

~~TOP 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

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...)

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

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).

TOP SECRET//COMINT//NOFORN

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...)

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

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

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

50 U.S.C. § 1801(h) (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 Liepmann, 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] [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

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]

[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]

[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. ██████████. Minimization requirements of Prior Orders, other than those requirements embodied in the 2008 FBI SMPs or the NCTC minimization procedures approved in Docket No. ██████████, 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 ██████████ 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.

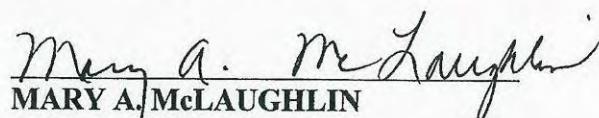
~~TOP SECRET//COMINT//NOFORN~~

(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
Judge, United States Foreign
Intelligence Surveillance Court

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

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