SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

Reporting Period: June 1, 2009 – November 30, 2009

May 2010

[redacted] b6

~~CL REASON: 1.4(c)~~
~~DECL ON: 20350326~~
~~DRV FROM: MET T 06~~

(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence

May 2010

Reporting Period: June 1, 2009 – November 30, 2009

(U) SECTION 1: INTRODUCTION

(U) The FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2438, now codified at 50 U.S.C. § 1881a (hereinafter "FAA"), requires the Attorney General and the Director of National Intelligence to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq*. (hereinafter "FISA"), as amended by the FAA, and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. As required by the Act, a team of oversight personnel from the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) have conducted compliance reviews to assess whether the authorities under Section 702 of FISA have been implemented in accordance with applicable procedures and guidelines, described below. This report sets forth DOJ and ODNI's third joint compliance assessment under Section 702 of FISA, as amended by the FAA, covering the period June 1, 2009, through November 30, 2009 (the "reporting period").[1]

(U) Section 702(l) of FISA, as amended by the FAA, provides:

> Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subjection (f) and shall submit each assessment to—
>
> (A) the Foreign Intelligence Surveillance Court; and
> (B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—(i) the congressional intelligence committees; and (ii) the Committees on the Judiciary of the House of Representative and the Senate.

(U) The targeting procedures referred to in subsection (d) are procedures that the Attorney General must adopt, in consultation with the Director of National Intelligence, "that are reasonably designed to (A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (B) prevent the intentional

[1] (U) This report accompanies the Semiannual Report of the U.S. Department of Justice Concerning Acquisitions under Section 702 of the FISA, which is submitted pursuant to Section 707 of FISA, as amended by the FAA, and covers the same reporting period.

acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." Section 702(d) (2) requires that these procedures be reviewed by the FISC.

(U) The minimization procedures referred to in subsection (e) must also be adopted by the Attorney General in consultation with the Director of National Intelligence. They must meet the definition of "minimization procedures" under Section 101(4) or 301(4), as appropriate, of FISA.[2] They must also be reviewed and approved by the FISC.

(U) The guidelines referred to in subsection (f) similarly must be adopted by the Attorney General, in consultation with the Director of National Intelligence. The purpose of these guidelines is to ensure compliance with the limitations set forth in Section 702(b), which are as follows:

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

---

[2] (U) Section 101(h) provides:

"Minimization procedures", with respect to electronic surveillance, means--
(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, 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;
(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (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;
(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; and
(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a) [50 USCS § 1802(a)], procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 [50 USCS § 1805] is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

These guidelines, the Attorney General's Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (the Attorney General's Acquisition Guidelines), were adopted by the Attorney General in consultation with the Director of National Intelligence on August 5, 2008.

[redacted] b1

[redacted] b1

[redacted] b1

[redacted] b1

(U) As with the prior joint assessments, this joint assessment first provides a description of the process by which the authorities granted under Section 702 are implemented. It then describes the conduct of the compliance assessments themselves – explaining the methodology used by the joint DOJ and ODNI team to review the measures being used to implement the authorities – and assesses compliance with the procedures and guidelines. These descriptions are necessary to provide context for the findings.

~~(U//FOUO)~~ This assessment finds that during the reporting period, the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The compliance incidents for the reporting period are described in detail in the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of FISA, March 2010, submitted as required by Section 707(b)(1) of FISA, as amended by the FAA (the "Section 707 Report"). As with the prior joint assessments, those compliance incidents are analyzed here to determine whether there are patterns or trends that might indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented measures to prevent recurrences. First, as in the prior joint assessment reports, it should be noted that the joint oversight team has not found indications in these compliance incidents of any intentional or willful attempts to violate or circumvent the requirements of the Act. Second, the number of compliance incidents remains small, [redacted] Third, certain types of compliance incidents continue to occur, indicating the need for continued focus on measures to address underlying causes, including the potential need for additional measures. The oversight team is continuing to evaluate the manner in which it conducts oversight to find areas to make oversight more efficient and effective. b1

(U) SECTION 2: IMPLEMENTATION OF SECTION 702 AUTHORITIES - OVERVIEW

[redacted] b1

~~(S)~~ I. Overview - NSA

~~(TS//SI//NF)~~ NSA seeks to acquire foreign intelligence information concerning specific targets [redacted] from or with the assistance of electronic communication service providers, as defined in section 701(b)(4) of FISA, as amended by the FAA.[4] As required by b1

[4] (U) Specifically, Section 701(b)(4) provides:

> The term 'electronic communication service provider' means -- (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code; (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code; (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

Section 702, those targets must be non-United States persons[5] reasonably believed to be located outside the United States. [redacted]

b1

~~(S)~~ [redacted]

b3

[redacted]

b1

~~(TS//SI//NF)~~ Once information is collected [redacted], it is subject to FISC-approved minimization procedures. NSA's minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. [redacted]

b1

[5] (U) Section 101(i) of FISA defines "United States person" as follows:

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

[redacted]

b1

[redacted]

b3

[redacted] b1

~~(S)~~ NSA's targeting procedures address, among other subjects, the manner in which NSA will determine that a person targeted under Section 702 is a non-United States person reasonably believed to be located outside the United States, [redacted] and the documentation required. b1

(U) A. Location.

~~(S)~~ The procedures provide that NSA's targeting determinations should be made in light of the totality of the circumstances based on the information available [redacted] b1 b3

[redacted] [10] b1

[8] [redacted] b3

[9] ~~(S)~~ NSA has developed a list of factors to facilitate training and tasking for its analysts to use when identifying [redacted] and meeting documentation requirements under the "totality of the circumstances" requirement. [redacted] b1

[10] [redacted]

[redacted]

[redacted] [11] b1 b3

[redacted]

[redacted] [13] b1 b3

---

[11] [redacted] b1

[12] [redacted]

[13] [redacted]

(U) B. United States Person Status.

~~(S)~~ With respect to the United States person status [redacted], the procedures provide that, in many cases, the information NSA reviews [redacted] may also give some indication as to whether the individual is a non-United States person. [redacted] b1

[redacted] b3

[redacted] b1

~~(S//SI//~~[redacted] b3

---

[14] [redacted] b1

[redacted]

b1

[redacted]

b3

[redacted]

b1

(U) E. Documentation.

~~(S)~~ [redacted] The citation is a reference that identifies the source of the information, [redacted], enabling oversight personnel to locate and review the information that led the analyst to his/her reasonable belief. [redacted]

b3

[redacted]

b1

[redacted] b1

[redacted] b3

~~(S)~~ The source records cited [redacted] sheets are contained in a variety of NSA data repositories. These records are retrieved by NSA, when requested by the DOJ/ODNI oversight team, to verify determinations [redacted]

[redacted] b1

[redacted]

[redacted] b3

(U) G. Oversight and Compliance.

~~(S)~~ The procedures require that NSA's Signals Intelligence Directorate (SID), together with NSA's Office of General Counsel (OGC), provide training on the procedures. They further provide that SID Oversight and Compliance will conduct oversight activities and make any necessary reports, including those relating to incidents of non-compliance, to the NSA Inspector General and NSA's OGC, and will ensure that necessary corrective actions are taken to address any identified deficiencies. SID Oversight and Compliance conducts spot checks of targeting decisions and

disseminations to ensure compliance with procedures. In December 2009, NSA deployed updated and improved platform-based training, which includes a competency test, for Section 702 and Protect America Act (PAA) data, some of which is still retained by NSA. Information on the NSA internal web site is updated by SID Oversight and Compliance as appropriate regarding implementation of Section 702 authorities.

~~(S)~~ NSA has instituted internal training programs, access control procedures, standard operating procedures, compliance incident reporting measures, and similar processes to implement the requirements of the targeting procedures. Only analysts who have received certain types of training and authorizations are provided access to the Section 702 program data. They must review an NSA OGC training program; [redacted] and must take an examination. The databases NSA analysts use are subject to audit/review by SID Oversight and Compliance, as well as by the NSA's Office of Inspector General (OIG). They may consult standard operating procedures for guidance, as well as supervisors, SID Oversight and Compliance personnel, NSA OGC attorneys, and the NSA Office of Compliance. b1

~~(S)~~ In addition, the procedures provide that DOJ and ODNI will conduct oversight of NSA's exercise of authority under Section 702 of the Act, including periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures at least once every sixty days (further discussed below).

~~(S)~~ The procedures call for NSA to report to DOJ and ODNI any incidents of non-compliance with the procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States, with a requirement to purge from NSA's records any resulting collection. NSA must also report any incidents of non-compliance, [redacted] Additionally, if NSA learns, after targeting a person reasonably believed to be outside the United States, that the person is inside the United States, or if NSA learns that a person who NSA reasonably believed was a non-United States person is in fact a United States person, NSA must terminate the acquisition, and treat any acquired communications in accordance with its minimization procedures. In each of the above situations, the Section 702 procedures during this reporting period required NSA to report the incident to DOJ and ODNI within the time specified in the targeting procedures of learning of the incident. b1

~~(S)~~ NSA has established an incident tracking and reporting standard operating procedure to implement the foregoing. NSA has indicated that such incidents are tracked using a pre-established tracking template that includes fields for the information to be reported to DOJ and ODNI. In addition to the Oversight and Compliance office, the NSA OGC and OIG are included in the process.

~~(U/FOUO)~~ In July 2009, NSA established the Office of the Director of Compliance, which is responsible for continuous modernization and enforcement of all mission compliance strategies and activities to ensure their relevance and effectiveness. This office complements and reinforces the intelligence oversight program of the NSA Inspector General and oversight responsibilities of the NSA General Counsel by creating a Comprehensive Mission Compliance Program (CMCP) to

ensure that progress is made across the board at NSA. This compliance program includes, among other things, special compliance activities focused on select FISA authorities as well as awareness and training which ensures a robust compliance training and education program for employees. [redacted] b1

~~(S)~~ II. Overview- FBI

(S) FBI is authorized [redacted] to acquire foreign intelligence information [redacted] The FBI targeting procedures [redacted] are set forth in an exhibit [redacted] b3

[redacted] b1

[redacted][16] [redacted] b3

---

[15] [redacted] b1

[16] [redacted]

~~(S)~~ A. FBI Targeting Procedures.

[redacted] FBI is authorized to acquire foreign intelligence information [redacted]

b1

[redacted]

b1

[redacted]

b1

[redacted]

b1

[redacted]

[redacted]

b1

[redacted]

(U) B. Documentation.

[redacted]

b3

~~(S//NF)~~ FBI has created a system to track the purging of information from its systems.

[redacted]

b1

(U) C. Oversight and Compliance.

[redacted][17]

---

17 [redacted]

b3

[redacted]

b1

[redacted]

[redacted]

b3

[redacted]

b1

[redacted]

b3

(U) IV. Overview -Minimization.

~~(S)~~ As referenced above, once [redacted] has been tasked for collection, non-publicly available information collected as a result of these taskings that concerns United States persons must be minimized. The FISC-approved minimization procedures require such minimization in the acquisition, retention, and dissemination of foreign intelligence information. As a general matter, minimization procedures under Section 702 are similar in most respects to minimization under other FISA orders. [redacted] The minimization procedures, however, do reflect differences from minimization under FISA orders where Section 702 imposed additional obligations or restrictions. For example, the Section 702 minimization procedures require, with limited exceptions, the purge of any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States, but is in fact located inside the United States at the time the communication is acquired, or was in fact a United States person at the time of targeting.

b1

(U) SECTION 3: CONDUCT OF COMPLIANCE ASSESSMENT ACTIVITIES

(U) I. Work of the Compliance Assessment Team.

(U) A. Compliance Assessment Team Members.

(U) Compliance assessment activities have been jointly conducted by DOJ and ODNI. Specifically, a joint team has been assembled, consisting of members from the DOJ's National Security Division (NSD), ODNI's Civil Liberties and Privacy Office (CLPO), ODNI's Office of General Counsel (OGC), ODNI's Office of Inspector General (OIG), and ODNI's Office of Deputy DNI for Collection. The team members play complementary roles in the review process. While all team members seek to ensure compliance with requirements and review available documentation, DOJ focuses on [redacted] reviews and completing reporting requirements, and ODNI seeks to identify programmatic and interagency issues.

b1

(U) B. Compliance Assessment Visits.

~~(S//NF)~~ The team organized its reviews based on the 60-day review cycle required by the procedures under each certification. For the reporting period, the on-site visits were as follows:

Date of Visit	[redacted]	Agency	Taskings Reviewed
August 6, 2009	[redacted]		June 2009
August 13, 2009	[redacted]		June 1 – July 31, 2009
September 3, 2009	[redacted]		July 2009

b1

September 22, 2009	[redacted]	June 1 – July 31, 2009
October 6, 2009	[redacted]	August 2009
October 13, 2009	[redacted]	August 1 – September 30, 2009
October 26, 2009	[redacted]	August 1 – September 30, 2009
November 10, 2009	[redacted]	September 2009
December 9, 2009	[redacted]	October 2009
December 10, 2009	[redacted]	October 1 – November 30, 2009
December 15, 2009	[redacted]	October 1 – November 30, 2009
January 12, 2010	[redacted]	November 2009

b1

~~(S//NF)~~ ODNI and DOJ have assessed the oversight process used since Section 702 was implemented in 2008, and has identified certain positive results. The oversight team has found that a large percentage of compliance incidents reported in the Section 707 Reports have been self-identified by the agencies. To optimize current resources in the oversight process, ODNI and DOJ are consulting on the best ways to maximize oversight resources.

b1

~~(S/NF)~~ To begin this change, the oversight team has instituted meetings [redacted] ODNI and DOJ assess that these discussions will enhance communications among the parties concerned with Section 702 collection, and will help reduce the number of reportable compliance incidents.

[redacted]

~~(S//SI//NF)~~ Review of statistical information regarding the number [redacted] on coverage is helpful for oversight planning purposes, trend and pattern analysis, and evaluation of underlying causes.

b1

[redacted]

b3

[19] [redacted]

[20] [redacted]

b1

[21] [redacted]

[redacted]

b1

[redacted]

b3

[redacted]

(U) **II. The Compliance Review Process.**

~~(S)~~ **A. Review Process - NSA.**

~~(S)~~ Prior to a visit date, NSA electronically sends [redacted] tasked during the review period to DOJ and ODNI. DOJ attorneys conduct a review of [redacted][22] and prepare a detailed report of their findings, which they share with the ODNI members of the review team. During their reviews, DOJ attorneys seek to determine whether the [redacted] meet the documentation standards required by NSA's targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA's foreignness determinations. For those [redacted] that, on their face, meet standards and provide sufficient information, no further supporting documentation is requested for the onsite review. DOJ attorneys then identify the [redacted] that, without further review of the cited documentation, did not provide sufficient information, and set forth their questions for each of those [redacted]. The review team then focuses on those [redacted] during the subsequent review.

b1

~~(S)~~ This initial review serves an important function for the review team. By reviewing the documentation "off site," the DOJ attorneys can analyze [redacted] with care, and make initial review assessments based on the type of information set forth on the selector sheets. For

[redacted]

b3

b1

[22] ~~(S)~~ As further discussed in the Section 707 Report, in August 2009, ODNI and DOJ learned that they had not been provided with [redacted]. NSA is continuing to evaluate its retrieval process to ensure that the [redacted] are also provided for review.

[redacted] b1

~~(S)~~ During the onsite review, the team examines [redacted] together with NSA SID Oversight and Compliance personnel, NSA attorneys and other NSA personnel as required. The team has access to [redacted] and interacts as needed with analysts to ask questions, identify issues, clarify ambiguous entries, and provide guidance on areas of potential improvement. Interaction continues following the onsite reviews in the form of e-mail and telephonic exchanges to answer questions and clarify issues. b1

~~(S)~~ Following the completion of a 60-day review cycle, DOJ prepares a report documenting the results of the review for that period. This report is provided to congressional committees as an attachment to the Section 707 Report. It documents the relevant time period of the review, the date of the onsite visit, the agencies reviewed, the number and types of [redacted], and a detailed summary of the findings for that review period. These reports contain specific details – without providing [redacted] – that explain, [redacted], the issues addressed by the oversight team as part of its review during that period, and the outcome of each issue.

b1

~~(S)~~ B. Review Process – FBI.

~~(S)~~ For FBI, the review team schedules a visit in advance with FBI, so that FBI can prepare

[redacted] b3

[redacted] b1

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

b1

[redacted]

b1

[redacted]

[redacted]

b3

(U) D. Review Process – Minimization.

~~(S)~~ During the onsite visits to NSA, the team reviews NSA's [redacted] of Section 702-acquired data to verify compliance with minimization procedures. The team reviews all serialized reports based on Section 702-acquired data that NSA identifies as containing United States person information. The results of these reviews have been documented and included as attachments to the Section 707 Report. During this review period, the team also began to take a random sample of reports not identified by NSA to ensure that NSA was accurately identifying all reports containing United States person information.

[redacted]

b1

[redacted] b1

[redacted] b3

(U) E. Review Process – Compliance Incident Reports.

~~(S)~~ The targeting procedures during the reporting period required that incidents of non-compliance be reported to DOJ and ODNI within five business or seven calendar days (depending on the applicable set of procedures) of the reporting agency learning of the incident. These reports are reviewed by the team, with follow-up questions asked for clarification and action. These incidents are often discussed during the regularly scheduled reviews. Where necessary, the team also has conducted onsite investigations of particular incidents. Compliance incidents have been reported to the FISC in individual compliance notices to the Court, filings related to the FISC's review of the [redacted], and/or in the Section 707 report. b1

~~(S//NF)~~ On August 25, 2009, the FISC ordered that DOJ provide reports to the FISC every 90 days providing the FISC with timely and effective notification of compliance issues involving the Government's implementation of its authorities under Section 702, including matters not covered by notices pursuant to Rule 10(c) of the Rules of Procedures for the FISC. The first report was filed with the FISC on December 7, 2009.[23]

(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS

~~(U//FOUO)~~ This assessment finds that during the reporting period, the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States. Processes have been put in place to implement these authorities and to impose internal controls for compliance and verification purposes.

~~(S)~~ There have been some compliance incidents during the reporting period representing a very small percentage of the overall activity. The DOJ and ODNI oversight team does not believe

[23] ~~(S//NF)~~ The first report covered the period August 25, 2009 through November 30, 3009, a period greater than 90 days. The time for reporting was extended for the first report in order to correspond with the reporting period for this Semiannual Assessment Report and the corresponding Section 707 Report.

these incidents represent an intentional attempt to circumvent or violate the procedures required by the Act.

~~(S)~~ The compliance incidents for the reporting period are described in detail in the Section 707 Report, and, as with the prior joint assessments, are analyzed here to determine whether there are patterns or trends that might indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented measures to prevent recurrences. The oversight team is continuing to review the efficacy of those measures on a continuing basis.

(U) I. Compliance Incidents – General.

~~(S)~~ As previously stated, the compliance incidents identified in this reporting period have been separately reported in detail in the Section 707 Report. The Section 707 Report covers those compliance incidents in the Attorney General's Third Semiannual Report Concerning Acquisitions under Section 702 of FISA.

(U) The compliance incidents are reviewed here in general terms to assess broader implications – the details are not repeated unless directly relevant to a point being made.

(U) A. Statistical Data Relating To Compliance Incidents.

[redacted] b1

[redacted] b3

~~(TS//SI//NF)~~ The value of statistical information in assessing compliance in situations such as this is unclear. A single incident, for example, may have broad ramifications. Multiple incidents

[24] [redacted] b1

[25] [redacted]

may increase the incident count, but may be deemed of very limited significance. There are, however, certain observations that can be made. [redacted] b1

[redacted] b3

~~(S)~~ In seeking to assess the value of such statistical data, the oversight team is evaluating the means for collecting and analyzing such data. For example, it may be useful to examine the statistical data through the lens of each agency. Moreover, it may prove useful to analyze the types of incidents that comprise the "numerator" and the type of activity that those incidents are being compared against – the denominator – in order to derive more targeted metrics and insights.

[redacted] b1

b3

[redacted] b1

[redacted]

[redacted] b1

~~(S)~~ Again, the joint oversight team does not wish to over-emphasize what can be inferred from statistics such as these. In particular, as stated in the prior report, the incidents themselves must be examined, since each – individually or collectively – might be indicative of patterns, trends, or underlying causes with broader implications.

[redacted] b1

[redacted] b3

[redacted] b1

[redacted] b3

[redacted] b1

26 [redacted]

[redacted]

b1

[redacted]

b3

~~(S)~~ As previously discussed, this joint assessment focuses on reviewing the compliance incidents reported in the Section 707 Report for purposes of identifying trends, patterns, and underlying causes. [redacted]

b1

[redacted]

[redacted][27]

b3

[redacted]

[redacted]

b1

[27] (U) Incident citations refer to the citations used in the Section 707 Report.

[redacted]

b1

[redacted] [28]

b3

[redacted]

[redacted] [29]

b1

b3

[redacted]

b1

[28] [redacted]

[29] ~~(U//FOUO)~~ Section 702(b)'s limitation on targeting United States persons does not contain an exception for consent.

[redacted]

b1

[redacted] [30]

b3

[redacted]

b1

[redacted]

b3

[redacted] [31]

[30] [redacted]

b1

[31] [redacted]

[redacted] b1

[redacted][32]

[redacted] b3

[redacted] b1

[redacted]

[redacted] b3

[redacted] b1

[32] [redacted]

[redacted] b1

[redacted] b3

[redacted] b1

[redacted] b3

[redacted] b1

[redacted] b3

[redacted] b1

[redacted] b1

[redacted] b3

[redacted]

[redacted] b1

~~(S)~~ I. Documentation Incidents.

~~(S)~~ As described in the Section 707 Report, documentation issues are summarized in compliance review memoranda prepared by DOJ following each on-site review. These memoranda detail the number and types of documents reviewed, the specific issues identified on a [redacted] basis, and how each issue was resolved during or following the on-site review. Each review memorandum is attached to the Section 707 Report. b1

~~(S)~~ The oversight team has noted continued improvement in documentation practices. [redacted] b3 The addition of the targeting rationale [redacted] is helping to provide explanatory information to further understand why a particular [redacted] is being tasked.

~~(S)~~ While interactions between oversight and agency personnel have helped improve expectations and understandings regarding documentation practices, as with the last joint assessment, the review memoranda attached to the Section 707 Report continue to note specific issues on a case-by-case basis. [redacted] b1 Discussions between the oversight team and agency

personnel continue regarding the level and type of detail appropriate to support certain taskings, particularly when technical information is not available.

[redacted]

b1

b3

b1

b3

b1

b1

[redacted]

b1

[redacted]

b3

[redacted]

b1

[redacted]

b3

~~(S)~~ **IV. Review of Compliance Incidents - FBI.**

[redacted]

b1

(U) SECTION 5: CONCLUSIONS.

~~(U//FOUO)~~ During the reporting period, the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The joint oversight team has not found indications of any intentional or willful attempts to violate or circumvent the requirements of the Act in the compliance incidents assessed above. The number of compliance incidents remains small, particularly when compared with the total amount of activity. Certain types of compliance incidents continue to occur, indicating the need for continued focus on measures to address underlying causes. The oversight team will continue to review the efficacy of measures to address the causes of compliance incidents during the next reporting period. In addition, the oversight team is continuing to evaluate the manner in which it conducts oversight to find areas to make oversight more efficient and effective.