~~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)

I. 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 (b)(1); (b)(3); (b)(7)(A); (b)(7)(E) FBI conducted two simultaneous large, wide-ranging, and rapidly developing counterterrorism investigations, (b)(1); (b)(3); (b)(7)(A) [14] These investigations involved Court-authorized electronic surveillance and physical search of multiple targets and facilities.

[14] (b)(1); (b)(3); (b)(7)(A); (b)(7)(E)

(S//NF)

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]

[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 Numbe*[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

b(6) and b(7)(C)

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