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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

MEMORANDUM OPINION

This matter is before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on the "Government's Ex Parte Submission of [redacted] and Related Procedures, Ex Parte Submission of [redacted], and Request for an Order

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

Approving [redacted]," which was filed on July 31, 2012 ("July 31 Submission"). For the reasons set forth below, the government's request for approval is granted in part. In summary, the Court finds that the certifications included as part of the July 31 Submission contain all the required statutory elements and that the targeting and minimization procedures adopted for use in connection with those certifications are consistent with the applicable statutory requirements and the Fourth Amendment. However, in light of a recently-disclosed compliance incident that is still being investigated by the government, the Court is unable to complete its review of the amendments to previously-approved certifications that are included as part of the July 31 Submission. Therefore, in a separate order entered pursuant to 50 U.S.C. § 1881a(j)(2), the Court is granting the government's request for an extension of the time in which the Court must complete its review of the amendments.[1]

I. BACKGROUND

The July 31 Submission includes [redacted] certifications that have been executed by the Attorney General ("AG") and the Director of National Intelligence ("DNI") pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which is codified at 50 U.S.C. § 1881a[redacted] Each [redacted] accompanied by the supporting affidavits of the Director of the National Security Agency ("NSA"), the Director of the Federal

[1] See 50 U.S.C. § 1881a(i)(1)(B)-(C) (requiring the Court to complete its review and issue an order within 30 days after the date on which a certification or amendment is submitted).

Bureau of Investigation ("FBI"), and the Director of the Central Intelligence Agency ("CIA"); two sets of targeting procedures, for use by NSA and FBI respectively; and four sets of minimization procedures, for use by NSA, FBI, CIA, and the National Counterterrorism Center ("NCTC"), respectively.

Like the acquisitions approved by the Court in all prior Section 702 dockets, collection under [redacted] will be limited to "the targeting of non-United States persons reasonably believed to be located outside the United States." [redacted]

[redacted]

[redacted]

II. REVIEW OF [redacted]

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

(1) [redacted] been made under oath by the AG and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see [redacted]

(2) [redacted] each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see [redacted]

(3) as required by 50 U.S.C. § 1881a(g)(2)(B), each [redacted] accompanied

---

[2] The July 31 Submission also includes amendments to the [redacted] been submitted by the government and approved by the Court in all prior Section 702 dockets. See [redacted] (collectively, the "Prior 702 Dockets"). The amendments, which have been authorized by the AG and the DNI, provide that information collected under the certifications in the Prior 702 Dockets will, effective upon the Court's approval, be handled subject to the same minimization procedures that have been submitted for use in connection with [redacted] As noted above and discussed further below, a recently-disclosed compliance incident that is still being investigated by the government will preclude the Court from completing its review of these amendments without further development of the record. Accordingly, the Court is issuing a separate order granting the government's motion for an extension of time in which the Court must complete its review of the pending amendments to previously-approved certifications.

by the applicable targeting procedures[3] and minimization procedures;[4]

(4) [redacted] supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);[5] and

(5) [redacted] an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D), see [redacted][6]

The Court therefore finds that [redacted] all the required statutory elements. 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is required to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). See 50 U.S.C. § 1881a(i)(2)(B) and (C). Section 1881a(d)(1) provides that the targeting procedures must be "reasonably designed" to "ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all

---

[3] The NSA and FBI targeting procedures are attached [redacted] as Exhibits A and C, respectively.

[4] The NSA, FBI, CIA, and NCTC minimization procedures are attached [redacted] as Exhibits B, D, E, and G, respectively.

[5] See Affidavits of General Keith B. Alexander, Director, NSA (Tab 1 [redacted]; Affidavits of Robert S. Mueller, III, Director, FBI (Tab 2 [redacted]; and Affidavits of John O. Brennan, Director, CIA (Tab 3 [redacted].

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

intended recipients are known at the time of the acquisition to be located in the United States." Section 1881a(e)(1) requires that the minimization procedures "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4)," which is set out in full in Subpart C below. Finally, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A).

A. The NSA Targeting Procedures.

The NSA targeting procedures included as Exhibit A to the July 31 Submission are identical to the corresponding procedures that were approved by the Court in 2012. Nevertheless, one issue requires discussion. On [redacted] 2013 – well after the start of the 30-day time period within which the Court must complete its review of the July 31 Submission, see 50 U.S.C. § 1881a(i)(1)(B)-(C) – the government reported a compliance incident involving the post-targeting review that NSA conducts to ensure that telephone numbers tasked under Section 702 continue to be used by non-United States persons who are reasonably believed to be located outside the United States. The disclosure of this compliance problem complicates the Court's review of the July 31 Submission.

By way of background, since the government first implemented its authority under Section 702 in 2008, the NSA targeting procedures have stated that, for telephone numbers, NSA's post-targeting review [redacted] the following checks:

[redacted]

[redacted]; see also July 31 Submission, [redacted].

[redacted] the government has previously assured the Court [redacted] "[t]he checks are done for each selector;" [redacted] "[t]he results of these [redacted] checks are reviewed by experienced analysts [redacted] The Court has expressly relied upon these assurances in concluding that NSA's targeting procedures are reasonably designed to ensure that targeting is limited to non-U.S. persons reasonably believed to be located outside the United States and consistent with the Fourth Amendment. See Docket No. 702(g)-08-01, Sept. 4, 2008 Mem. Op. at 11, 16, 19.

On [redacted] 2013, the government submitted a Preliminary Notice of Compliance Incident disclosing a problem with NSA's [redacted] post-targeting checks for telephone numbers [redacted] Notice"). A subsequent notice filed on [redacted] 2013, provides additional information on the subject [redacted] Notice"). Together, the two notices explain that [redacted]

[redacted]

[redacted]

[redacted]

At the [redacted] hearing, the government provided additional information regarding NSA's [redacted] 2013 "fix" [redacted]

[redacted]

Based on the information that has been provided by the government to date, the Court is satisfied that NSA is prepared to comply – and will, in fact, comply – with the "Post-Targeting Analysis" provisions of the NSA minimization procedures with respect to the information that will be acquired pursuant to the [redacted] Accordingly, the noncompliance problem discussed above does not preclude the Court from finding, for purposes of the 2013 certifications, that NSA's targeting procedures are "reasonably designed" to "ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of

any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." See Section 1881a(d)(1).[7]

---

[7] As noted above, however, NSA's past noncompliance with the post-tasking analysis requirements of its targeting procedures substantially affects the Court's review of the amendments to the prior Section 702 certifications that are included as part of the July 31 Submission. As a result of the noncompliance, NSA likely failed altogether to detask certain facilities that were no longer eligible for Section 702 collection, and it likely failed to detask others in a timely fashion. Those failures, in turn, likely resulted in NSA's acquisition of communications falling outside the scope of Section 702, as NSA no longer had a reasonable belief that the users of such facilities were located outside the United States. See [redacted] Notice at 2-3 (disclosing [redacted]). It is also likely that other communications – [redacted] were not properly identified by NSA as "domestic communications," which generally are subject to prompt deletion under NSA's minimization procedures, but were instead incorrectly retained in NSA's systems as "foreign communications." See, e.g., [redacted] NSA Minimization Procedures) at 7 (§ 3(c)(1)) (rules for retention of raw data); id. at 8-10 (§ 5) (rules for retention of domestic communications); id. at 10-13 (§§ 6-7) (rules for handling foreign communications).

The government is still investigating these matters, and the record concerning them remains incomplete. Accordingly, the Court cannot complete its required review of the amendments at this time. Until the scope of the past overcollection is determined, it will, for example, be difficult for the Court to assess whether, for purposes of information acquired under past certifications, NSA's revised minimization procedures meet FISA's definition of minimization procedures, which requires, among other things, "specific procedures" that are "reasonably designed . . . to minimize the . . . 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). Furthermore, because the acquisition of telephone communications to or from persons located inside the United States is likely to constitute "electronic surveillance" within the meaning of Section 1801(f), any overcollection resulting from NSA's noncompliance with its targeting procedures implicates FISA's prohibition on the use or disclosure of information with knowledge or reason to know that such information was obtained through unauthorized electronic surveillance. See 50 U.S.C. § 1809(a)(2). To permit full consideration of these issues on a complete record, the Court is entering a separate order granting the government's motion for an extension of the time in which the Court must complete its review of the amendments.

B. The FBI Targeting Procedures.

The FBI targeting procedures included as part of the [redacted] submission differ in two respects from the corresponding procedures that have previously been approved by the Court. Both changes concern the FBI's process for determining whether or not an electronic communications account is appropriate for targeting [redacted] i.e., that the account is not used by any United States person or any person located inside the United States.

[redacted]

[redacted]

Thus, before the FBI targeting procedures are applied, NSA will have already determined through application of its own targeting procedures – which the Court has previously found meet the pertinent statutory requirements – that the user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States. See Amended FBI Targeting Procedures at 1 § I.1.

[redacted]

[redacted]

[redacted]

[8] As discussed elsewhere in this opinion, the government has recently disclosed a compliance problem concerning [redacted] post-tasking checks that NSA performs for [redacted] telephone numbers targeted under Section 702. It is the Court's understanding that there exists no similar problem for [redacted] post-tasking checks conducted by NSA for electronic communications accounts. See [redacted] Notice at 1.

[redacted]

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the revised FBI targeting procedures are reasonably designed: (1) to ensure that any acquisition authorized under [redacted] is limited to targeting persons reasonably believed to be located outside the United States, and (2) to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States, as required by Section 1881a(d).

C. The NSA, FBI, and CIA NCTC Minimization Procedures.

The Court must determine whether the minimization procedures included as part of the July 31 Submission meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) and 1821(4) with respect to acquisitions that will be made pursuant to the [redacted] See 50 U.S.C. § 1881a(j)(2)(C). The definitions at Sections 1801(h) and 1821(4) are substantively identical for present purposes and define "minimization procedures" in pertinent part as:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;[9]

---

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

(1) information that relates to, and if concerning a United States person is

(continued...)

> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

50 U.S.C. § 1801(h); see also id. § 1821(4).[10] For the reasons set forth below, the Court concludes that the minimization procedures accompanying the 2013 certifications satisfy this

---

[9](...continued)
necessary to, the ability of the United States to protect against –

> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

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

> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

[10] The definitions of "minimization procedures" set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to "the purposes . . . of the particular physical search") (emphasis added). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h)).

definition, as required by 50 U.S.C. § 1881a(e).

1. The NSA Minimization Procedures.

The government has made two noteworthy changes to the NSA minimization procedures, which are included as Exhibit B to the July 31 Submission. First, Section 6.b has been modified to clarify that the restrictions on the dissemination of information derived from foreign communications "of or concerning a United States person" apply not just to "report[s]," but also to disseminations in any form. See Amended NSA Minimization Procedures at 11. This change is consistent with Section 1801(h).

Second, Section 8(c), which provided rules for sharing unminimized data concerning [redacted] has been deleted. [redacted] The deletion of this provision, which would not by its terms apply to information collected pursuant to the 2013 Certifications, therefore poses no difficulty under Section 1801(h).

2. The FBI Minimization Procedures.

The only noteworthy change to the FBI minimization procedures included as Exhibit D to the July 31 Submission involves Section IV.H, which governs the dissemination of Section 702-acquired information concerning computer intrusion events to non-governmental parties. The

previously-approved version of Section IV.H permitted the FBI, in the event Section 702 information "reveals that a private entity or individual has been victimized by a computer intrusion event or is at risk of being [so] victimized," to "provide notice" to such entity or person "that their computer networks or systems have been compromised or are otherwise at risk of being compromised." See, e.g., [redacted] Exh. C (FBI Minimization Procedures) at 26 (§ IV.H). As revised, Section IV.H provides as follows:

> The FBI may disseminate FISA-acquired information that reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime and that it reasonably believes may assist in the mitigation or prevention of computer intrusions or attacks to private entities or individuals that have been or are at risk of being victimized by such intrusions or attacks, or to private entities or individuals (such as Internet security companies and Internet Service Providers) capable of providing assistance in mitigating or preventing such intrusions or attacks. Wherever reasonably practicable, such dissemination should not include United States person identifying information unless the FBI reasonably believes it is necessary to enable the recipient to assist in the mitigation or prevention of computer intrusions or attacks.

Revised FBI Minimization Procedures at 26-27 (§ IV.H).

The new language: (1) clarifies that disseminated information must constitute foreign intelligence information, be necessary to understanding foreign intelligence information or assess its importance, or consist of evidence of crime; (2) states that such information may be provided not only to victims of computer intrusions or attacks, but also to persons or entities capable of assisting in mitigating or preventing such attacks; and (3) expressly requires that, when practicable, United States person identifying information not be included in such disseminations unless it is deemed necessary to assist in mitigating or preventing an intrusion or attack. The

revised provision is identical to Section IV.H of the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act, which were most recently approved by the Court as amended on June 3, 2013 ("FBI SMPs"). The inclusion of the same language in the FBI's Section 702 minimization procedures raises no issue under Section 1801(h).

One additional issue warrants discussion. On [redacted] 2013, the government submitted a Notice of Compliance Incident Regarding Storage of Raw FISA-Acquired Information ([redacted] Notice") in which it reported potentially substantial noncompliance by the FBI with provisions of the FBI SMPs for electronic surveillance and physical search. Because the FBI minimization procedures for Section 702 contain similar provisions, the [redacted] Notice has potential implications here.

The FBI SMPs for electronic surveillance and physical search require, among other things, that FBI electronic storage systems have certain capabilities: for example, such systems must be able to track how personnel access raw data and record query terms that they use, see FBI SMPs §§ III.B.3, III.D, and to permit appropriate personnel to mark reviewed data as pertinent or non-pertinent, see id. § III.C. The FBI's section 702 minimization procedures contain similar corresponding provisions. See Amended FBI Minimization Procedures §§ III.B.3, III.C & III.D. The markings required by these provisions enable the FBI to implement access restrictions and destruction requirements that apply to raw information that has never been reviewed or that has been reviewed but not found pertinent. See, e.g., FBI SMPs § III.G.1.

In the [redacted] Notice, the government disclosed various types of FBI systems that:

> generally are not configured to apply the retention time limits to particular FISA-acquired information or the attorney-client privilege, or other, minimization markings. These systems also do not track queries or information that has been exported from these systems. And, except for [redacted], these systems generally do not log or track accesses. Furthermore, there are no FBI policies regarding the above systems containing raw FISA-acquired information, as required by the FBI SMPs.

[redacted] Notice at 3. These systems range from an individual laptop onto which an agent may download raw FISA-acquired information "in order to more easily manipulate and analyze the data," id. at 2, to [redacted] a system that is generally available within the FBI.

[redacted]

On [redacted] 2013, the Court issued an Order in Response to Notice of Non-Compliance Submitted on [redacted] 2013 ("[redacted] Order") addressing the government's disclosure of this problem and requiring additional action. The Court noted that "a widespread practice of storing raw FISA-acquired information in systems where access cannot be tracked . . . and . . . the applicable retention and destruction schedule cannot be effectively implemented would undermine central protections of U.S. person information under the FBI SMPs." [redacted] Order at 4. Because the government had "provided no information about how it proposes to address this concern," the Court ordered the FBI, by September 9, 2013, to

> . . . remove all FISA-acquired information from FBI electronic and data storage systems that do not comply with all applicable marking, auditing, and notification requirements[] of the FBI SMPs (hereinafter "non-compliant systems"), and thereafter [to] refrain from placing FISA-acquired information on non-compliant systems, except insofar as the FBI determines that storing, reviewing or analyzing

> particular FISA-acquired information on a non-compliant system is necessary to properly analyze that information for foreign intelligence.

Id. at 4-5 (footnote omitted; emphasis in original). As relevant here, the Court further ordered that the government be prepared to discuss the following questions (among others) at a hearing scheduled for [redacted] 2013:

> a. What is the current state of compliance of FBI electronic and data storage systems with all applicable marking, auditing, and notification requirements of the FBI SMPs (and corresponding provisions of the FBI minimization procedures for information obtained pursuant to 50 U.S.C. § 1881a)?
>
> b. What is the current state of the FBI's ability to implement the retention and destruction schedule set out at Section III.G.1 of the FBI SMPs (and corresponding provisions of the FBI minimization procedures for information obtained pursuant to 50 U.S.C. § 1881a)?

Id. at 5-6.

On [redacted] 2013, the government submitted a Supplemental Notice Regarding Storage of Raw FISA-Acquired Information by the FBI ("[redacted] Notice"), in which it clarified that the instances of noncompliance that were the subject of the [redacted] Notice were limited to information acquired pursuant to either Title I or III of FISA. See [redacted] Notice at 2. The [redacted] Notice further explained that the FBI stores raw Section 702-acquired information in [redacted exempt under b(7)E] compliant with the applicable minimization procedures. See id. at 1-2. The government has also informed the Court that, in its investigation of this matter to date, the Department of Justice's Office of Intelligence "has not identified instances of FISA Section 702-acquired information being stored in systems not compliant with the FBI [minimization procedures]." Id. at 2. According to the government, the FBI is in the process of

surveying field offices regarding the manner in which FISA-acquired information, including Section 702 information, is stored, and will provide updated information to the Court at or before the [redacted] 2013 hearing. Id.

In light of the information furnished by the government to date, the Court is satisfied the FBI is prepared to comply with the marking, auditing, and notification requirements of its Section 702 minimization procedures with respect to the information that will be acquired pursuant to [redacted] Accordingly, the noncompliance described in the [redacted] Notice does not preclude the Court from finding that the amended FBI minimization procedures meet the requirements of Section 1801(h).

3. The CIA Minimization Procedures.

The CIA minimization procedures included as Exhibit E to the July 31 Submission include only one noteworthy change. The government has added a new Section 1.d, which provides as follows:

> For purposes of these procedures, the terms "Central Intelligence Agency," "CIA," and "CIA personnel" refer to any employees of the CIA and any other personnel acting under the direction, authority, or control of the Director of the CIA, as well as to employees of other U.S. Government agencies who are physically located at CIA and who are granted access to CIA systems to perform duties in support of CIA operations, but who retain the authorities and responsibilities of their parent organization. Such personnel must specifically agree to: comply with these minimization procedures; comply with all CIA direction on the handling of information acquired under Section 702; and not make any use of, share, or otherwise disseminate any information acquired pursuant to Section 702 without specific CIA approval.

Amended CIA Minimization Procedures at 1. This provision merely clarifies that all personnel working in support of CIA operations are bound by the CIA minimization procedures, whether or

not they are actually employees of the CIA. Accordingly, it presents no issue under Section 1801(h).

4. TheNCTC Minimization Procedures

The NCTC Minimization Procedures attached as Exhibit G to the July 31 Submission are identical to the corresponding procedures approving the 2012 Certifications. For the same reasons the Court provided in approving the NCTC minimization procedures in 2012, the Court again finds that these procedures satisfy the requirements of Section 1801(h).

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

The final question before the Court is whether the targeting and minimization procedures, as applied to the information that will be acquired pursuant to [redacted] are consistent with the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A). The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the "foreign intelligence exception" to the warrant requirement of the Fourth Amendment. See Docket No. 702(i)-08-01, Sept. 4, 2008 Mem. Op. at 35-36. Hence, the question for the Court is whether the agency's targeting and minimization procedures, as implemented, are reasonable. See id. at 37. To determine whether a particular governmental action is reasonable, and thus permissible, under the Fourth Amendment, the Court must balance the governmental interests at stake against the degree of intrusion on Fourth Amendment-protected interests, taking into account the totality of the circumstances. See id. (citing cases).

The Court has previously recognized that the government's national security interest in

conducting acquisitions pursuant to Section 702 "'is of the highest order of magnitude.'" Id. at 37 (quoting In re Directives Pursuant to Section 105B of FISA, Docket No. 08-01, Opinion at 20 (FISA Ct. Rev. Aug. 22, 2008)).[11] On other side of the balance, the targeting procedures are, as discussed above, reasonably designed to target non-United States persons who are located outside the United States and who are therefore not protected by the Fourth Amendment. See id. (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)). Nevertheless, the Court has recognized that the government's collection under Section 702 includes the incidental acquisition of substantial quantities of information concerning United States persons and persons located inside the United States who are entitled to Fourth Amendment protection. See [redacted] Oct. 3, 2011 Mem. Op. at 72-74.

The Court concluded previously that the targeting and minimization procedures put forth by the government in 2011 and 2012 are adequate to protect the substantial Fourth Amendment interests that are implicated by the government's collection under Section 702, including the incidental acquisition of non-target information concerning United States persons and persons located in the United States. See [redacted] Nov. 30, 2011 Mem. Op. at 11-15; [redacted] 2012 Mem. Op. at 43-44. In sum, the Court determined that the 2011 and 2012 procedures contain various measures which, taken together, "tend to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States

[11] A declassified version of the opinion in In re Directives is available at 551 F.3d 1004 (FISA Ct. Rev. 2008).

will be used or disseminated" by the government and ensure that "non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary." See [redacted], Nov. 30, 2011 Mem. Op. at 13-14. The basic framework of protections formed by the previously-approved procedures remains intact. Accordingly, weighing the completing interests at stake, the Court is satisfied that the compliance problems and relatively minor changes discussed above do not individually or collectively preclude it from again finding that, for purposes of [redacted] the targeting and minimization procedures are consistent with the Fourth Amendment.

IV. CONCLUSION

For the foregoing reasons, the Court finds that [redacted] all the required statutory elements and that the targeting and minimization procedures adopted for use in connection with [redacted] consistent with 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment. An order approving [redacted] and the use of the accompanying procedures is being entered contemporaneously herewith.

ENTERED this 30th day of August 2013, in [redacted]

REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that [redacted] referenced above [redacted] the required statutory elements and that the targeting procedures and minimization procedures approved for use in connection with [redacted] consistent with the requirements of 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

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

ENTERED this 30th day of August 2013, at 2:45 p.m. Eastern Time, in [redacted]

[redacted]

REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

I, [redacted] Chief Deputy Clerk, FISC, certify that this document is a true and correct co[redacted]
June 13, 20[redacted] exempt under b(6) se