharing that the Court has previously approved for the National Security Agency (NSA) and the Central Intelligence Agency (CIA).[8] An order that was originally issued in 2002 and extended in 2004 permits NSA and CIA to receive raw information from FBI electronic surveillance and physical search of terrorism-related targets, subject to Court-approved minimization procedures for those agencies. See Docket No. [redacted], Order issued on July 22, 2002; Order issued on May 19, 2004.

NCTC analysts do not presently have access to the raw FISA information that their counterparts at FBI, CIA, and NSA work with. Instead, under a separate order issued in 2008, NCTC is authorized to receive certain FISA-derived information from terrorism cases that FBI has uploaded to its Automated Case System (ACS) database. ACS 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 via ACS has already been subject to minimization by the FBI. The Court approved procedures in 2008 that permit the FBI to make information in ACS available to NCTC analysts without further review, provided that such access is limited to classifications of cases that are likely to contain information related to terrorism or counterterrorism and that NCTC applies its own Court-approved minimization procedures to such information. Docket No. [redacted] Memorandum Opinion ("NCTC Opinion") issued on Oct. 8, 2008, at 3-6. The

---

[7](...continued)
of foreign intelligence information pursuant to Section 1881c. In such cases, when reviewing the dissemination provisions of those procedures pursuant to Section 1881c(c)(1)(C), the Court understands references within those procedures to information obtained through electronic surveillance and physical search to include information obtained through Section 1881c acquisitions.

[8] The Court has authorized FBI to share with CIA and NSA raw FISA information from the above-described categories of cases, only if the FBI acquired the information on or after January 1, 2001. See FBI SMPs Opinion, at 6-7, 11. The government does not seek authorization for the FBI to share raw information acquired before that date with NCTC, CIA or NSA. See April 23, 2012 Submission, at 4 n.4.

Court found that such access was "consistent with the need of the United States to obtain, produce and disseminate foreign intelligence information" under § 1801(h)(1). NCTC Opinion at 3.

In broad terms, the current proposal would put NCTC on the same footing as CIA and NSA with regard to terrorism-related information obtained by the FBI under FISA: NCTC would be authorized to receive and analyze raw data prior to FBI review and evaluation, and to use and disseminate the results of its analysis in accordance with its own Court-approved minimization procedures. The government argues persuasively that permitting NCTC to receive and work with raw FISA information would substantially contribute to the ability to produce and disseminate terrorism-related foreign intelligence information.

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). In 2010, the President directed NCTC to establish a process to prioritize and exhaustively pursue terrorism threats. Declaration of Andrew Liepman, Principal Deputy Director, NCTC ("NCTC Declaration"), at 5, attached as Exhibit E to the April 23, 2012 Submission.

The government reports that, since 2008, NCTC's ability to access information from terrorism-related cases in ACS "has been extremely valuable." April 23, 2012 Submission at 16. For example, NCTC's review of information in ACS "provided the basis for a number of long-term strategic products," and "access to ACS has provided a significant source of information for several high-level NCTC intelligence products," including the President's Daily Brief. Id. 18-19.

Providing NCTC with access to raw FISA information is expected to provide greater benefits. Under the current arrangement, NCTC cannot have access to FISA information before it is reviewed by FBI personnel and put into a report or other form of work product that is then uploaded into ACS. The government's proposal would permit NCTC to receive and work with the raw information directly, without delay. Id. at 17. It would also permit NCTC to analyze information in its original (or closer-to-original) form, rather than filtered through the analytic judgments of FBI personnel. Id. at 16-17. "[G]iven NCTC's different mission [and] unique access to information from a broad range of sources," it is anticipated that NCTC personnel will sometimes be able to interpret or use raw FISA information differently than an FBI agent would.

Id. at 20; see also NCTC Declaration at 17 (describing case where FBI analyst who was working at NCTC recognized the significance of a piece of raw FBI FISA information [redacted]).[9]

In short, the Court is persuaded that bringing NCTC's expertise and resources to bear on the immediate analysis of raw FISA data, in comparison with its working with derivative reporting after it is prepared by the FBI, will enhance the government's ability to identify, extract, and exploit counterterrorism information. FBI's providing this information to NCTC will be, in the language of Section 1801(h)(1), "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[10] For this reason, procedures that permit the sharing of raw data with NCTC can be consistent with the requirements of Section 1801(h)(1).

The Court further finds that Section 1801(h)(2) does not prohibit the proposed transmittal of raw information from the FBI to NCTC. Section 1801(h)(2) applies to dissemination of FISA information that is neither foreign intelligence information as defined at Section 1801(e)(1), nor evidence of a crime disseminated under Section 1801(h)(3). For information within its scope, Section 1801(h)(2) requires minimization procedures to prohibit disseminations that identify a U.S. person "unless such person's identity is necessary to understand foreign intelligence information or assess its importance." For the reasons stated above, the proposed sharing of raw data may be regarded as necessary for NCTC to understand, and assess the importance of, the

---

[9] The government further notes that experience in recent high-intensity international terrorism investigations suggests that such cases would substantially benefit from NCTC's being able to support the FBI with a cadre of experienced counterterrorism analysts who can help review raw FISA information, while also drawing on NCTC's other counterterrorism resources. April 23, 2012 Submission at 20-22.

[10] As set out above, Section 1801(h)(1) requires procedures that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination," of U.S. person information," consistent with foreign intelligence needs. § 1801(h)(1) (emphasis added). The government suggests that the passage of raw FISA information from one agency to another may not be a "dissemination" in circumstances where the receiving agency will be required to apply its own FISA-compliant minimization procedures to that information. See April 23, 2012 Submission at 26 n.16; see also NCTC Opinion at 5. The Court need not decide whether FBI's passing raw information to NCTC constitutes a dissemination. The discussion in the text assumes arguendo that the passage of raw information from FBI to NCTC constitutes a "dissemination," and the Court finds that the procedures permitting that "dissemination" nonetheless comply with Section 1801(h).

foreign intelligence information it is seeking to identify and extract. Because the transmittal of raw data necessarily includes any U.S. person identities embedded within the data, the FBI may transmit such U.S. person identities to NCTC, in the manner proposed by the government, without violating Section 1801(h)(2).

Moreover, there is reason to think that Section 1801(h)(2) may not apply at all to the proposed transmittal of raw information to NCTC. The language of this provision suggests that it is directed at the transmittal of finished reporting, which is the context in which the foreign intelligence significance of U.S. person identities can be evaluated.[11] If there is any ambiguity on this point, the legislative history confirms that Section 1801(h)(2) does not prohibit the transmittal of unreviewed information that may contain U.S. person identities:

> Because minimization is only required with respect to information concerning U.S. persons, where communications are encoded or otherwise not processed . . . there is no requirement to minimize . . . until their contents are known. Nevertheless, the minimization procedures can be structured to apply to other agencies of the Government, so that if [another] agency . . . decodes or processes the communication, it could be required to minimize the retention and dissemination of information therein concerning U.S. persons.

H.R. Rep. 95-1283, pt. 1, at 57-58.

Consequently, the Court concludes that the FBI may transmit raw FISA information to NCTC, provided that NCTC handles the raw information in accordance with minimization procedures that comport with Section 1801(h).

III. The Adequacy of NCTC's Minimization Procedures Under Section 1801(h)

The government proposes to replace NCTC's current minimization procedures with a new set of procedures. See NCTC Standard Minimization Procedures for Information Acquired by the FBI Pursuant to Title I, Title III, or Section 704 or 705(b) of the FISA ("NCTC SMPs"), attached as Exhibit C to the April 23, 2012 Submission. Most of the substantive provisions of the NCTC SMPs closely resemble provisions of the 2008 FBI SMPs or of the minimization

---

[11] Also, as noted above, Section 1801(h)(2) does not apply to dissemination of foreign intelligence information as defined at Section 1801(e)(1), which includes counterterrorism information. Because the FBI will only share raw information with NCTC if it has been acquired in terrorism-related cases, one would expect that much of the foreign intelligence information gleaned from this data will fall within Section 1801(e)(1).

procedures now in effect for CIA's handling of raw information from FBI terrorism-related collections, as approved in Docket No. [redacted] A number of these parallel provisions are identified below.

The NCTC SMPs will govern the retention, use, and dissemination of information received from the FBI in raw form, see NCTC SMPs Preamble, at 1, as well as FBI information from terrorism-related cases that appears in ACS or other FBI general indices, see id. § E, at 11-12.[12] In addition to the NCTC SMPs, NCTC personnel will be required to follow any Court-approved special or particularized minimization procedures that FBI provides to NCTC" regarding a particular case. See id. § A.9, at 4.[13]

NCTC will be obliged to specially mark FISA information received from the FBI, whether it is in raw or derivative form. NCTC SMPs § A.8, at 4; § B.1, at 5. Only appropriately trained NCTC personnel will have access to raw FISA information. Id. § B.1, at 5; § F.2, at 12. Queries of the raw FISA data "must be reasonably designed to find and extract foreign intelligence information." Id. § C.1, at 6.

"Metadata" – i. e., "dialing, routing, addressing, or signaling information associated with a communication" that is not "information concerning the substance, purport, or meaning of the

---

[12] NCTC may take action "in apparent departure from these procedures in order to protect against an immediate threat to human life," provided "that it is not feasible to obtain a timely modification of these procedures" from the Attorney General and the Court. NCTC SMPs § A.5.b, at 3. If such action is taken, the Court must be notified promptly. Id. The current FBI procedures contain a substantively identical provision. See 2008 FBI SMPs § I.E., at 3.

[13] For its part, FBI will be required to communicate to NCTC case-specific information – including the identity and U.S. person status of the target and applicable case-specific minimization procedures – when it makes raw FISA information available to NCTC. Proposed FBI SMPs § IV.G.4, at 34. These requirements generally track the FBI's current obligations to provide case-specific information to CIA and NSA when it shares raw FISA data with those agencies. See Docket No [redacted] Motion for Amended Orders Permitting Modified Minimization Procedures, filed on May 10, 2002, at 12-13. One of the proposed amendments to the 2008 FBI SMPs makes these obligations an explicit part of the provision of the FBI standard minimization procedures that governs information sharing with CIA and NSA pursuant to Docket Number [redacted] Proposed FBI SMPs § IV.E, at 32. After a period of non-compliance, the government has established a process for FBI to provide such case-specific information and procedures to CIA and NSA, and the FBI will use a similar process to provide them to NCTC. See April 22, 2012 Submission at 9-12.

communication," id. § A.3.b, at 2 – may be retained indefinitely for intelligence analysis purposes. Id. § C.3, at 6. All other raw information, including the substantive contents of communications, is subject to a specific retention schedule. Unless a modification is approved by the Court, raw information that has not been reviewed must be destroyed within five years of the expiration date of the authorization pursuant to which it was acquired, id. § B.2.a, at 5, and information that has been reviewed, but not found to be pertinent,[14] is subject to heightened access controls after [redacted] from such date and must be destroyed after [redacted] Id. § B.2.b., at 5.[15] This retention schedule, including the authority to retain metadata indefinitely, is in accord with the retention provisions of the current FBI SMPs. See 2008 FBI SMPs § III.G.1, at 25-26.

As a general rule, NCTC analysts may use information that is reviewed and found to be pertinent; however, additional restrictions apply to information concerning [redacted] see NCTC SMPs § A.3.h, at 2, § C.4, at 6-7, and attorney-client communications, see id. § C.6, at 7-8. These provisions substantively track provisions of the current FBI and CIA procedures, respectively.[16]

---

[14] For ease of reference, this Opinion and Order uses the phrase "not found to be pertinent" to describe data that has been reviewed, but not found to be information that reasonably appears to be foreign intelligence information, that is necessary to understand foreign intelligence information or assess its importance, or that is evidence of a crime.

[15] The government proposes that, for purposes of calculating retention periods under NCTC SMPs § B.2, information "that FBI acquired pursuant to Orders that expired prior to the effective date of the NCTC SMPs be deemed . . . to have been acquired pursuant to an Order that expired on the effective date of the NCTC SMPs." April 23, 2012 Submission at 40. The Court approved a similar means of transitioning to a new retention schedule when the current version of the FBI SMPs was adopted in 2008. See FBI SMPs Opinion, at 6. The Court approves this approach because the resulting retention periods are reasonable as applied to a body of information that is newly available to NCTC.

[16] See 2008 FBI SMPs § III.C.2, at 13-14 [redacted]; Docket No. [redacted] CIA Minimization Procedures for Information From FISA Electronic Surveillance and Physical Search Conducted by the FBI ("CIA Minimization Procedures") § 4.a, at 4-5 (attorney-client communications), attached as Exhibit A to the Motion for Amended Orders Permitting Modified Minimization Procedures filed on May 10, 2002; see also infra note 27 regarding how NCTC will handle attorney-client communications.

When disseminating foreign intelligence information NCTC must remove the identities of U.S. persons, unless an identity is necessary to understand foreign intelligence information or assess its importance. NCTC SMPs § D.1, at 8.[17] Otherwise, the requirements for disseminating information to federal, state, tribal, and local officials, and to foreign governments, are largely patterned after corresponding provisions of the 2008 FBI SMPs.[18] Any significant differences are discussed infra at pages 12-17. NCTC personnel also may retain, process or disseminate information when reasonably necessary to fulfill specific legal requirements or to conduct lawful oversight of its handling of FISA information. NCTC SMPs § A.6.D, at 4; compare 2008 FBI SMPs § I.F, at 3 ("Nothing in these procedures shall restrict the FBI's performance of lawful oversight functions of its personnel."); CIA Minimization Procedures § 3.d, at 3-4 (general standards for retention and dissemination do not prohibit "retention or dissemination of information required by law to be retained or disseminated") .

The Court finds that the NCTC SMPs are "specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular [collection], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need . . . to obtain, produce, and disseminate foreign intelligence information," within the meaning of Section 1801(h)(1). As noted above, the NCTC SMPs are substantially patterned on procedures that the Court has previously found to comport with Section 1801(h)(1), when applied by other agencies to the same set of terrorism-related information. The fact that, under the current proposal, NCTC will be handling the information is not, in and of itself, a cause for added concern. While certain provisions, which correspond to proposed amendments to the 2008 FBI SMPs, merit additional discussion, see infra pp. 12-19, the Court is satisfied that the NCTC SMPs, taken as a whole, satisfy Section 1801(h)(1).

Likewise, the Court finds that Section D.1 of the NCTC SMPs, which regulates the dissemination of U.S. person identities, comports with Section 1801(h)(2).

---

[17] Under the terms of Section D.1, this requirement to remove U.S. person identities applies to foreign intelligence information falling under either subsection of the definition at Section 1801(e).

[18] Compare NCTC SMPs § D.1, 3, at 8-9 with 2008 FBI SMPs at § 4.A-C, at 27-30. Similarly, the provisions for disclosing raw information in order to obtain technical or linguistic assistance from another federal agency are substantively identical for NCTC and the FBI. Compare NCTC SMPs § D.5, at 10 with 2008 FBI SMPs § 4.D, at 30-32.

As noted above, Section 1801(h)(3) specifies that minimization procedures shall "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." Section A.7 of the NCTC SMPs satisfies this requirement.[19]

IV. Amendments to FBI SMPs (and Corresponding Provisions of the NCTC SMPs)

The government also seeks to amend the current FBI SMPs in several respects that are not directly related to sharing raw FISA information with NCTC. For the most part, as noted below, the corresponding provisions of the proposed NCTC SMPs track these amendments to the FBI SMPs.[20]

A. Expansion of Authorities to Disseminate Information

Most significantly, the Proposed FBI SMPs seek to expand the FBI's authority to disseminate reporting based on FISA information to federal, state, local, and tribal officials and agencies.[21] First, the Proposed FBI SMPs revise the description of what information the FBI may

---

[19] Notwithstanding other provisions of these minimization procedures, information that is not foreign intelligence information, but reasonably appears to be evidence of a crime that has been, is being, or is about to be committed, may be retained and disseminated (including United States person identities) to the FBI and other appropriate federal law enforcement authorities, in accordance with [50 U.S.C. §§ 1806(b) and 1825(c)], Executive Order No. 12333 (as amended), and other applicable crimes reporting requirements or procedures.

NCTC SMPs § A.7, at 4.

[20] For ease of reference, the agency handling information will generally be referred to as "the FBI," even when the discussion pertains equally to NCTC when operating under the corresponding provision of its proposed procedures.

[21] With regard to foreign governments, the Proposed FBI SMPs explicitly provide for dissemination of evidence of a crime for law enforcement purposes, in addition to foreign intelligence disseminations. See Proposed FBI SMPs § IV.C, at 28-30. The Court finds this provision to be reasonable and in conformance with Section 1801(h), and makes the same

(continued...)

disseminate to federal, state, local, and tribal recipients. Under the Proposed FBI SMPs, the FBI may disseminate "FISA-acquired information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information or assess its importance." Proposed FBI SMPs § IV.A, at 27 (emphasis added). The corresponding provision of the 2008 FBI SMPs refers only to "FISA-acquired information that reasonably appears to be foreign intelligence information." 2008 FBI SMPs § IV.A, at 27.[22] The Court finds that this revision is reasonable and comports with Section 1801(h)(1)-(2), and makes the same finding with regard to the corresponding language in the NCTC SMPs. See NCTC SMPs § D.1, at 8.[23]

The Proposed FBI SMPs also expand the range of federal, state, local, and tribal recipients to whom such foreign intelligence disseminations may be made. The 2008 FBI SMPs state that the FBI may make such disseminations "to federal, state, local and tribal officials and agencies with responsibilities directly related to the information proposed to be disseminated." 2008 FBI SMPs § 4.A, at 27 (emphasis added).[24] In contrast, the Proposed FBI SMPs permit foreign intelligence disseminations to "federal, state, local and tribal officials and agencies with responsibilities relating to national security that require access to foreign intelligence information." Proposed FBI SMPs § IV.A, at 27 (emphasis added).

---

[21](...continued)
finding with regard to the corresponding provision of the NCTC SMPs. See NCTC SMPs § D.3, at 8-9.

[22] A separate provision addresses dissemination of evidence of a crime to federal, state, local, and tribal officials and remains unchanged. See 2008 FBI SMPs § IV.B, at 28; Proposed FBI SMPs § IV.B, at 28.

[23] The amendments to the FBI procedures also change certain references to "dissemination" of information to "disclosure" of information. Compare, e. g., 2008 FBI SMPs § IV.D, at 30 with Proposed FBI SMPs § IV.D, at 30. The government advises that this change in terminology is not intended to alter the substance of these provisions. See April 23, 2012 Submission at 26 n.16.

[24] Section IV.A of the 2008 FBI SMPs further provides that "[i]nformation that reasonably appears to be foreign intelligence information not directly related to responsibilities of such agencies may be disseminated incidental to the dissemination of information [that is] directly related" to those responsibilities. (Emphasis added.) This language is stricken by the proposed amendments to the FBI procedures and rendered superfluous by the expanded dissemination standards sought by those amendments.

This expansion of recipients implicates Section 1801(h)(1)'s requirement of "specific procedures . . . that are reasonably designed . . . to 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" (emphasis added). While both versions of Section IV.A contain a general statement that "information may be disseminated only consistent with [such] need," the 2008 FBI SMPs contain a specific requirement that serves to ensure that authorized disseminations are responsive to that need – namely, that the recipients have responsibilities that are directly related to the information they receive. Under the Proposed FBI SMPs, the required nexus between recipient and information is more general – the receiving official need only have "responsibilities relating to national security that require access to foreign intelligence information," not further specified. Thus, for example, the duties of a Coast Guard official may include guarding against a waterborne terrorist attack, which would constitute national security-related responsibilities that require access to certain categories of foreign intelligence information, as defined at Section 1801(e)(1)(A)-(B); however, those duties might bear no relation to intelligence about a cabinet re-shuffling in a foreign government, even though such information could qualify as foreign intelligence information under Section 1801(e)(2)(B). The difference between foreign intelligence information that directly relates to an official's responsibilities, and foreign intelligence information generally, is likely to be especially pronounced for state, local, and tribal officials, whose responsibilities will typically be limited to a particular jurisdiction, as well as by subject matter.

The government justifies this revision as necessary for the FBI to ensure that foreign intelligence information reaches all governmental personnel with a legitimate need for it. The 2008 FBI SMPs implicitly assume that FBI personnel can and will identify those officials across the federal government, and within state, local, and tribal governments, who have a need for particular foreign intelligence information. Declaration of Eric Velez-Villar, Assistant Director, Directorate of Intelligence, FBI ("FBI Declaration"), at 6-7, attached as Exhibit D to the April 23, 2012 Submission. But the FBI's ability to do so is limited. Sometimes, FBI personnel may be unaware that a particular agency or office has a legitimate need for information on a given subject. FBI Declaration at 9-11. On other occasions, FBI personnel may not, at the time of dissemination, have fully ascertained the significance of a piece of information. Id. at 11. In either case, the distribution list formulated by the FBI will be under-inclusive.

The government contrasts this mode of dissemination, in which an analyst "pushes" reporting out to particular recipients, with disseminations in which recipients have access to a body of reporting, stored on classified information repositories, and "pull" out of it particular information that they identify as responsive to their current needs. April 23, 2012 Submission at 46-47. Intelligence agencies in recent years have increasingly employed the "pull" model of dissemination. See FBI Declaration at 5-7. The government contends that intelligence consumers are better acquainted with their information needs than the originators of the reports

that are uploaded onto these information repositories. April 23, 2012 Submission at 49-50. The risk of under-inclusive distribution is therefore reduced. The government further points to

> the substantial added benefit of allowing users to enter a search, review the results of that search, and assess each piece of information in the context of the others. This is essential to analysts' ability to discern connections between data points and understand the relevance of facially disparate reports . . . . Thus, in addition to permitting wider sharing of information, the proposed dissemination standard would also permit recipients to make more effective use of that information.

NCTC Declaration at 14.

As for non-federal recipients of information, the government notes that "[s]tate, local and tribal governments are considered critical partners in national counterterrorism efforts," including "dissemination of information and intelligence." Id. at 3. The government further asserts that, although the need to disseminate foreign intelligence information to such governments occurs most frequently in counterterrorism cases, it is not limited to counterterrorism. "Indeed, state, local, and tribal officials are engaged, for example, in cybersecurity and weapons of mass destruction (WMD) preparedness. They also regulate, police, or otherwise interact with sites containing nuclear, radiological, chemical, or biological hazards." FBI Declaration at 17. These threats do not "fall exclusively under counterterrorism." Id.

The Court is persuaded that exclusive reliance on a "push" model of dissemination involves a substantial risk of under-inclusion and could impede analysts' efforts to assemble fragments of information from different sources into a coherent whole. These disadvantages significantly militate against a finding that FISA can countenance only this manner of disseminating intelligence reporting. Cf. In Re Sealed Case, 310 F.3d 717, 743 (FISC Rev. 2002) (per curiam) ("effective counterintelligence, we have learned, requires the wholehearted cooperation of all the government's personnel who can be brought to the task"). But that is not the end of the Court's analysis. Having recognized a foreign intelligence need to allow for "pull" disseminations to federal, state, local, and tribal officials, the Court must assess under Section 1801(h)(1) whether the government's proposal is reasonably designed to prohibit the dissemination of U.S. person information, consistent with that need.

First, the Court is mindful that the information in question is not raw FISA information. Rather, insofar as it concerns U.S. persons, information disseminated under this provision will at a minimum have been determined to "reasonably appear[ ] to be foreign intelligence information or [to be] necessary to understand foreign intelligence information or assess its importance." Proposed FBI SMPs § IV.A, at 27. While it is not permissible to disseminate any foreign intelligence reporting to any conceivable recipient, U.S. person information contained within

finished reporting is likely to be less sensitive than U.S. person information embedded within raw FISA information, and may properly be disseminated in a range of circumstances. Moreover, it is noteworthy that the balance that the government seeks to strike for operational and security reasons – achieving broad availability of information needed by trusted users to perform their jobs, while avoiding unwarranted access by other persons or for other purposes – is at least roughly comparable to FISA's goal of restricting disseminations of U.S. person information to cases where there is a foreign intelligence or law enforcement need.

The Court also finds helpful the government's explanation of how "pull" disseminations are effected in practice. Access to such systems is limited "to those users (a) who have the necessary security clearance, (b) whose agency has determined that they require access to particular systems to fulfill their work responsibilities, and (c) who retrieve specific disseminated products in response to queries in the course of their official duties." FBI Declaration at 7-8.[25] In the judgment of the Office of the Director of National Intelligence, "it is reasonable to conclude that the decision" to grant access to such a system is based on a "need to access the information in those systems . . . to fulfill a national security-related responsibility." April 23, 2012 Submission at 48. The FBI, for its part, will decide on an individualized basis which information repositories should receive a particular intelligence product, based on an analysis of factors such as "the sensitivity of the information, . . . U.S. person privacy concerns, . . . and the value of the information." FBI Declaration at 16.

In the Court's view, it is important that there be effective protections against indiscriminate or otherwise improper accessing of information concerning U.S. persons on these systems. Avoiding such practices is the difference between a system of dissemination that is no broader than necessary for full exploitation of foreign intelligence information and one that permits unwarranted disseminations. At the same time, however, the Court recognizes that the potential recipients of such disseminations are scattered across a large number of agencies at various levels of government. It would be awkward, if not unworkable, to regulate the behavior of all potential recipients through minimization procedures that are predominantly directed at the FBI and NCTC. In view of these considerations, the Court is prepared to rely on the government's representations of how FISA information will be disseminated on these classified information systems in its assessment of the proposed dissemination provisions.

---

[25] See also id. at 11 (referring to "rules requiring users to only use systems in fulfillment of their official duties"); NCTC Declaration at 13 ("searchable repositories . . . generally are subject to access policies that require users to use systems only in fulfillment of their official duties. Individuals' use of these systems is also generally subject to audit.").

For these reasons, and based on the representations summarized above, the Court finds that Section IV.A of the Proposed FBI SMPs, and the corresponding provision at Section D.1 of the NCTC SMPs, satisfy the requirements of 50 U.S.C. § 1801(h)(1)-(2). In view of the Court's reliance on factual representations that are extrinsic to the procedures themselves, the government is directed to report on the implementation of this authorization of "pull" disseminations. See infra p. 21.

B. Other Amendments to the FBI SMPs (and Corresponding Provisions of the NCTC SMPs)

Categories of Sensitive Information: Section III.C.3 of the 2008 FBI SMPs requires FBI personnel to continually analyze collection results and establish case-specific categories of non-pertinent information. The government is also required to describe these categories in renewal applications. The proposed amendment would eliminate these requirements in favor of emphasizing the need for particular care in reviewing identified categories of sensitive information (e. g., information about religious, educational, and political activities of U.S. persons) and to prohibit the use of sensitive information in an analysis or report unless it reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or evidence of a crime. See Proposed FBI SMPs § III.C.3, at 14-15. The current practice of generating case-specific categories is not legally required, so long as there are other safeguards for U.S. person information that bring the procedures into compliance with Section 1801(h). Because such safeguards are present, the Court has no difficulty in approving this amendment, as well as the corresponding provision of the NCTC SMPs. See NCTC SMPs § C.5, at 7.

FISC Role in Extension of Retention Periods: The 2008 FBI SMPs provide that the retention periods for unreviewed information, as well as for reviewed information that has not been found to be pertinent, may be extended if "specific authority is obtained from an Assistant Director of the FBI (AD)," the Department of Justice's National Security Division (NSD), and the Foreign Intelligence Surveillance Court (FISC). See 2008 FBI SMPs § 3.G.1.a-b, at 25-26. The proposed amendments would permit such extensions if "specific authority is obtained from an Assistant Director of the FBI (AD) and NSD to retain the material, and the FISC approves a new retention period upon a finding that such modification is consistent with the applicable statutory definition of 'minimization procedures.'" See Proposed FBI SMPs § 3.G.1.a-b, at 24-25. Because the new language merely describes more precisely the Court's statutory role in

reviewing minimization procedures, the Court approves this amendment, as well as the corresponding provision of the NCTC SMPs. See NCTC SMPs § B.2.a-b, at 5.[26]

[redacted] *Certain Privileged Communications*: The 2008 FBI SMPs have detailed requirements for handling attorney-client communications in various contexts. In cases where a target is under federal criminal charges, the FBI is required to establish a team of persons who have no role in the prosecution to conduct the initial review of acquired information. See 2008 FBI SMPs § III.E.1.a, at 17. As soon as that review team identifies "a privileged communication concerning the charged criminal matter between the target and the attorney representing the target in that matter," the FBI is required [redacted] to "ensure that whenever any user reviews information or communications acquired from that search or surveillance, which are in an FBI electronic and data storage system containing raw FISA-acquired information, he receives electronic notification that attorney-client communications have been acquired during the search or surveillance," so that other users know "that they may encounter privileged communications." Id. § III.E.1.e, at 18-19. In other cases involving the acquisition of communications between a client under criminal charges and an attorney representing the client in that matter, the FBI is required, at a minimum, to implement procedures [redacted] implements an electronic notification process of the type described above. Id. § III.E.2.a-b, d, at 19-20. The Proposed FBI SMPs retain all of these protections.

The 2008 FBI SMPs also require that, when the FBI determines that an attorney-client communication within one of the above-described categories has been identified, the FBI shall

---

[26] When these FBI retention periods were first approved in 2008, the Court permitted the FBI to "treat any information acquired pursuant to [previous orders] as if that information" had been found to be pertinent, provided that such information previously "had been marked 'pertinent' in FBI systems, or had otherwise been found to meet the logging or indexing standards of the FBI standard minimization procedures previously applicable to such information." FBI SMPs Opinion at 11. The Court approved this approach in view of the "undoubted burdens that a comprehensive re-review [of information reviewed before November 2008] would involve." Id. at 6. The government has not proposed any change in this way of handling information reviewed before November 1, 2008. Without comparable relief, this information would present the same practical difficulties under the corresponding provision of the Proposed FBI SMPs. Accordingly, the Court approves treating information reviewed before November 2008 in the same manner as was approved in the FBI SMPs Opinion.

[redacted] the Court finds that these provisions, as a whole, provide adequate protection for privileged communications in criminal matters.[27]

* * *

For the foregoing reasons, the Court finds that the Proposed FBI SMPs and the NCTC SMPs, implemented in the manner described in the April 23, 2012 Submission, in conjunction with any case-specific minimization procedures applicable under prior orders that reference the 2008 FBI SMPs, satisfy the definitions of "minimization procedures" at 50 U.S.C. §§ 1801(h) and 1821(4).

It is accordingly ORDERED that:

(1) Effective May 18, 2012, all prior orders of the FISC that authorized the FBI to conduct electronic surveillance or physical search, and all prior orders of the FISC that authorized acquisitions of foreign intelligence information under 50 U.S.C. § 1881c and that approved the use of the dissemination provisions of the 2008 FBI SMPs (collectively "Prior Orders"), are amended as follows:

(a) Subject to the exceptions and modifications specified in subparagraphs (b) through (f) below: (i) the FBI's acquisition, retention, and dissemination of information acquired pursuant to Prior Orders shall be governed by the Proposed FBI SMPs, in lieu of the 2008 FBI SMPs; and (ii) NCTC's retention and dissemination of information acquired

---

[27] The attorney-client provisions of the proposed NCTC procedures are significantly different from those in the FBI procedures. For example, when NCTC encounters a privileged communication between a criminal defendant and his attorney in that matter, monitoring of the communication will cease and "[t]he relevant portion of the tape, document, or other material . . . will be placed under seal or otherwise sequestered within NCTC data repositories and NSD will be notified so that appropriate procedures may be established," [redacted] See NCTC SMPs § C.6, at 7. Given that NCTC personnel are much less likely than FBI personnel to be active participants in criminal investigations and prosecutions, the Court finds that the NCTC attorney-client procedures to be reasonable and appropriate for that agency.

pursuant to the Prior Orders shall be governed by the NCTC SMPs, in lieu of the NCTC minimization procedures approved in Docket No [redacted] Minimization requirements of Prior Orders, other than those requirements embodied in the 2008 FBI SMPs or the NCTC minimization procedures approved in Docket No. [redacted], shall remain in effect in accordance with the terms of those Prior Orders.

(b) For purposes of calculating retention periods pursuant to NCTC SMPs § B.2, Prior Orders that expired before May 18, 2012, shall be deemed to have expired on May 18, 2012. For purposes of calculating retention periods pursuant to Proposed FBI SMPs § III.G, Prior Orders that expired before November 1, 2008, shall be deemed to have expired on November 1, 2008.

(c) The FBI may treat any information acquired pursuant to Prior Orders as if that information reasonably appeared to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime, provided that, prior to November 1, 2008, such information had been marked "pertinent" in FBI systems, or had otherwise been found to meet the logging or indexing standards of the FBI standard minimization procedures previously applicable to such information.

(d) This amendment of Prior Orders does not authorize sharing of un-minimized information acquired before January 1, 2001, with CIA or NSA pursuant to the minimization procedures approved in Docket Number [redacted] or with NCTC pursuant to the minimization procedures approved herein.

(e) Certain FBI data storage systems shall remain exempt from the marking requirements of Section III.B.5 and Section III.C.1 of the Proposed FBI SMPs, and from the electronic notification requirements of Section III.E.1.e and Section III.E.2.d of the Proposed FBI SMPs, as described and explained in the FBI SMPs Opinion at 7-9, 11-12.

(f) As is currently the case under the 2008 FBI SMPs, the government is not required to conduct minimization briefings as described by Section V.C of the Proposed FBI SMPs pursuant to Prior Orders issued before November 1, 2008. See FBI SMPs Opinion at 6, 10.

(2) The amendment described in paragraph (1) is effective as of May 18, 2012. Actions taken prior to that date with respect to information acquired pursuant to Prior Orders shall remain governed by, and evaluated under, the minimization procedures applicable to that information at the time that action was taken.

(3) Henceforward, NCTC shall apply the NCTC SMPs approved herein to information it has received from the FBI pursuant to Docket No. [redacted], in lieu of the minimization procedures for NCTC previously approved by the FISC in Docket No. [redacted]

(4) The government shall describe how foreign intelligence information has been disseminated, pursuant to the procedures approved herein, to federal, state, local, and tribal recipients under circumstances where such recipients have been granted the ability to access information that is not directly related to their responsibilities ("'pull' disseminations," as described supra at pages 14-16). Such a description shall be provided in the report to be submitted to the Court pursuant to Section VII of the Proposed FBI SMPs and in the report to be submitted to the Court pursuant to Section G of the NCTC SMPs.

(5) In addition, and separate from the reports described in paragraph (4) above, the government shall promptly report to the Court in writing any material change in, or deviation from, the controls and policies governing how other federal, state, local or tribal recipients access FBI or NCTC reporting that includes FISA information concerning U.S. persons via "pull" disseminations, as those controls and policies have been represented to the Court in this matter.

ENTERED at 1:30 p.m. on this 18th day of May, 2012.

Mary A. McLaughlin

MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court