U.S. Department of Justice

United States Attorney
Southern District of New York

86 Chambers Street
New York, New York 10007

August 11, 2015

By Electronic Mail

David E. McCraw, Esq.
Jeremy A. Kutner, Esq.
The New York Times Company
620 Eighth Avenue
New York, NY 10018
E-mail: mccrad@nytimes.com
jeremy.kutner@nytimes.com

Re: *The New York Times Co. and Charlie Savage v. National Security Agency*, 15 Civ. 2383 (KBF)

Dear David and Jeremy:

This Office represents the National Security Agency ("NSA"), the defendant in the above-referenced matter. Pursuant to the Scheduling Order, dated May 15, 2015, NSA has completed its review and processing of the attached documents. NSA is releasing 16 documents with redactions. Information has been redacted from these documents pursuant to 5 U.S.C. §§ 552(b)(1), (b)(3), and (b)(6). Each redacted document being released has been marked with the applicable FOIA exemption or exemptions.

If you have any questions, please do not hesitate to contact us.

Sincerely,

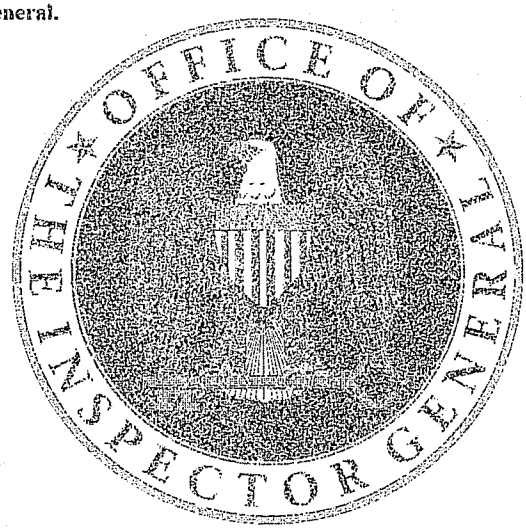
PREET BHARARA
United States Attorney for the
Southern District of New York

By: */s/ John Clopper*
JOHN D. CLOPPER
ANDREW E. KRAUSE
Assistant United States Attorneys
Telephone: (212) 637-2716/2769
Facsimile: (212) 637-0033
E-mail: john.clopper@usdoj.gov
andrew.krause@usdoj.gov

Enclosures

National Security Agency/Central Security Service

Further dissemination of this report outside the Office of the Inspector General, NSA is *PROHIBITED* without the approval of the Inspector General.



Inspector General Report

~~(TS//SI//NF)~~ REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS

ST-06-0018
5 SEPTEMBER 2006

DERIVED FROM: NSA/CSSM 1-52
DATED: 20041123
DECLASSIFY ON: MR

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts inspections, audits, and investigations. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations; to provide intelligence oversight; to protect against fraud, waste, and mismanagement of resources; and to ensure that NSA/CSS activities are conducted in compliance with the Constitution, laws, executive orders, regulations, and directives. The OIG also serves as ombudsman, assisting all NSA/CSS employees and affiliates, civilian and military.

(U) INSPECTIONS

(U) The inspection function conducts management and program evaluations in the form of organizational and functional reviews, undertaken either as part of the OIG's annual plan or by management request. The inspection team's findings are designed to yield accurate and up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with laws and regulations; the recommendations for corrections or improvements are subject to followup. The inspection office also partners with the Inspectors General of the Service Cryptologic Elements to conduct joint inspections of the consolidated cryptologic facilities.

(U) AUDITS

(U) The internal audit function is designed to provide an independent assessment of programs and organizations. Performance audits evaluate the economy and efficiency of an entity or program, as well as whether program objectives are being met and operations are in compliance with regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests or complaints; at the request of management; as the result of irregularities that surface during an inspection or audit; or at the initiative of the Inspector General.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

5 September 2006
IG-10693-06

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court (FISC) Order: Telephony Business Records (ST-06-0018)—ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This report summarizes the results of our assessment of Management Controls for Implementing the FISC Order: Telephony Business Records. The report incorporates management's response to the draft report.

2. (U//~~FOUO~~) As required by NSA/CSS Policy 1-60, *NSA/CSS Office of the Inspector General*, actions on OIG audit recommendations are subject to monitoring and followup until completion. Consequently, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." The status report should provide sufficient information to show that corrective actions have been completed. If a planned action will not be completed by the original target completion date, please state the reason for the delay and give a revised target completion date. Status reports should be sent to [redacted] Assistant Inspector General, at OPS 2B, Suite 6247, within 15 calendar days after each target completion date.

(b)(3)-P.L. 86-36

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] Assistant Inspector General, on 963-2988 or via e-mail at [redacted]

Brian McAndrew

BRIAN R. MCANDREW
Acting Inspector General

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: MR

DISTRIBUTION:
DIR
D/DIR
SIGINT Director
SID Program Manager for CT Special Projects, S
Chief, SID O&C
SSG1, [redacted]
SID Deputy Director for Customer Relationships
SID Deputy Director for Analysis and Production
Chief, S2I5
SID Deputy Director for Data Acquisition
Chief, S332
GC
AGC(O)

(b)(3)-P.L. 86-

~~(TS//SI//NF)~~ ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (FISC) ORDER: TELEPHONY BUSINESS RECORDS

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//STLW//OC,NF)~~ **Background:** The Order of the FISC issued 24 May 2006 in *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things* [redacted] No. BR-06-05 (the Order) states that "[t]he Inspector General and the General Counsel shall submit a report to the Director of NSA (DIRNSA) 45 days after the initiation of activity [permitted by the Order] assessing the adequacy of management controls for the processing and dissemination of U.S. person information. DIRNSA shall provide the findings of that report to the Attorney General." The Office of the Inspector General (OIG), with the Office of the General Counsel's (OGC) concurrence, issued the aforementioned report on 10 July 2006 in a memorandum with the subject *FISA Court Order: Telephony Business Records (ST-06-0018)*. Subsequently, DIRNSA sent the memorandum to the Attorney General. This report provides the details of our assessment of management controls that was reported to DIRNSA and makes formal recommendations to Agency management.

FINDING

~~(TS//SI//STLW//OC,NF)~~ ***The management controls designed by the Agency to govern the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order are adequate and in several aspects exceed the terms of the Order. Due to the risk associated with the collection and processing of telephony metadata involving U.S. person information, three additional controls should be put in place. Specifically, Agency management should:***

(1) design procedures to provide a higher level of assurance that non-compliant data will not be collected and, if inadvertently collected, will be swiftly expunged and not made available for analysis.

(2) separate the authority to approve metadata queries from the capability to conduct queries of metadata under the Order.

(3) conduct periodic reconciliation of approved telephone numbers with the logs of queried numbers to verify that only authorized queries have been made under the Order.

(U) Criteria

~~(TS//SI//STLW//OC,NF)~~ **The Order.** The Order authorizes NSA to collect and retain telephony metadata to protect against international terrorism and to process and disseminate this data [redacted] To protect U.S. privacy rights, the Order states specific terms and restrictions regarding the collection, processing, retention,[1] dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order. To ensure compliance with these terms and restrictions, the Order also mandates Agency management to implement a series of procedures to control the access to and use of the archived data collected pursuant to the Order. These control procedures are clearly stated in the Order. Appendix B includes a summary of the key terms of the Order and the related mandated control procedures.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) **Standards of Internal Control.** Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with applicable laws and regulations. The General Accounting Office's *Standards for Internal Control in the Federal Government*, November 1999 (the Standards), presents the standards that define the minimum level of quality acceptable for management control in government. NSA/CSS Policy 7-3, *Internal Control Program*, advises that evaluations of internal control should consider the requirements outlined by the Standards. The OIG uses the Standards as the basis against which management control is evaluated.

~~(TS//SI//NF)~~ Documented Procedures are Needed to Govern the Collection of Telephony Metadata

~~(TS//SI//NF)~~ Control procedures for collecting telephony metadata under the Order were not formally designed and are not clearly documented. As a result, management controls do not provide reasonable assurance that NSA will comply with the following terms of the Order:

[1] ~~(TS//SI)~~ We did not assess the controls over retention at this time as the Order allows data to be retained for five years.

NSA may obtain telephony metadata, which includes comprehensive communications, routing information, including but not limited to session identifying information, trunk identifier, and time and duration of a call. Telephony metadata does not include the substantive content of any communications, or the name, address, or financial information of a subscriber or customer.

~~(TS//SI//NF)~~ As required by the Order, OGC plans to examine periodically a sample of call detail records to ensure NSA is receiving only data authorized by the court. (This is the only control procedure related to collection that is mandated by the Order.) Although this will detect unauthorized data that has been loaded into the archived database, there should also be controls in place to prevent unauthorized data from being loaded into the database. In addition, good internal control practices require that documentation of internal control appear in management directives, administrative policies, or operating manuals. At a minimum, procedures should be established to:

- monitor incoming data on a regular basis,
- upon discovery of unauthorized data, suppress unauthorized data from analysts' view, and
- eliminate unauthorized data from the incoming data stream.

~~(TS//SI//STLW//NF)~~ With these proposed control procedures in place, the risk that Agency personnel will mistakenly collect types of data that are not authorized under the Order will be minimized. Although the primary and secondary orders prohibit the providers from passing specific types of data to NSA, mistakes are possible. For example, in responding to our request for information, Agency management discovered that NSA was obtaining two types of data that may have been in violation of the Order: a 16-digit credit card number and name/partial name in the record of Operator-assisted calls. (It should be noted that the name/partial name was not the name of the subscriber from the provider's records; rather, a telephone operator entered name at the time of an Operator-assisted call.)

~~(TS//SI//STLW//NF)~~ In the case of the credit card number, OGC advised that, in its opinion, collecting this data is not what the Court sought to prohibit in the Order; but recommended that it still be suppressed on the incoming data flow if not needed for contact chaining purposes. In the case of the name or partial name, OGC advised that, while not what it believed the Court was concerned about when it issued the Order, collecting this information was not in keeping with the Order's specific terms and that it should also be suppressed from the incoming data flow. OGC indicated that it will report these issues to the Court when it seeks renewal of the authorization. Agency management noted that these data types were

blocked from the analysts' view. Management also stated that it will take immediate steps to suppress the data from the incoming data flow. These steps should be completed by July 31, 2006.

Recommendation 1

~~(TS//SI)~~ Design and document procedures to provide a higher level of assurance that non-compliant data will not be collected and, if inadvertently collected, will be swiftly expunged and not made available for analysis.

(ACTION: [redacted])

(b)(3)-P.L. 86-36

(U) Management Response

CONCUR. ~~(TS//SI//STLW//NF)~~ Management concurred with the finding and recommendation and has already partially implemented the recommended procedures to block the questionable data from the providers' incoming dataflow. A final system upgrade to block the questionable data from one remaining provider is scheduled for [redacted] Testing is currently ongoing.

(b)(3)-P.L. 86-36

Status: OPEN
Target Completion Date: [redacted]

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

~~(TS//SI//NF)~~ Additional Controls are Needed to Govern the Processing of Telephony Metadata

~~(TS//SI//NF)~~ Agency management designed, and in some ways exceeded, the series of control procedures over the processing of telephony metadata that were mandated by the Order; however, there are currently no means to prevent an individual who is authorized access the telephony metadata from querying, either by error or intent, a telephone number that is not compliant with the Order. Therefore, additional controls are needed to reduce the risk of unauthorized processing.

~~(TS//SI//STLW//OC,NF)~~ Processing refers to the querying, search, and analysis of telephony metadata. To protect the privacy of U.S. persons, the Order restricts the telephone numbers that may be queried:

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

Based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number [redacted]

A telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.

~~(TS//SI//NF)~~ Agency management designed the series of control procedures over the processing of telephony metadata that were mandated by the Order. In a short amount of time, Agency management modified existing systems and designed new processes to:

- document justifications for querying a particular telephone number,
- obtain and document OGC and other authorized approvals to query a particular telephone number, and
- maintain automatic audit logs of all queries of the telephony metadata.

~~(TS//SI//NF)~~ These controls are adequate to provide reasonable assurance that justifications are sound, approvals are given and documented, and that there is a record of all queries made. Agency management even exceeded the intent of the Order by fully documenting the newly developed processes in Standard Operating Procedures and by developing enhanced logging capability that will, once completed, generate additional reports that are more usable for audit purposes.

~~(TS//SI//NF)~~ Two additional control procedures are needed to provide reasonable assurance that only telephone numbers that meet the terms of the Order are queried.

~~(TS//SI//NF)~~ The authority to approve metadata queries should be segregated from the capability to conduct metadata queries.

~~(TS//SI//NF)~~ The Chief and Deputy Chief of the Advanced Analysis Division (AAD) and five Shift Coordinators[2] each have both the authority to approve the querying of telephone numbers under the Order and the capability to conduct queries. The Standards of

[2] ~~(TS//SI//NF)~~ The Order grants approval authority to seven individuals: the SID Program Manager for CT Special Projects, the Chief and Deputy Chief of the AAD, and four Shift Coordinators in AAD. In practice, Agency management transferred the authority of the SID Program Manager for CT Special Projects to one additional Shift Coordinator. Approval authority therefore remains limited to seven individuals as intended by the Order.

Internal Control in the Federal Government require that key duties and responsibilities be divided among different people to reduce the risk of error or fraud. In particular, responsibilities for authorizing transactions should be separate from processing and recording them. This lack of segregation of duties increases the risk that Shift Coordinators and the Chief and Deputy Chief of AAD will approve and query, either by error or intent, telephone numbers that do not meet the terms of the Order.

Recommendation 2

~~(TS//SI)~~ Separate the authority to approve metadata queries from the capability to conduct queries of metadata under the Order.

(ACTION: Chief, Advanced Analysis Division)

(U) Management Response

CONCUR. ~~(TS//SI//STLW//NF)~~ Management concurred with the finding but stated that it could not implement the recommendation because of constraints in manpower and analytic expertise. As an alternative, management recommended that SID Oversight & Compliance (O&C) routinely review the audit logs of the Chief and Deputy Chief of the Advanced Analysis Division and Shift Coordinators to verify that their queries comply with the Order. This alternative would be developed in conjunction with actions taken to address Recommendation 3 and is contingent on the approval of a pending request to SID management to detail [redacted] computer programmers to the team. Management is also negotiating with O&C to accept the responsibility for conducting the recommended reconciliations.

Status: OPEN
Target Completion Date: [redacted] (b)(3)-P.L. 86-36

(U) OIG Comment

~~(TS//SI//STLW//NF)~~ Although not ideal, management's alternative recommendation to monitor audit logs to detect errors will, at a minimum, mitigate the risk of querying telephone numbers that do not meet the terms of the Order. Therefore, given the existing manpower constraints, management's suggested alternative recommendation meets the intent of the recommendation.

~~(TS//SI//NF)~~ ***Audit logs should be routinely reconciled to the records of telephone numbers approved for querying.***

~~(TS//SI//NF)~~ Management controls are not in place to verify that those telephone numbers approved for querying pursuant to the Order are the only numbers queried. Although audit logs document all queries of the archived metadata as mandated by the Order, the logs are not currently generated in a usable format, and Agency management does not routinely use those logs to audit the telephone numbers queried. The Standards of Internal Control in the Federal Government recommends ongoing reconciliations to "make management aware of inaccuracies or exceptions that could indicate internal control problems." The lack of routine reconciliation procedures increases the risk that errors will go undetected.

Recommendation 3

~~(TS//SI)~~ **Conduct periodic reconciliation of approved telephone numbers with the logs of queried numbers to verify that only authorized queries have been made under the Order.**

(ACTION: SID Special Program Manager for CT Special Projects)

(U) Management Response

CONCUR. ~~(TS//SI//STLW//NF)~~ Management concurred with the finding and recommendation and presented a plan to develop the necessary tools and procedures to implement the recommendation. However, management stated that completion of the planned actions is contingent on the approval of a pending request to SID management to detail [redacted] computer programmers to the team. (b)(3)-P.L. 86-36 Management is also negotiating with O&C to accept the responsibility for conducting the recommended reconciliations.

Status: **OPEN**
Target Completion Date: [redacted] (b)(3)-P.L. 86-36

(U) OIG Comment

(U) Planned action meets the intent of the recommendation. However, should SID management not grant the request for additional computer programmers or O&C not accept responsibility for conducting the reconciliations, management must promptly inform the OIG and present an alternative plan.

Observation

~~(TS//SI//NF)~~ *At the time of our review, there was no policy in place to periodically review telephone numbers approved for querying under the Order to ensure that the telephone numbers still met the criteria of the Order. Although the Order is silent on the length of time a telephone number may be queried once approved, due diligence requires that Agency management issue a policy decision on this matter and develop procedures to execute the decision.*

~~(TS//SI//NF)~~ Management Controls Governing the Dissemination of U.S. Person Information are Adequate

~~(TS//SI//NF)~~ Agency management implemented the series of control procedures governing the dissemination of U.S. person information mandated by the Order. O&C designs and implements controls to ensure USSID SP0018 compliance across the Agency, to include obtaining the approval of the Chief of Information Sharing Services and maintaining records of dissemination approvals, as required by the Order. No additional procedures are needed to meet the intent of the Order. Furthermore, these procedures are adequate to provide reasonable assurance that the following terms of the Order are met:

> Dissemination of U.S. person information shall follow the standard NSA minimization procedures found in the Attorney General-approved guidelines (USSID 18).

~~(TS//SI//NF)~~ Management Controls Governing Data Security are Adequate

~~(TS//SI//NF)~~ Agency management implemented the series of control procedures governing the data security of U.S. person information as mandated by the Order, such as the use of user IDs and passwords. Agency management exceeded the terms of the Order by maintaining additional control procedures that provide an even higher level of assurance that access to telephony metadata will be limited to authorized analysts. Most of these controls had been in place prior to and aside from the issuance of the Order. Only the requirement that OGC periodically monitor individuals with access to the archive was designed in response to the Order. Combined, these procedures are adequate to provide reasonable assurance that Agency management complies with the following terms of the Order:

> DIRNSA shall establish mandatory procedures strictly to control access to and use of the archived metadata collected pursuant to this Order.

~~(TS//SI//NF)~~ Additionally, O&C plans to reconcile the list of approved analysts with a list of authorized users to ensure only approved analysts have access to the metadata.

~~(TS//SI//NF)~~ Management Controls Governing the Oversight of Activities Conducted Pursuant to the Order are Adequate

~~(TS//SI//NF)~~ As mandated by the Order, Agency management designed plans to provide general oversight of activities conducted pursuant to the Order. The Order states that,

> The NSA Inspector General, the NSA General Counsel, and the Signals Intelligence Directorate Oversight and Compliance Office shall periodically review this program.

~~(TS//SI//STLW//OC,NF)~~ Specifically, Agency management designed the following plans that are adequate to ensure compliance with the Order.

- ~~(TS//SI//NF)~~ The OGC will report on the operations of the program for each renewal of the Order.
- ~~(TS//SI//NF)~~ O&C plans to conduct periodic audits of the queries.
- ~~(TS//SI//NF)~~ OIG planned to audit telephony metadata collected and processed under the Presidential Authorization. Upon issuance of the Order, the audit was put on hold to complete the court-ordered report. OIG will modify the audit plan to include the new requirements of the Order. Once sufficient operations have occurred under the Order to allow for a full range of compliance and/or substantive testing, the audit will proceed.

(U) Conclusion

~~(TS//SI//NF)~~ The activities conducted under the Order are extremely sensitive given the risk of encountering U.S. person information. The Agency must take this responsibility seriously and show good faith in its execution. Much of the foundation for a strong control system is set up by the Order itself, in the form of mandated control procedures. In many ways, Agency management has made the controls even stronger. Our recommendations will address control weaknesses not covered by the Order or Agency management and will meet Federal standards for internal control. Once the noted weaknesses are addressed, and additional controls are implemented, the management control system will provide reasonable assurance that the terms of the Order will not be violated.

APPENDIX A

(U) About the Audit

This page intentionally left blank

(U) ABOUT THE AUDIT

(U) Objectives

~~(TS//SI)~~ The overall objective of this review was to determine whether management controls will provide reasonable assurance that Agency management complies with the terms of the Order. Specific objectives were to:

- verify that Agency management has designed the control procedures mandated by the Order.
- assess the adequacy of all management controls in accordance with the *Standards of Internal Control in the Federal Government*.

(U) Scope and Methodology

(U//~~FOUO~~) The audit was conducted from May 24, 2006 to July 8, 2006.

(U//~~FOUO~~) We interviewed Agency personnel and reviewed documentation to satisfy the review objectives.

~~(TS//SI)~~ We did not conduct a full range of compliance and/or substantive testing that would allow us to draw conclusions on the efficacy of management controls. Our assessment was limited to the overall adequacy of management controls, as directed by the Order.

~~(TS//SI)~~ As footnoted, we did not assess controls related to the retention of telephony metadata pursuant to the Order. As the Order authorizes NSA to retain data for up to five years, such controls would not be applicable at this time.

(U) Prior Coverage

1. (U//~~FOUO~~) Interim Report of the STELLARWIND Program: *Need for Documentation and Development of Key Processes*, 14 May 2004
2. ~~(C)~~ Interim Report of the STELLARWIND Program: *Need for Increased Attention to Security-Related Aspects of the STELLARWIND Program*, 13 September 2004

This page intentionally left blank

Appendix B

(U//~~FOUO~~) Telephony Business Records FISC Order - Mandated Terms and Control Procedures

This page intentionally left blank

(U) Business Records FISC Order

(U) Mandated Terms and Control Procedures

~~(TS//SI//NF)~~

Control Area	Terms of the Order	Responsible Entity	Control Procedures
Collection of Metadata	NSA may obtain telephony metadata, which includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, communications device identifier, etc.), trunk identifier, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 USC 2510(8) or the name, address, or financial information of a subscriber or customer (pg. 2, para 2).	OGC	At least twice every 90 days, OGC shall conduct random spot checks, consisting of an examination of a sample of call detail records obtained, to ensure that NSA is receiving only data as authorized by the Court and not receiving the substantive content of the communications (pg. 10, para (4)J).

~~(TS//SI//NF)~~

Control Area	Terms of the Order	Responsible Entity	Control Procedures
Processing (Search & Analysis, or Querying of Archived Metadata)	Although data collected under this order will be broad, the use of that information for analysis shall be strictly tailored to identifying terrorist communications and shall occur solely according to the procedures described in the application (pg. 6, para (4)D). Any search or analysis of the data archive shall occur only after a particular known telephone number has been associated with [redacted] (pg. 5, para (4)A). • Based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted] (pg. 5, para (4)A); • A telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution (pg. 5, para (4)A). DIRNSA shall establish mandatory procedures strictly to control access to and use of the archived data collected pursuant to this Order (pg. 5, para (4)A).	OGC PM, Chief or D/Chief of AAD, Shift Coordinators PM; Chief & D/Chief of AAD, & Shift Coordinators AAD Analysts (b)(3)-P.L. 86-36 [redacted] and Technical Support OGC OGC	OGC shall review and approve proposed queries of archived metadata based on seed account numbers reasonably believed to be used by U.S. persons (pg. 6, para (4)C). Queries of archived data must be approved by one of seven persons: SID PM for CT Special Projects, the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division, or one of the four specially authorized CT Advanced Analysis Shift Coordinators in the Analysis and Production Directorate of SID (pg. 7, para (4)D). SID PM for CT Special Projects; Chief and Deputy Chief, CT Advanced Analysis Division, and CT Advanced Analysis Shift Coordinators shall establish appropriate management controls (e.g., records of all tasking decisions, audit and review procedures) for access to the archived data (pg. 8, para (4)G). *Maintain a record of justifications because* at least every ninety days, the Department of Justice shall review a sample of NSA's justifications for querying the archived data (pg. 8, para (4)E). When the metadata archive is accessed, the user's login, IP address, date and time, and retrieval request shall be automatically logged for auditing capability (pg. 6, para (4)C). OGC will monitor the functioning of this automatic logging capability (pg. 6, para (4)C). Analysts shall be briefed by OGC concerning the authorization granted by this Order and the limited circumstances in which queries to the archive are permitted, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of the archived data (pg. 6, para (4)G).

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

Control Area	Terms of the Order	Responsible Entity	Control Procedures
Dissemination of U.S. Person Information	Dissemination of U.S. person information shall follow the standard NSA minimization procedures found in the Attorney General-approved guidelines (USSID 18) (pgs. 6-7, para (4)D) & pg. 8, para (4)G).	Chief of Information Sharing Services in SID	Prior to the dissemination of any U.S. person identifying information, the Chief of Information Sharing Services in SID must determine that the information identifying the U.S. person is in fact related to Counterterrorism information and that it is necessary to understand the Counterterrorism information or assess its importance (pg. 7, para (4)D). A record shall be made of every such determination (pg. 7, para (4)D).
Metadata Retention	Metadata collected under this Order may be kept online (that is, accessible for queries by cleared analysts) for five years, at which time it shall be destroyed (pg. 8, para (4)F).	[redacted] and Technical Support	None **(b)(3)-P.L. 86-36**
Data Security	~~(TS//SI//NF)~~ DIRNSA shall establish mandatory procedures strictly to control access to and use of the archived data collected pursuant to this Order (pg. 5, para (4)A).	[redacted] and Technical Support OGC	The metadata shall be stored and processed on a secure private network that NSA exclusively will operate (pg. 5, para (4)B). Access to the metadata archive shall be accomplished through a software interface that will limit access to this data to authorized analysts controlled by user name and password (pg. 5, para (4)C). OGC shall monitor the designation of individuals with access to the archive (pgs. 5-6, para (4)C).
Oversight	The IG, GC, and the SID Oversight and Compliance Office shall periodically review this program (pg. 8, para (4)H).	IG, GC, and SID Oversight and Compliance Office DIRNSA	The IG and GC shall submit a report to DIRNSA 45 days after the initiation of the activity assessing the adequacy of the management controls for the processing and dissemination of U.S. person information (pg. 8, para (4)H). DIRNSA shall provide the findings of that report to the Attorney General (pg. 9, para (4)H).

This page intentionally left blank

Appendix C

~~(U//FOUO)~~ Full Text of Management Comments

This page intentionally left blank

~~TOP SECRET//COMINT//STLW//NOFORN//20301115~~

PROGRAM MEMORANDUM

PM-031-06 Reissued
29 Aug 2006

To: Office of the Inspector General

Cc:
Counterterrorism Production Center
Chief, SID Oversight and Compliance
SSG1

(b)(3)-P.L. 86-36

SUBJECT: ~~(TS//SI//NF)~~ PMO Response to IG-10681-06, Subject Draft Report on the Assessment of Management Controls for implementing the FISA Court Order: Telephony Business Records (ST-06-0018)

1. (U//~~FOUO~~) The SIGINT Directorate Program Office appreciates and welcomes the Inspector General Office's review of program operations as required by the subject court order. The Program Office offers the following response.

2. ~~(TS//SI//NF)~~ This report presents three findings/recommendations. Finding one pertains to procedures to provide a higher level of assurance that non-compliant data will not be collected and, if inadvertently collected, will be swiftly expunged and not made available for analysis. Finding two pertains to the goal to separate the authority to approve metadata queries from the capability to conduct queries. Finding three pertains to the requirement to conduct periodic reconciliation of approved telephone numbers with the logs of queried numbers to verify that only authorized queries have been made.

3. ~~(TS//SI//STLW//NF)~~ With respect to Finding One, the Program Office acknowledges that the item is factually correct and concurs with the assessment with comment. It should be noted that internal management controls, known as software rules that are part of the database, do prevent the data in question from ever being loaded into the operational contact chaining databases. Still, the data in question did exist in the dataflow and should be suppressed on the provider-end as the OIG recommends.

(b)(3)-P.L. 86-36

a. ~~(TS//SI//STLW//NF)~~ Corrective Actions: Although already partially implemented among the providers, the final system upgrade necessary to block the data in question from one provider on the incoming dataflow is scheduled to be in place Testing continues at this time.

(b)(3)-P.L. 8

4. ~~(TS//SI//NF)~~ Finding Two recommends two additional controls. With respect to the first, "The authority to approve metadata queries should be segregated from the capability to conduct metadata queries", the Program Office agrees the assessment has merit, but cannot implement the required corrective actions. In theory, the OIG recommendation is sound and conforms fully to the standards of internal control in the Federal Government. In practical terms, it is not something that can be easily implemented given the

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: 20301115

~~TOP SECRET//COMINT//STLW//NOFORN//20301115~~

risk/benefit tradeoff and real world constraints. Manpower ceilings and available analytic expertise are the two most significant limiting factors.

5. ~~(TS//SI//NF)~~ The Advanced Analysis Division (S2I5) is comprised of personnel of varying grades and experience levels. Given the requirements of the court order, the Shift Coordinators are required to be the most experienced intelligence analysts, have the most training and consequently hold the most senior grade levels. They therefore are given the authority to approve data queries, and because of their status can also execute queries. Removing this dimension of their authorities would severely limit the versatility of the most experienced operations personnel. Also, as their title implies, they are also the most senior personnel present during each operational shift and in effect control the ops tempo on the operations floor. Replicating that senior structure to accommodate the OIG recommendation is not possible given current manning authorizations and ops tempo.

a. ~~(TS//SI//NF)~~ However, there are checks and balances already in place to help mitigate the risks cited. For example, the Shift Coordinators routinely approve queries into the database based on selectors meeting a reasonable articulable suspicion standard IAW with NSA OGC written guidelines and verbal briefings. Any queries initiated from probable U.S. selectors must be individually approved by the OGC. In this way, the risk of error or fraud associated with the requirements of the court order is acceptably mitigated within available manning and analytic talent constraints.

b. ~~(TS//SI//NF)~~ Corrective Actions: Corrective actions cannot be implemented without significantly increasing manning levels of senior, highly skilled analysts. In our view, the benefit gained will not justify the manpower increase required. However, it may be possible to implement additional checks and audits on the query approval process. As recommended in the response to Finding Three below, Oversight and Compliance could, if they accept an expanded role, use (yet to be developed) new automated software tools to regularly review the audit logs of all shift coordinators. With software changes to the audit logs it would be possible to easily compare numbers approved and their accompanying justifications against numbers chained. In this way, it would be possible to review the shift coordinator's actions against the standards established by the court. The Program Office recommends that this corrective action be pursued as part of the long term goal discussed below.

6. ~~(TS//SI//NF)~~ Finding Three reads "conduct periodic reconciliation of approved telephone numbers with the logs of queried numbers to verify that only authorized queries have been made under the order". The Program Office agrees with this assessment. However, competing priorities for the software programming talent necessary to implement improvements to the audit logs, as well as to perform the programming necessary to create automated reconciliation reports, require that this issue be addressed as a long term goal.

a. ~~(TS//SI//NF)~~ If SID management approves a pending Program Office request to detail [redacted] computer programmers to the team for six-to-nine month rotations, suitable procedures and software tools could be implemented. Also, the Program Office has approached the office of Oversight and Compliance about accepting the responsibility of conducting the recommended audits. That negotiation is ongoing.

(b)(3)-P.L. 86-36

b. ~~(TS//SI//NF)~~ Corrective Action: Acceptable tools and procedures can be developed [redacted] Assuming the Program team's request is granted, this initiative can be completed [redacted] The corrective action will include:

(b)(3)-P.L. 86-36

1. (U//~~FOUO~~) Improvements to the audit logs to make them more user friendly

2. (U//~~FOUO~~) Reports that provide a useable audit trail from requester, to approver, to any resulting reports. These reports will be used to automatically identify any discrepancies in the query process (i.e. queries made, but not approved).

3. (U//~~FOUO~~) Complete the negotiations with SID Oversight & Compliance

7. (U//~~FOUO~~) Please contact me if you have additional questions.

(b)(3)-P.L. 86-36

[redacted]

SID Program Manager
CT Special Programs

IT'S EVERYBODY'S BUSINESS –

TO REPORT SUSPECTED INSTANCES OF FRAUD,
WASTE, AND MISMANAGEMENT, CALL OR VISIT
THE NSA/CSS IG DUTY OFFICER
ON 963-5023s/ [redacted] (b)(3)-P.L. 86-36
IN OPS2A/ROOM 2A0930

IF YOU WISH TO CONTACT THE OIG BY MAIL,
ADDRESS CORRESPONDENCE TO:

DEPARTMENT OF DEFENSE
NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE
ATT: INSPECTOR GENERAL
9800 SAVAGE ROAD, STE 6247
FT. MEADE, MD 20755-6247

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ NSA Controls for FISC Business Records Orders

ST-10-0004
12 May 2010

Derived from: NSA/CSSM 1-52
Dated: 20070108
Declassify on: 20320108

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assesses whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

12 May 2010
IG-11154-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Advisory Report on the Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004) – ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This advisory report summarizes results of pilot testing by the Office of the Inspector General in support of the Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004).

2. ~~(TS//SI//NF)~~ The IG found three control weaknesses related to querying data collected under the Business Records Order, as well as concerns related to the dissemination of information. Because we found no incidents of non-compliance and the control weaknesses should be resolved with the release of a new selector tracking application planned for May 2010, we will not make formal recommendations at this time, and no management response is required. However, we will monitor the situation and make formal recommendations as appropriate. Also, while the IG will not formally track these suggestions in accordance with our current policy, they will be subject to review in future audits.

3. (U//~~FOUO~~) To discuss this report further, please contact Assistant Inspector General [redacted] on 963-2988(s) or by e-mail at [redacted] (b)(3)-P.L. 86-36

4. (U) We appreciate the courtesy and cooperation extended to the audit team throughout the review.

George Ellard

GEORGE ELLARD
Inspector General

DISTRIBUTION:
D/GC(O) [redacted]
Chief, SV42 [redacted]
Chief, S12 [redacted]
Chief, S2I4 [redacted]
Chief/TD [redacted]
DoJ/NSD [redacted]

(b)(6)

cc:
IG
D/IG
D13
D14
D1 AIG for Follow-up
Chief, SV
Chief, S1
Chief, S2I
Chief, S3
Chief S33
Chief, S332
Chief, T12
Chief, T122
Chief, T1222
OGC IG POC [redacted]
SID IG POC [redacted]
TD IG POC [redacted]

(b)(3)-P.L. 86-36

(U) EXECUTIVE SUMMARY

~~(TS//SI//NF)~~ *This report provides the results and related findings of pilot testing of NSA controls to comply with the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR). These results will be used to design test objectives for monthly testing from January to December 2010. NSA complied with the BR Order for the six pilot test objectives tested and within the time periods covered. Although we found no incidents of non-compliance, pilot testing disclosed weaknesses in controls over the querying of certain types of selectors, as well as concerns related to the dissemination of BR information that should be brought to management's attention. Because weaknesses related to querying should be resolved with NSA's implementation of a new application to track BR selectors in May 2010, we will closely monitor the implementation of this application as part of our monthly testing and make formal recommendations as necessary.*

(U) Background

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ **The Business Records Order**

~~(TS//SI//NF)~~ Pursuant to a series of Orders issued by the FISC beginning in May 2006, NSA has been receiving and analyzing certain call detail records or telephony metadata [redacted] [redacted] NSA refers to the Orders collectively as the "BR Order" or "BR FISA."

~~(TS//SI//NF)~~ The BR Order provides NSA access to bulk call detail records that primarily include records of telephone calls between the United States and abroad or wholly within the United States. [redacted] [redacted] To access this data, NSA must conclude that, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, facts give rise to a reasonable articulable suspicion (RAS) that an identifier is [redacted] [redacted] This collection of information is not available to NSA through its other foreign intelligence information collection. It is valuable to NSA analysts tasked with identifying potential threats to the U.S. homeland and interest abroad by enhancing the analyst's ability to identify, prioritize, and track terrorist operatives and

their support networks in the United States and abroad using call chaining [redacted] techniques.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ The primary BR Order in effect during pilot testing was signed on 16 December 2009 and expired on 12 March 2010. Because the bulk call detail records provided to NSA include primarily records of telephone calls that either have one end in the United States or are purely domestic, the Order defines a series of requirements NSA must follow to protect the privacy rights of U.S. persons.

(U) **Continuous Auditing**

~~(TS//SI//NF)~~ To assess NSA's controls for complying with the BR Order, we will use a continuous auditing methodology by performing monthly testing of NSA's compliance with certain requirements for a period of 12 months. Continuous auditing is one of many tools used within the audit profession to provide reasonable assurance that the control structure surrounding an operational environment is suitably designed, established, and operating as intended. The results of pilot testing reported here will be used to design monthly test objectives.

(U) Pilot Test Results and Related Findings

~~(TS//SI//NF)~~ NSA complied with the BR Order for the six pilot test objectives within the stated time periods and scope limitations.[1] Appendix B includes detailed test results and related scope limitations for each test objective. Although we found no instances of non-compliance, we identified control weaknesses related to querying that increase NSA's risk of non-compliance and will limit future testing if not addressed. We also identified concerns related to dissemination that should be brought to management's attention.

~~(TS//SI//NF)~~ **Control Weaknesses Related to Querying**

~~(TS//SI//NF)~~ The BR FISA Database used to track the approval status and justifications of BR selectors does not adequately track information necessary to implement effective preventive and detective controls to ensure compliance with the following requirements:

- ~~(TS//SI//NF)~~ The NSA Office of General Counsel (OGC) must review selectors associated with U.S. persons to verify that RAS determinations are not based solely on activities protected by the First Amendment to the Constitution;

- ~~(TS//SI//NF)~~ Authorized officials must revalidate RAS determinations of foreign and U.S. selectors within one year and 180 days, respectively; and

(b)(3)-P.L. 86-36

[1]We do not include here [redacted] instances of non-compliance with dissemination rules that NSA had already reported in June 2009 and for which NSA had taken appropriate corrective action.

- ~~(TS//SI//NF)~~ Analysts who query time-restricted selectors must be made aware of the time period for which the RAS determination applies so that the information may be minimized.

~~(TS//SI//NF)~~ Specifically, the database is not designed to tag and track selectors associated with U.S. persons, revalidation dates, or time-restricted selectors as separate and distinct fields. Though analysts might include such information in the "comments" field, that field is not easily searchable or usable in designing controls. Separate fields are needed to integrate preventive controls into [redacted] and ensure the completeness of detective controls, such as weekly audits by the SIGINT Directorate (SID) Office of Oversight and Compliance. As a result, NSA increases its risk of non-compliance with these requirements, and the scope of testing on selectors associated with U.S. persons and revalidation dates may be limited.[2]

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Management stated that the Homeland Security Analysis Center (HSAC/S2I4) and Technology Directorate representatives decided not to correct control weaknesses because such modifications could take enough time so as to overlap with the release of a new selector management application called [redacted] now planned for May 2010. Initial demonstrations and requirements documents suggest that [redacted] will resolve these weaknesses. Not only will key data be tracked to enable controls that will detect instances of non-compliance, but controls will also be added to prevent querying of selectors that have not been properly approved by OGC or revalidated within appropriate timeframes. [redacted] has also been designed to track time-restricted selectors, and SIGINT managers are defining related requirements to configure [redacted] with appropriate preventive and detective controls.[3]

~~(TS//SI//NF)~~ Because NSA recognizes these weaknesses and plans to release [redacted] in May 2010, we will not make formal recommendations to correct control deficiencies in the existing database. Time-restricted selectors are not currently a compliance risk because management removed all [redacted] time-restricted selectors from querying as they were determined to no longer have intelligence value. We suggest that management not reinstate time-restricted selectors until [redacted] is in place and [redacted] can be configured with appropriate preventive and detective controls.

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ The HSAC/S2I4 is managing the risk associated with revalidations by implementing temporary manual processes to track revalidations and by using more stringent timeframes than those required by the Order. We will use the manual process to test revalidation dates as part of our monthly testing and will make formal recommendations as necessary.

(b)(3)-P.L. 86-36

[2] ~~(TS//SI//NF)~~ We did not include time-restricted selectors in pilot testing because determining compliance with the requirement was too subjective to apply the continuous auditing methodology.
[3] ~~(TS//SI//NF)~~ [redacted] is NSA's corporate contact chaining system used to store and analyze BR data.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ After NSA reported [redacted] incidents in 2009 when selectors associated with U.S. persons had been queried without having been reviewed by OGC, HSAC/S2I4 reiterated this requirement in its procedures and training. However, without preventive controls in place, NSA remains at risk for non-compliance, and our monthly testing will continue to be limited [redacted] We will closely monitor [redacted] release as part of our monthly testing and make formal recommendations as necessary.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ **Concerns Related to Dissemination**

~~(TS//SI//NF)~~ With the exception of exculpatory material used in litigation, the BR Order requires that all disseminations of U.S. person information derived from BR metadata made outside NSA, whether in formal reporting or in response to requests for information or other forms of communication, be approved by one of five NSA officials. The BR Order does not state that the authority may be further delegated. The Order also requires that NSA provide the FISC with a weekly report of all dissemination.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ As described in Appendix B, pilot testing showed NSA to be compliant for the two dissemination objectives tested, with the exception of [redacted] instances in which the Deputy Chief of Information Sharing Services (ISS/S12) signed dissemination authorizations in the Chief's absence. Because these instances were known and reported by NSA in 2009, we are not reporting them as compliance incidents here. However, we found two areas for improvement and management consideration:

- ~~(TS//SI//NF)~~ The process to obtain and document dissemination authorizations for serialized SIGINT reports signed by the Chief of ISS/S12 and compile Weekly Dissemination Reports was largely manual and, therefore, dependent on the diligence of the staff and the strength of standard operating procedures. Because of the relatively small amount of information disseminated [redacted] during 2009), the risks of using a manual process were manageable, but management should consider automating dissemination approvals and tracking, should BR-related dissemination increase.

(b)(1)
(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ ISS/S12 did not maintain individual dissemination authorizations for non-serialized disseminations made outside NSA, such as briefings, as required by its standard operating procedures. Though such approvals could be tracked to e-mails, it would be more prudent to maintain formal documentation, as required in the procedures, so that NSA can easily demonstrate compliance with the BR Order.

(U) Plans to Continue Monthly Testing

~~(TS//SI//NF)~~ We will continue to test these objectives as part of monthly testing starting with January 2010 data and with the following additions:

- ~~(TS//SI//NF)~~ Verify that RAS approvals are made by Homeland Mission Coordinators or other authorized officials.
- ~~(TS//SI//NF)~~ Verify that RAS approval or revalidation dates are within authorized timeframes (180 days for domestic selectors and one year for foreign).
- ~~(TS//SI//NF)~~ Include queries [redacted] Database to test access, RAS approvals, OGC reviews, and number of hops.

~~(TS//SI//NF)~~ Because the transition to [redacted] will create a new control environment, we might extend testing past the planned year to ensure the reliability of results. We will test selector revalidations using the temporary manual process currently in place. However, limitations to test selectors associated with U.S. persons will remain until [redacted] is implemented.

(b)(3)-P.L. 86-36

This page intentionally left blank

APPENDIX A

(U) About the Audit

This page intentionally left blank

(U) ABOUT THE AUDIT

(U) Objectives

~~(TS//SI//NF)~~ The objective of this audit is to test whether controls to ensure NSA compliance with key terms of the BR Order are operating as intended. Specifically, we tested the following objectives to determine NSA compliance and assess the feasibility and reasonableness of including these objectives in monthly testing:

1. ~~(TS//SI//NF)~~ Only authorized individuals accessed BR data in December 2009.
2. ~~(TS//SI//NF)~~ Selectors queried in December 2009 were documented as either approved to have met the RAS standard or were queried for data integrity purposes.
3. ~~(TS//SI//NF)~~ Selectors queried in December 2009 that were associated with a U.S. person were documented as having been verified by OGC that RAS determinations were not based solely on activities protected by the First Amendment to the Constitution.
4. ~~(TS//SI//NF)~~ Selectors queried in December 2009 were chained to no more than three hops.
5. ~~(TS//SI//NF)~~ BR-related information disseminated outside NSA in serialized SIGINT reports during 2009 was approved by the Chief of Information Sharing Services or other authorized official.
6. ~~(TS//SI//NF)~~ Weekly Dissemination Reports issued in 2009 completely and accurately reported BR-related information that was disseminated in serialized SIGINT reports.

~~(TS//SI//NF)~~ Of the 58 NSA requirements in the BR Order signed on 16 December 2009, we decided to pilot test these six objectives because they were relatively stable, at risk for technical non-compliance or violation of privacy rights, and testable using the continuous auditing methodology. For a requirement to be testable, compliance must be clearly objective and verifiable by supporting data.

(U) Scope

(U//~~FOUO~~) We conducted pilot testing from January to March 2010.

~~(TS//SI//NF)~~ We reviewed the following data: [redacted] audit logs for December 2009, RAS approval dates from the BR FISA database, RAS-approved U.S. person selectors, and access lists maintained on the

(b)(3)-P.L. 86-36

[redacted] SharePoint website. We verified that serialized SIGINT reports issued in 2009 were supported by dissemination authorizations. We also reviewed Weekly Dissemination Reports and supporting documentation.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) We met with individuals from OGC, SID, and the Technology Directorate, including the SID Office of Oversight and Compliance (SV), ISS/S12, HSAC/S2I4, SID Issues Support Staff (S02321), Analytic Capabilities (T12), Structured Repositories (T132), and [redacted] Operations (T1222).

(U) **Scope Limitations**

(U//~~FOUO~~) As described in the findings and Appendix B, we had three significant scope limitations during pilot testing:

- ~~(TS//SI//NF)~~ We did not test whether OGC had reviewed RAS determinations of queried non-U.S. selectors associated with U.S. persons, as mandated by the Order, because existing databases did not definitively identify these selectors.
- ~~(TS//SI//NF)~~ We did not test whether selectors had been revalidated within the authorized timeframes because existing databases did not track revalidation dates.
- ~~(TS//SI//NF)~~ We did not test whether non-serialized dissemination was approved by the Chief, ISS/S12, or other authorized officials because approvals were documented in e-mails rather than formal dissemination authorizations. For the same reason, we did not test whether Weekly Dissemination Reports accurately and completely reported non-serialized dissemination.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ [redacted]

(U) Methodology

~~(TS//SI//NF)~~ To test NSA's compliance with querying requirements, we compared all selectors documented in [redacted] audit logs that had been queried in December 2009 against access lists, RAS approvals documented in the BR FISA database, and OGC reviews documented in the Homeland Requests Database. We also counted the number of hops

(b)(3)-P.L. 86-36

chained for each selector in the [redacted] audit logs. We researched any anomalies to make a final determination of compliance.

(b)(3)-P.L. 86-36

(TS//SI//NF) To test NSA's compliance with dissemination requirements, we identified all serialized SIGINT reports with the BR-related SIGINT [redacted] that were issued in 2009 and documented in the [redacted] NSA's management information system that contains statistical information about serialized SIGINT reports. We verified that each report had been documented in a dissemination authorization signed by the Chief, ISS/S12 or other authorized individual. We then used this information to verify the completeness and accuracy of the Weekly Dissemination Reports.

(b)(1)
(b)(3)-P.L. 86-36

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) Prior Coverage

(TS//SI//NF) On 10 July 2006, in a memorandum entitled *FISA Court Order: Telephony Business Records (ST-06-0018)*, the OIG issued "a report to the Director of NSA 45 days after the initiation of the activity [permitted by the Order] assessing the adequacy of the management controls for the processing and dissemination of U.S. person information." We issued this report with the OGC's concurrence and as mandated by the Order. We issued a separate report on 5 September 2006 that provided the details of the findings and made formal recommendations to management.

This page intentionally left blank

APPENDIX B

(U) Pilot Test Results

This page intentionally left blank

(U) PILOT TEST RESULTS

(TS//SI//NF)

Area	Test Results	Scope Limitations	Test Period
1. Access	Using [redacted] unique seed selectors, all [redacted] queries were made by authorized personnel.	None; however, we limited our testing to queries made in [redacted] and did not test queries made to the [redacted]	Dec 2009
2. RAS Approval of Selectors	All [redacted] seed selectors queried for intelligence analysis purposes were documented as RAS approved. Of the [redacted] seed selectors not RAS approved, all were queried for demonstration or data integrity purposes and only one resulted in contact chaining. The exception was conducted by a Data Integrity Analyst who had permission to query outside the existing control structure.	We verified RAS approvals, not revalidation dates, and did not verify that the approving official was a Homeland Mission Coordinator or other official authorized to make RAS approvals. We also limited our testing to queries made in [redacted] and did not test queries made to the [redacted]	(b)(3)-P.L. 86-36 Dec 2009
3. OGC Review of Selectors Associated with U.S. Persons	All [redacted] queried seed selectors that were presumed to be associated with U.S. persons were reviewed by OGC. In one case, the approval was documented as "verbal."	We limited testing to selectors presumed to be associated with U.S. persons [redacted] Therefore, we did not test OGC reviews of non-U.S. selectors associated with U.S. persons because the existing database does not track this information. Management has since estimated there to be about [redacted] of these selectors. We also limited our testing to queries made in [redacted] and did not test queries made to the [redacted]	Dec 2009
4. Chaining	All queries were chained to no more than three hops from the seed selector.	None; however, we limited our testing to queries made in [redacted] and did not test queries made to the [redacted]	Dec 2009
5. Dissemination of Serialized SIGINT Reports	Of the [redacted] serialized SIGINT reports issued, all but [redacted] were approved by the Chief or Acting Chief of ISS/S12. We are not considering the [redacted] instances as non-compliant because they were known and reported by NSA in the end-to-end report issued in 2009. In those instances, the Deputy Chief of ISS/S12, who was not stated in the BR Order as being authorized to approve BR-related dissemination outside NSA, signed the dissemination authorizations in the Chief's absence. ISS/S12 has since revised procedures to designate the Deputy Chief as Acting Chief in the Chief's absence.	We limited our testing to serialized SIGINT reports that were tracked [redacted] Other types of dissemination, such as briefings and responses to requests for information, were not easily testable because ISS/S12 used e-mails rather than dissemination authorizations to document approvals formally.	(b)(3)-P.L. 86-36 2009
6. Weekly Dissemination Reports	Weekly Dissemination Reports completely and accurately reported all [redacted] serialized SIGINT reports issued, except for one issued before weekly reports became mandated in June 2009.	To maintain consistency with our tests of dissemination authorizations, we limited testing to serialized SIGINT reports that were tracked in [redacted]	2009

(b)(1)
(b)(3)-P.L. 86-36

(TS//SI//NF)

This page intentionally left blank

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – January to March 2010 Test Results

(ST-10-0004A)

28 May 2010

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assesses whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

01 June 2010
IG-11160-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – January to March 2010 Test Results (ST-10-0004A)

1. (U//~~FOUO~~) This report summarizes the results of our January, February, and March 2010 testing using the continuous auditing methodology.

2. ~~(TS//SI//NF)~~ **Audit Objectives** We are conducting monthly testing of NSA controls to comply with the Foreign Intelligence Surveillance Court Business Records (BR) Order to determine whether these controls are operating as intended.

3. ~~(TS//SI//NF)~~ **Pilot Testing** The Pilot Test Report (IG-11154-10) was issued on 12 May 2010. It concluded that NSA had complied with the BR Order for the six pilot test objectives tested and within the time periods covered. Although no incidents of non-compliance were found, pilot testing disclosed weaknesses in controls over querying certain types of selectors, as well as concerns related to the dissemination of BR information. Weaknesses related to querying should be resolved with NSA's implementation of a new application to track BR selectors, which NSA now hopes to release in June 2010. We will monitor the situation as part of our monthly testing and make formal recommendations as needed.

4. (U//~~FOUO~~) **Monthly Test Objectives** See Appendices A - C for details of January, February, and March 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the Business Records FISA BRF metadata made by authorized individuals (e.g., analysts and data integrity analysts)?

- (U//~~FOUO~~) Reasonable Articulable Suspicion RAS Approval of Queried Selectors: Did all queries use RAS-approved seed selectors?

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S.-person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator (HMC)?

- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report serialized dissemination of BRF metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized SIGINT Reports with BRF Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

5. (U//~~FOUO~~) **Monthly Test Results** We found no instances of non-compliance for the months of January and February 2010. However, significant scope limitations remained for all months in testing Office of General Counsel (OGC) reviews of selectors associated with U.S. persons because of control weaknesses reported in the Pilot Test Report. Also, [redacted] we found an expired selector marked as approved [redacted] and queried for foreign intelligence purposes. The U.S. person selector [redacted] and was due for revalidation [redacted] based on the Court mandated 180-day requirement for revalidation of a U.S. person selector. This selector was then queried [redacted] after it had expired. The selector was changed to NOT APPROVED [redacted] After being notified of this non-compliance, Special FISA, Oversight, Processing and Support (SV4) issued an incident report [redacted] This error underscores the control weakness in selector revalidations that we reported in the Pilot Test Report. It also raises a question regarding separation of duties when Data Integrity Analysts (DIAs) are able to query for data integrity and foreign intelligence purposes. We will make formal recommendations to address these findings in a separate report.

(b)(3)-P.L. 86-36

6. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight

DISTRIBUTION:
D21
Chief,
Chief,
Chief, S2I4
Chief/TD,
DoJ

(b)(6)

cc:
Chief, D4 (J. DeLong)
Acting GC (P. Reynolds)
Chief, SV
DDCR, S1
Chief, S2
Chief, S2I
Chief, T12
Chief, T122
Chief, T1222
OGC IG POC
SID IG POC
TD IG POC
D1
D12
D13
D14

(b)(3)-P.L. 86-36

APPENDIX A

(U) January 2010 Test Results

(U) This page intentionally left blank.

(U) January 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the BR Order, with noted scope limitations, for the time period 1-31 January 2010. The rating definitions are included in Appendix D of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All queries from and queries from the were made by authorized individuals.	None	**Compliant**
2. RAS Approval of Queried Selectors	Of the queries performed in the seed selectors of were validated as approved. The remaining queries were for data integrity purposes. The seed selectors of queries were RAS approved. The remaining queries were for data integrity purposes.	**(b)(3)-P.L. 86-36** None	**Compliant**
3. OGC Review of U.S. Person Selectors	All RAS-approved U.S. person seed selectors queried in were reviewed by OGC for First Amendment concerns as required. No U.S. person seed selectors were queried in the	Because of a control weakness reported in the Pilot Test Report, we had to limit testing to seed selectors presumed to be associated with U.S. persons We did not review approvals of foreign selectors associated with U.S. persons because the existing database does not track this information.	**Compliant, with Scope Limitations**
4. Chaining	All queries from and the were chained to no more than three hops from the seed selector.	None	**Compliant**
5. Revalidation of Queried Selectors	The seed selectors queried for foreign intelligence purposes were approved by authorized HMCs within the Court's timeframes. The seed selectors that were not RAS approved were queried for data integrity purposes.	None	**Compliant**
6. Weekly Dissemination Reports	Weekly Dissemination Reports completely and accurately reported the serialized SIGINT reports issued.	We decided to limit testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable.	**Compliant**
7. Dissemination of Serialized SIGINT Reports with BRF Metadata	The Chief of Information Sharing Services approved the serialized SIGINT reports issued.	We decided to limit testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable.	**Compliant**

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

APPENDIX B

(U) February 2010 Test Results

(U) This page intentionally left blank.

(U) February 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the BR Order, with noted scope limitations, for the time period 1-28 February 2010. The rating definitions are included in Appendix D of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All queries from and queries from the were made by authorized individuals.	None	Compliant
2. RAS Approval of Queried Selectors	Of the queries performed in the seed selectors of were validated as approved. The remaining queries were for data integrity purposes. The seed selectors of queries were RAS approved. The remaining queries were for data integrity purposes.	(b)(3)-P.L. 86-36 None	Compliant
3. OGC Review of U.S. Person Selectors	All RAS-approved U.S. person seed selectors queried in were reviewed by OGC for First Amendment concerns as required. Only one U.S. person seed selector was queried in the it was RAS approved and reviewed by OGC for First Amendment concerns as required.	Due to a control weakness reported in the Pilot Test Report, we limited testing to seed selectors presumed to be associated with U.S. persons We did not review approvals of foreign selectors associated with U.S. persons because the existing database does not track this information.	Compliant, with Scope Limitations
4. Chaining	All queries from and the were chained to no more than three hops from the seed selector.	None	Compliant
5. Revalidation of Queried Selectors	The seed selectors queried for foreign intelligence purposes were approved by authorized HMCs within the Court's timeframes. The seed selectors that were not RAS approved were queried for data integrity purposes.	None	Compliant
6. Weekly Dissemination Reports	Weekly Dissemination Reports completely and accurately reported the serialized SIGINT reports issued.	We decided to limit testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable.	Compliant
7. Dissemination of Serialized SIGINT Reports with BRF Metadata	The Chief of Information Sharing Services (S12) or the S12 Deputy with authority granted in a Staff Processing Form (SPF) approved the serialized SIGINT reports issued.	We decided to limit testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable.	Compliant

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

APPENDIX C

(U) March 2010 Test Results

(U) This page intentionally left blank.

(U) March 2010 Test Results

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ Test results show that NSA complied with most requirements of the BR Order, with noted scope limitations, for the time period 1-31 March 2010. [redacted] The rating definitions are included in Appendix D of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All [redacted] queries from [redacted] and [redacted] queries from the [redacted] were made by authorized individuals.	None	Compliant
2. RAS Approval of Queried Selectors	Of the [redacted] queries performed in [redacted] the seed selectors of [redacted] were validated as approved. The remaining [redacted] queries were for data integrity purposes. The seed selectors of [redacted] queries were RAS approved. The remaining [redacted] queries were for data integrity purposes.	None (b)(3)-P.L. 86-36	Compliant
3. OGC Review of U.S. Person Selectors (b)(1) (b)(3)-P.L. 86-36	All [redacted] RAS-approved U.S. person seed selectors queried in [redacted] were reviewed by OGC for First Amendment concerns as required. [redacted] U.S. person seed selectors were queried in the [redacted] each was RAS approved and reviewed by OGC for First Amendment concerns as required.	Because of a control weakness reported in the Pilot Test Report, we limited testing to seed selectors presumed to be associated with U.S. persons [redacted] We did not review approvals of foreign selectors associated with U.S. persons because the existing database does not track this information.	Compliant, with Scope Limitations
4. Chaining	All [redacted] queries from [redacted] and the [redacted] were chained to no more than three hops from the seed selector.	None	Compliant
5. Revalidation of Queried Selectors	[redacted] of the [redacted] seed selectors queried for foreign intelligence purposes were approved by authorized HMCs within the Court's timeframes. The remaining [redacted] seed selectors that were not RAS approved were queried for data integrity purposes.	None	Non-compliant
6. Weekly Dissemination Reports	Weekly Dissemination Reports completely and accurately reported the [redacted] serialized SIGINT reports issued.	We decided to limit testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable.	Compliant
7. Dissemination of Serialized SIGINT Reports with BRF Metadata	The Chief of Information Sharing Services approved the [redacted] serialized SIGINT reports issued.	Testing was limited to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable.	Compliant

~~(TS//SI//NF)~~

(U) This page intentionally left blank.

APPENDIX D
(U) Rating System

(U) This page intentionally left blank.

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with Scope Limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records April 2010 Test Results

(ST-10-0004B)

10 June 2010

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assesses whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

10 June 2010
IG-11163-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – April 2010 Test Results (ST-10-0004B)

1. (U//~~FOUO~~) This report summarizes the results of our April 2010 testing using the continuous auditing methodology.

2. ~~(TS//SI//NF)~~ **Audit Objectives** We are conducting monthly testing of NSA controls to comply with the Foreign Intelligence Surveillance Court (FISC) Business Records (BR) Order to determine whether these controls are operating as intended.

3. (U//~~FOUO~~) **Monthly Test Results and Objectives** We found no instances of non-compliance for the month of April 2010. However, significant scope limitations remained in testing Office of General Counsel (OGC) reviews of selectors associated with U.S. persons because of control weaknesses reported in the Pilot Test Report issued on 12 May 2010 (IG-11154-10). This report details April 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries of the Business Records (BR) metadata made by authorized individuals (e.g., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?
- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?
- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S.-person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator (HMC)?
- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report serialized dissemination of BR metadata outside NSA?
- ~~(TS//SI//NF)~~ *Dissemination of Serialized SIGINT Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

4. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight

DISTRIBUTION:
D21 [redacted]
SV42 [redacted]
S12 [redacted]
S2I4 [redacted]
T1222 [redacted]
DoJ [redacted]

(b)(6)

cc:
D4 (J. DeLong)
Acting GC (P. Reynolds)
SV [redacted]
S1 [redacted]
S2 [redacted]
S2I [redacted]
T12 [redacted]
T122 [redacted]
T1222 [redacted]
OGC IG POC [redacted]
SID IG POC [redacted]
TD IG POC [redacted]
D1 [redacted]
D12
D13
D14

(b)(3)-P.L. 86-36

(U) This page intentionally left blank

(U) April 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the BR Order, with noted scope limitations, for the time period 1-30 April 2010.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All queries from and queries from the were made by authorized individuals.	None	**Compliant**
2. RAS Approval of Queried Selectors	Of the queries performed in the seed selectors of were validated as approved. The remaining queries were for data integrity purposes or were "ident lookups" The seed selectors of queries were RAS approved. The remaining queries were for data integrity purposes.	None **(b)(3)-P.L. 86-36**	**Compliant**
3. OGC Review of U.S. Person Selectors	All RAS-approved U.S. person seed selectors queried in were reviewed by OGC for First Amendment concerns as required. U.S. person seed selectors were queried in the were reviewed by OGC for First Amendment concerns as required.	Because of a control weakness reported in the Pilot Test Report, we had to limit testing to seed selectors presumed to be associated with U.S. persons We did not review approvals of foreign selectors associated with U.S. persons because the existing database does not track this information.	**Compliant, with scope limitations**
4. Chaining	All queries from and the were chained to no more than three hops from the seed selector.	None	**Compliant**
5. Revalidation of Queried Selectors	The seed selectors queried for foreign intelligence purposes were approved by authorized HMCs within the Court's timeframes. The seed selectors that were not RAS approved were queried for data integrity or "ident lookup" purposes.[1]	None	**Compliant**
6. Weekly Dissemination Reports	Weekly Dissemination Reports completely and accurately reported the serialized SIGINT reports issued.	We decided to limit testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable.	**Compliant**
7. Dissemination of Serialized SIGINT Reports with BR Metadata	The Chief of Information Sharing Services approved the serialized SIGINT reports issued.	We decided to limit testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable.	**Compliant**

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[1] ~~(C//REL TO USA, FVEY)~~ "Ident lookup" refers to querying a selector using to determine the approval status of a selector. In such cases, the Emphatic Access Restriction controls will prevent chaining of a selector that is not marked as approved for querying, and return an error message to the analyst. Because the selector was not actually chained, there is no violation of the Order.

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses

(ST-10-0004C)

29 September 2010

Derived From: NSA/CSS Classification Guide 1-52
Dated: 20070108
Declassify On: 20350712

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

29 September 2010
IG-11201-10

TO: DISTRIBUTION

~~(TS//SI//NF)~~ SUBJECT: Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C) — ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This report summarizes the results of our review of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records. We found that the delayed implementation of a new selector tracking application resulted in control weaknesses and the querying of an expired selector. Our review also identified a control weakness regarding data integrity functions. Management concurred with the findings and recommendations and has already completed one recommendation by implementing the new selector tracking application and verifying that controls are in place.

2. (U//~~FOUO~~) We incorporated management's comments in the report, where appropriate, and included the full text of management responses in Appendix D. As required by NSA/CSS Policy 1-60, *NSA/CSS Office of the Inspector General,* all recommendations and planned corrective actions are subject to follow-up until completion. Status reports should be directed to [redacted] Assistant Inspector General for Follow-up, at OPS 2B8076, Suite 6247, within 15 calendar days after target completion dates.

(b)(3)-P.L. 86-36

3. (U//~~FOUO~~) We appreciate the cooperation and courtesies extended to our personnel throughout the review. If you need additional information or clarification, please contact [redacted] on 963-2988s or by e-mail at [redacted]

George Ellard

GEORGE ELLARD
Inspector General

ST-10-0004C

(U//~~FOUO~~) DISTRIBUTION:

SV42
S2I4
S313
T132

cc:
DIRNSA
OGC
DOC (J. DeLong)
SID (W. Crumm)
S02
SV
S2
S2I
S3
S31
TD
T1
T12
T1222
T13
OGC IG POC
SID IG POC
TD IG POC

(b)(3)-P.L. 86-36

DOJ NSD

(b)(6)

IG
D/IG
D1/AIG for Follow-up
D11
D12
D13
D14

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses

I. (U) EXECUTIVE SUMMARY

(U) OVERVIEW

~~(TS//SI//NF)~~ In May 2010, the Office of the Inspector General issued a Pilot Test Report (IG-111545-10) as part of our ongoing audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (BR) (ST-10-0004). In the report, we identified three control weaknesses in querying BR metadata. We did not make formal recommendations because the release of [redacted] a new selector tracking application that would address those weaknesses, was believed to be imminent—first in April 2010 and then in May 2010. However, because [redacted] release date kept slipping (it was released on 25 June 2010) and because a March 2010 query of an expired selector underscored one of those reported control weaknesses and identified an additional weakness regarding data integrity functions, we recommended that Agency management take immediate action.

(b)(3)-P.L. 86-36

(U) HIGHLIGHTS

~~(TS//SI//NF)~~ While testing March 2010 data, we found that an expired selector marked as approved was queried by a Data Integrity Analyst (DIA) for what seemed to be foreign intelligence purposes. The Department of Justice reported the query as an incident of non-compliance in August 2010; however, NSA disagreed that the query constituted a violation because the reasonable articulable suspicion approval was valid for the time-bounded period queried. Regardless, the query raised the following concerns:

- ~~(C//REL TO USA, FVEY)~~ A DIA was able to query an expired selector because controls were not in place to prevent such queries and the manual process that management had temporarily put in place did not identify the selector as needing revalidation.

- ~~(TS//SI//NF)~~ DIAs can query BR metadata for both data integrity and foreign intelligence purposes, increasing the risk for non-compliance with the Order.

~~(TS//SI//NF)~~ Management concurred with the recommendations in our audit report and completed one. Specifically, management released [redacted] in June 2010 and has verified that controls are now in place to address selector revalidations and the two remaining control weaknesses that we reported in the Pilot Test Report.

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

II. (U) BACKGROUND

~~(TS//SI//NF)~~ Terms of the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR)

~~(TS//SI//NF)~~ The FISC BR Order requires that U.S. selectors be revalidated every 180 days and that all other selectors be revalidated every year. Data Integrity Analysts (DIAs) can query any selector, regardless of its approval status, for data integrity purposes. However, DIAs are prohibited from querying expired selectors (i.e., selectors not revalidated within the mandated timeframe) for foreign intelligence purposes. A Department of Justice (DoJ) National Security Division representative stated that a query made by a DIA to provide direct assistance to a foreign intelligence analyst constitutes querying for foreign intelligence purposes because the query results are shared with the analyst for intelligence analysis.

~~(C//REL TO USA, FVEY)~~ To meet the querying terms of the BR Order, NSA implemented standard operating procedures requiring DIAs to operate within the same control structure as foreign intelligence analysts when providing direct assistance. Specifically, these procedures require that DIAs use the standard login, which prevents such violations as querying selectors that are not approved when "reviewing telephone identifiers prior to and or after the issuance of a serialized report," and "[helping] analysts interpret and understand the results of their queries." When DIAs conduct data integrity analysis, procedures require that they use a special login that bypasses such controls. The procedures specify that DIAs should not use the bypass login when providing direct assistance to foreign intelligence analysts.

~~(TS//SI//NF)~~ Testing of Compliance with the BR Order

~~(TS//SI//NF)~~ We began our review by pilot testing compliance with six requirements of the BR Order relating to querying and dissemination. The goal was to ensure that each requirement was testable using the continuous auditing method. To determine whether controls are operating as intended, we are continuing our review with monthly testing of NSA compliance with seven requirements of the BR Order for 2010. To date, we have completed testing and reported results of data from January through July 2010.

(U) This page intentionally left blank.

III. (U) FINDINGS

~~(TS//SI//NF)~~ During our monthly testing of March 2010 data, we found that a U.S. selector had not been revalidated at 180 days, as mandated by the BR Order, and the selector remained "approved" for querying in the BR Foreign Intelligence Surveillance Act (FISA) database for 16 days past the expiration date. As a result, a DIA was able to query that selector, in possible violation of the Order. This incident occurred because adequate controls were not in place to revalidate reasonable articulable suspicion (RAS) determinations of selectors, as mandated by the Order. We reported this weakness, along with two others, in our Pilot Test Report. The incident also revealed an additional control weakness: DIAs can query BR metadata for both data integrity and foreign intelligence purposes, increasing the risk for non-compliance.

(U//~~FOUO~~) Expired Selector Was Queried

(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

~~(C//REL TO USA, FVEY)~~ While testing March 2010 data, we found that an expired selector marked as approved had been queried by a DIA for what seemed to be foreign intelligence purposes. The U.S. person selector had been approved [redacted] but had not been revalidated on its expiration date, [redacted] The selector was still marked as approved [redacted] when, in response to a customer request for information associated with 2009 reporting, a DIA queried the selector [redacted] The DIA followed standard operating procedures for providing direct assistance by using a standard login rather than bypassing querying controls and did not indicate in the justification field that the query was for data integrity purposes. The selector was changed to "not approved" [redacted] 16 days after its expiration. No other queries of this selector had been made.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//REL TO USA, FVEY)~~ Because the query seemed to have been conducted for foreign intelligence purposes, we notified management of the possible non-compliance incident, and Special FISA Oversight and Processing (SV42) issued an incident report on 25 May 2010. On 2 August 2010, the DoJ National Security Division reported the query as a compliance incident pursuant to Rule 10(c) of the FISC Rules of Procedure, effective 17 February 2006 (see Appendix C). However, NSA disagreed with DoJ that the query constituted a violation of the Order because the RAS approval was valid for the time-bounded period queried by the DIA to answer the client's technical question. NSA's position is described in detail in Appendix D.

(U//~~FOUO~~) Controls Were Not in Place

~~(C//REL TO USA, FVEY)~~ A DIA was able to query an expired selector because controls were not in place to prevent such queries and the manual process that management had temporarily put in place did not identify this selector as needing revalidation. This weakness, along with two others, was identified in our Pilot Test Report. We did not make recommendations at that time because we found no incidents of non-compliance and the control weaknesses were to be resolved with the release of [redacted] a new selector tracking application, then planned for May 2010. (b)(3)-P.L. 86-36

~~(C//REL TO USA, FVEY)~~ Because [redacted] release date kept slipping, the risk for non-compliance remained for requirements related to U.S. persons, selector revalidations, and time-restricted selectors. However, Agency management reported on 28 June 2010 that [redacted] had been released on 25 June 2010 and was operational.

(U) RECOMMENDATION 1

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Immediately verify that controls in the newly released version of [redacted] are functioning to:

a. prevent querying selectors associated with U.S. persons without a documented Office of General Counsel review for First Amendment considerations;

b. prevent querying selectors not revalidated within BR-mandated limits (180 days and one year for U.S. and foreign selectors, respectively); and

c. tag, track, and identify time-restricted selectors.

(U) (ACTION: Homeland Security Analysis Center [S2I4] with SV42)

(b)(3)-P.L. 86-36

(U) Management Response

(U//~~FOUO~~) **CONCUR.** Management concurred with the finding and recommendation and has taken appropriate action. [redacted] was implemented on 25 June 2010, and the Director of Compliance, Office of General Counsel, SID Oversight and Compliance, and DoJ representatives were provided demonstrations and expressed their approval.

(U) OIG Comment

(U//~~FOUO~~) Management has taken corrective action that meets the intent of the recommendation.

(U//~~FOUO~~) Analysts' Duties Are Not Clearly Defined and Separated

~~(C//REL TO USA, FVEY)~~ The March 2010 query of an expired selector revealed another weakness: DIAs can query selectors for data integrity and foreign intelligence purposes. The *Standards for Internal Control in the Federal Government* state that key duties and responsibilities should be divided among different people to reduce the risk for error and fraud. No one individual should control all key aspects of transactions or events. Although DIAs do not conduct target analysis or report on targets, they might help a foreign intelligence analyst with a question on a target. In those cases, the DIA is querying for foreign intelligence purposes, not data integrity, and must use the same rules as foreign intelligence analysts. These procedures require that DIAs and foreign intelligence analysts use a standard login that invokes controls over querying, such as preventing the querying of selectors with a status of "not approved." However, DIAs also use special logins that bypass such controls and allow them, for example, to query selectors that are not approved, which is permitted for data integrity analysis but puts DIAs at risk for querying for foreign intelligence purposes without controls.

~~(C//REL TO USA, FVEY)~~ The March 2010 incident revealed that the functions of DIAs are not clearly defined and communicated. It is unclear whether the DIA's query was for data integrity or foreign intelligence purposes. The standards for internal control require that key areas of authority and responsibility be defined and communicated throughout the organization. The standards also call for managers to document clearly such internal control mechanisms in management directives, administrative policies, or operating manuals that are readily available.

~~(TS//SI//NF)~~ Although S2I4 management stated that they discussed with DoJ the appropriate functions of DIAs, personnel did not have a common understanding of the types of queries appropriate for foreign intelligence and data integrity purposes. Furthermore, existing guidance did not clearly link the types of queries with the purpose of querying, and supplementary guidance was still in draft. For example, after we identified that an expired selector had been queried in March 2010, it was unclear whether the query had violated the FISC BR Order. Specifically, personnel had differences of opinion as to whether the query had been for foreign intelligence purposes and, therefore, a violation or for data integrity purposes, which is not a violation.

~~(TS//SI//NF)~~ Without clearly defined roles, a distinct separation of duties, and well-understood policies that differentiate queries for foreign intelligence and data integrity purposes, DIAs are vulnerable to errors

and violations of the FISC BR Order. In particular, DIAs might mistakenly query selectors for foreign intelligence purposes while using the special login that bypasses key controls.

(U) RECOMMENDATION 2

~~(TS//SI//NF)~~ Clearly define and separate the duties of DIAs and foreign intelligence analysts. Specifically, implement controls to prevent an individual from querying BR metadata for both data integrity and foreign intelligence purposes and issue formal guidance to differentiate such queries.

(U) (ACTION: Exploitation Solutions Office [S313] and Structured Repositories [T132])

(U) Management Response

(U//~~FOUO~~) **CONCUR.** Management concurred with the finding and recommendation and provided target completion dates. Management plans to move data integrity functions out of S2I4 and into S313, and T132 and will develop appropriate procedures and job descriptions.

(U) OIG Comment

(U//~~FOUO~~) Planned and ongoing actions meet the intent of our recommendation.

IV. (U) ACRONYMS AND ORGANIZATIONS

~~(TS//SI//NF)~~ BR	Business Records
(U) DIA	Data Integrity Analyst
(U) DoJ	Department of Justice
(U) FISA	Foreign Intelligence Surveillance Act
(U) FISC	Foreign Intelligence Surveillance Court
(U) RAS	reasonable articulable suspicion
(U) S2I4	Homeland Security Analysis Center
(U) S313	Exploitation Solutions Office
(U) SV42	Special FISA Oversight and Processing
(U) T132	Structured Repositories

(U) This page intentionally left blank.

(U) APPENDIX A

(U) Objective, Scope, and Methodology

(U) This page intentionally left blank.

(U) ABOUT THE AUDIT

(U) Objective, Scope, and Methodology

(U) Objective

~~(TS//SI//NF)~~ The overall objective of this audit is to test whether controls to ensure NSA compliance with key terms of the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR) are operating as intended. During the pilot test phase of the audit, our objective was to determine NSA compliance and assess the feasibility and reasonableness of including in monthly testing six objectives related to querying and dissemination. For monthly testing, our objective is to test NSA's compliance with seven requirements of the BR Order and determine whether controls are operating as intended.

(U) Scope and Methodology

(U) We conducted pilot testing from January to March 2010; monthly testing of January through July 2010 data was conducted from March to August 2010.

~~(TS//SI//NF)~~ For both pilot testing and monthly testing, we compared all selectors that were documented in [redacted] audit logs and had been queried each month against access lists, reasonable articulable suspicion approvals documented in the Foreign Intelligence Surveillance Act BR database, and Office of General Counsel reviews documented in the Homeland Requests Database. We also counted the number of hops chained for each selector in the [redacted] audit logs. For monthly testing, we also applied these tests to queries of the [redacted] We researched any anomalies to make a final determination of compliance.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) We met with individuals from the Office of General Counsel (OGC), the SIGINT Directorate, and the Technology Directorate, including the SID Office of Oversight and Compliance, Information Sharing Services, Homeland Security Analysis Center, SID Issues Support Staff, Analytic Capabilities, Structured Repositories, and [redacted] Operations.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Details on the scope and methodology used for pilot testing, including scope limitations, are included in our Pilot Test Report (IG-11154-10). Details on monthly testing are included in the January to March 2010 Test Report (IG-11160-10), April 2010 Test Report (IG-11163-10), May 2010 Test Report (IG-11174-10), June 2010 Test Report (IG-11179-10), and July 2010 Test Report (IG-11188-10).

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions according to our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions according to our audit objectives.

(U) APPENDIX B

(U) Summary of Recommendations

(U) This page intentionally left blank.

ST-10-0004C

(U) Summary of Recommendations

Recommendation 1

~~(TS//SI//NF)~~ Immediately verify that controls in the newly released version of [redacted] are in place and functioning to:

(b)(3)-P.L. 86-36

a. prevent querying selectors associated with U.S. persons without a documented OGC review for First Amendment considerations;

b. prevent querying selectors not revalidated within BR-mandated limits (180 days and one year for U.S. and foreign selectors, respectively); and

c. tag, track, and identify time-restricted selectors.

(U) Status: CLOSED

Recommendation 2

~~(TS//SI//NF)~~ Clearly define and separate the duties of data integrity analysts and foreign intelligence analysts. Specifically, implement controls to prevent an individual from querying BR metadata for data integrity and foreign intelligence purposes, and issue formal guidance to differentiate such queries (ACTION: Exploitation Solutions Office [S313] and T132).

(U) Status: OPEN

(U) Target Completion Dates: [redacted] for ~~S313~~ for T132

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) APPENDIX C

~~(TS//SI//NF)~~ DoJ Letter to FISC Regarding Incident Involving the BR Order

(U) This page intentionally left blank.

U.S. Department of Justice

National Security Division

2010 AUG -2 PM 4:32

TOP SECRET//COMINT//NOFORN

Washington, D.C. 20530

The Honorable John D. Bates
United States Foreign Intelligence Surveillance Court
U.S. Courthouse
333 Constitution Avenue, N.W.
Washington, D.C. 20001

Re: Compliance Incident Involving In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from AT&T, the Operating Subsidiaries of Verizon Communications Inc., and Cellco Partnership d/b/a Verizon Wireless, and Sprint Relating to al Qaeda and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with al Qaeda and Associated Terrorist Organizations and the Government of Iran and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with the Government of Iran and Associated Terrorist Organizations, Docket Number BR 10-10 (TS)

Dear Judge Bates:

Pursuant to Rule 10(c) of the Foreign Intelligence Surveillance Court (FISC) Rules of Procedure, effective February 17, 2006, this letter further advises the Court of a compliance incident regarding docket number BR 10-10. A preliminary notice regarding the incident was filed with the Court on July 26, 2010. (S)

On February 26, 2010, in docket number BR 10-10, Judge Reggie B. Walton approved an application for tangible things. Judge Walton renewed that authority on May 14, 2010, in docket number BR 10-17, expiring on August 6, 2010. The Court's Primary Order in docket number BR 10-10 states: "The BR metadata may be accessed for the purposes of ensuring data integrity and developing and testing any technological measures designed to enable the NSA to comply with the Court's orders." Docket Number BR 10-10, Primary Order at 5. "Persons who query the BR metadata pursuant to this paragraph may only share the results of any such query with other specially-cleared NSA technical personnel," with limited exceptions, including when "a data integrity analyst [DIA] conduct[s] the query using a RAS-approved telephone identifier at the request of an analyst authorized to query the BR metadata" *Id.* at 5-6. (TS//SI//NF)

On July 16, 2010, the National Security Agency (NSA) advised the Department of Justice's National Security Division of the compliance incident described below:

TOP SECRET//COMINT//NOFORN

Classified by: David S. Kris, Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: 2 August 2035

- On March 9, 2010, a DIA queried the BR metadata in response to a Federal Bureau of Investigation (FBI) request for certain information relating to a United States telephone identifier referenced in a previously issued NSA report. Specifically, the FBI inquired whether the BR metadata contained information indicating that the identifier was roaming during in the [redacted] to [redacted] time frame. (TS//SI//NF)

- The reasonable, articulable suspicion (RAS) approval for the identifier expired on [redacted] before the query. (It had been RAS-approved on [redacted].) Still, the identifier was listed on the Station Table – historically, NSA's list of identifiers that have undergone RAS determinations – as RAS-approved until [redacted], at which time its status was changed to "not approved." (TS//SI//NF)

- The DIA used the identifier to conduct a single query of the BR metadata in the Transaction Database. Although the preliminary notice of this incident reported that the query was time-bounded to the period of [redacted] through [redacted], the query was not time-bounded. Rather, the DIA focused his review of the query results to the time period referenced in the FBI's request for information. (TS//SI//NF)

- Based on the query results, the DIA determined that no roaming data was available for the identifier, and NSA provided that information to the FBI. NSA did not issue a report based on this query. (TS//SI//NF)

This incident was discovered by the staff of NSA's Inspector General through their review of controls used to comply with the Court's Orders in this matter. NSA confirms that it conducted no queries using the identifier after the DIA's query described above. (TS//SI//NF)

At the time of this incident, NSA managed the RAS-approval status of identifiers on the Station Table through a periodic, manual review of those identifiers. NSA assesses that this compliance incident resulted from delays in the manual review process. NSA further assesses that a technical modification likely will prevent this sort of compliance incident from occurring in the future. In June 2010, NSA implemented a new program to manage and track requests to approve the use of identifiers that meet the RAS standard. This new program, among other things, automatically changes an identifier's status to "not approved" if it has not been re-approved for RAS within the time frame specified by the Court's orders. (TS//SI//NF)

[redacted], Global Capabilities Manager, Counterterrorism, reviewed a draft of this letter and confirmed its accuracy. (U)

Sincerely,

[redacted]

Section Chief, Oversight
National Security Division
U.S. Department of Justice

cc: The Honorable Reggie B. Walton

(U) APPENDIX D

(U) Full Text of Management Response

(U) This page intentionally left blank.

~~TOP SECRET//COMINT//NOFORN~~ DOCID: 4230249 REF ID:A4197247

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
OIG	2010-4645	

THRU	ACTION	EXREG SUSPENSE
	☐ APPROVAL	18 Aug 2010
SUBJECT	☐ SIGNATURE	KCC SUSPENSE
~~(TS//SI//NF)~~ SID Response: Quick-Reaction Draft Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C)	X INFORMATION	ELEMENT SUSPENSE 2 Aug 2010

DISTRIBUTION
SID, S02, S2, SV, D4, T12, OGC

SUMMARY

PURPOSE: ~~(TS//SI//NF)~~ To provide the SID Response to the subject DRAFT Report.

BACKGROUND: ~~(TS//SI//NF)~~ In May 2010, the OIG issued the Pilot Test Report (IG-11154-10) as part of the ongoing audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR) (ST-10-0004). The pilot testing identified three control weaknesses in querying BR metadata as well as concerns related to the dissemination of information. Because there was no evidence of non-compliance and the release of the new selector tracking application that would address the weaknesses [redacted] was imminent, the OIG didn't make formal recommendations opting to monitor the situation and make formal recommendations as necessary.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ The continual slippage of [redacted] release date [redacted] released June 25, 2010) coupled with the March 2010 non-compliance incident (which underscored one of the reported control weaknesses and identified an additional weakness) resulted in the OIG recommending Agency management take immediate action. The subject quick-reaction draft report is the result of the problem that warranted immediate attention by Agency Management.

DISCUSSION: ~~(TS//SI//NF)~~ The SID Response to the subject document has been coordinated with S2, SV, T12, D4 and OGC. It includes the response to the two Recommendations for SID Lead and NSA's response to the DOJ's notice of violation. Also included for your reference is the SV42 response to the March 2010 incident relative to the subject report.

(b)(3)-P.L. 86-36

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
for SID DIR	[redacted] 8-20-2010	963-7400	D4	John DeLong//email//8/6/10	
S02	[redacted] 8/19/10		OGC	[redacted] //email//8/9/10	963-8309
S2	[redacted] //s//3 Aug 10	963-3335	S3	[redacted]	
SV	[redacted] //email//2 Aug 10	963-1705	[redacted]		
T12	[redacted] //email//8/6/10	963-0247			

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
SID IG Liaison, [redacted]	S023	966-5590	11 August 2010

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

FORM A6796

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

~~(TS//SI//NF)~~ SID Response: Quick-Reaction Draft Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records – Control Weaknesses (ST-10-0004C)

~~(TS//SI//NF)~~ **Introduction**: The SID Response has been coordinated with the Deputy Directorate for Analysis and Production (S2), SID Oversight and Compliance (SV), and the Office of General Counsel (OGC) because the same issue is being addressed in parallel channels at the SID level and above. The Department of Justice (DOJ) filed a 10c notice of violation with the Foreign Intelligence Surveillance Court (FISC) to which NSA, through OGC, is providing a non-concurrence on describing this event as a violation. NSA's response to DOJ is included in the Background and Context section of this document. It is being provided to ensure that NSA provides consistent responses and appropriate context to these parallel reporting actions. While NSA does not agree that this event was clearly an 'incident of non-compliance,' it does highlight deficiencies in the previous selector management application; nevertheless it falls short of a compliance violation.

(b)(3)-P.L. 86-36

RECOMMENDATION 1: ~~(TS//SI//NF)~~ Immediately verify that controls in the newly released version of [redacted] are in place and functioning to:

a) prevent querying selectors associated with U.S. persons without a documented OGC review for First Amendment considerations,

b) prevent querying selectors not revalidated within BR-mandated limits (180 days and one year for U.S. and foreign selectors, respectively), and

c) tag, track, and identify time-restricted selectors.

If the conditions in a, b, and c cannot be verified, immediately develop and implement interim plans to address these weaknesses until [redacted] can be modified.

SID Action Element: Chief, S2I4 with SV42 and T1222

SID RESPONSE (August 2010): (U//~~FOUO~~) SID concurs with this recommendation. On 25 June 2010 the new selector management system, [redacted] was activated and all deficiencies noted in the OIG report have been addressed. The OIG has been provided real time updates associated with this release and has interacted with S2I4's [redacted] liaison in order to perform their own review of the application. Additionally, the Office of the Director of Compliance (ODoC), Office of General Counsel (OGC), SID Oversight and Compliance (SV), Office of the Inspector General (OIG) and Department of Justice representatives have all had [redacted] functionalities demonstrated to them and expressed their approval (see additional information in Explanatory Remarks section)

POC: [redacted] Chief, S2I4, CT Homeland Security Analysis, [redacted] 969-0224

(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

~~(TS//SI//NF)~~ Quick-Reaction Draft Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C)

~~(TS//SI//NF)~~ March 2010 Non-Compliance Incident – Additional Information

~~(TS//SI//NF)~~ SID Oversight and Compliance/FISA Authorities (SV4) emphasizes that all of the items listed in recommendation 1 are procedures and features of the [redacted] program that have been in place since June 28, 2010. NSA Way [redacted] initial operating capability was concluded by T12 personnel on June 22, 2010. This acceptance should serve as the testing verification for the requirements set out in recommendation 1 of the subject report.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Operational testing and evaluation is on-going under real-world use while the developers and technical oversight personnel are monitoring "bug reports" and user feedback with a keen eye toward compliance issues. In addition, an Emergency Change process is established with a cross-organization technical and oversight team in place to resolve any compliance findings or to determine adjustments to the program should changes in the legal environment occur.

(U) SV42 proposal related to Recommendation 2.

~~(TS//SI//NF)~~ Below are the DIA roles and specific functions as defined in the Data Integrity Analyst [redacted] Standard Operating Procedures (SOP), dated September 28, 2009, while the DIA's were assigned to the SIGINT Directorate.

~~(TS//SI//NF)~~ In the SOP, the DIA's have three tools or roles within [redacted] to perform their functions: (b)(3)-P.L. 86-36

A. The first role [redacted] and was described as only for the use of providing support to analysts both in and out of the CT product line.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

B. The second available role [redacted] Within this second role was a list of typical support:

1. Reviewing telephone identifiers prior to and or after the issuance of a serialized report or a Request for Information (RFI) in order to verify the accuracy of the [redacted] data. (b)(3)-P.L. 86-36
2. Helping analysts interpret and understand the results of their queries.
3. Confirm [redacted]

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

C. The third role [redacted] which provides the DIA by-pass capability. This third tool was described for use in technical and data integrity purposes only and the by-pass capability was specifically called out not to be used to support functions in sections A. or B above.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ SV4 recommends that those offices that have taken on the functions, previously or currently known as the Data Integrity Analysts, establish a policy that clearly defines and prohibits the use of RAS by-pass modes while working on data for or assisting other analysts for intelligence analysis purposes.

~~(TS//SI//NF)~~ The policy should state that the use of any RAS by-pass functions should be limited to processing and data formatting purposes to ensure that the metadata is accurate and usable by analysts and to ensure compliance with the FISA Court Orders.

~~(TS//SI//NF)~~ The policy should allow that technical support personnel or DNR Subject Matter Experts working with BR FISA metadata should be able to continue to provide *technical* support to intelligence analysts for the purposes of assistance with accuracy and technical interpretation of the metadata with or without any RAS by-pass function enabled.

~~(TS//SI//NF)~~ However, the policy should strictly prohibit the use of a RAS by-pass function by technical support personnel or DNR Subject Matter Experts as described above to assist with or provide any analytic interpretation of results of queries against the BR FISA database that would supply any information of intelligence value.

POC: [redacted] SV42, 969-0024
Approved by: [redacted] *Chief SID Oversight and Compliance, 2 August 2010*

(b)(3)-P.L. 86-36

RECOMMENDATION 2: ~~(TS//SI//NF)~~ **Clearly define and separate the duties of Data Integrity Analysts and Foreign Intelligence Analysts. Specifically, implement controls to prevent an individual from querying BR metadata for data integrity and foreign intelligence purposes and issue formal guidance to differentiate such queries.**

(U) (ACTION: Chief, S2I4 with SV42 and T1222)

SID RESPONSE (August 2010): ~~(TS//SI//NF)~~ SID does not concur that this is an action for Chief, Homeland Security Analysis (S2I4) as stated in the recommendation. Counterterrorism (CT) Production Center (S2I) does not intend to retain individuals in a 'data integrity analyst' (DIA) capacity and is working to transition those functions to where they fit better within SID. The DIA function is one of the legacy constructs tracing back to a former NSA compartmented program. The DIA's role was not clearly distinct from target analysts. S2I4 determined during the end-to-end reviews that data integrity analyst functions should be moved out of the production organization and aligned with other corporate elements within SID's SIGDEV Strategy and Governance (SSG) and Deputy Directorate for Data Acquisition (S3), who perform similar functions related to data integrity and fidelity at the point of ingest. Transition of DIA functions, not DIA positions, is ongoing with Cryptanalysis and Exploitation Services (CES) (S31)/Exploitation Solutions Office (ESO)(S313) and SSG. S2I has been working with Chief, Protocol Exploitations (S31323) on this transition of functions. S2I4 leadership has asked TD to relocate the single remaining DIA (a TD resource) to T spaces. The analyst who performed the March 2010 query recently took a new job in SSG.

POC: [redacted] Chief, S2I4, CT Homeland Security Analysis, [redacted] 969-0224
POC: [redacted] Chief S313, Exploitation Solutions Office, [redacted] 963-3101

(U) Background and Context:

(b)(3)-P.L. 86-36

~~(C//REL TO USA, FVEY)~~ Where S2I4 diverges from this report as written is in the description of the query performed in March 2010 as an 'Incident of Non-Compliance'. The report fails to provide adequate background context.

~~(TS//SI//NF)~~ The following was provided to OGC and DOJ for review as an explanation of the chain of events in the course of DOJ filing an initial 10c:

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ S2I4 has no contention that the query performed and noted in an OIG audit highlighted specific deficiencies in the legacy applications used to manage RAS approved selectors. These same findings were noted during the End-to-End reviews of both the Business Records and Pen Register Trap & Trace FISA programs. S2I4 leadership strongly agreed with the recommendation to delay the release of the application until such time as: 1) the End-to-End review findings were complete and had been fully discussed with DOJ and 2) those findings could be incorporated into to address compliance vulnerabilities. (b)(3)-P.L. 86-36

~~(S//NF)~~ A new revalidation process was established and implemented in the fall of 2009, albeit a completely manual process as was being re-engineered. Prior to release each program had a separate and distinct underpinned by its own application, leaving NSA with a purely manual process during this transition. S2I4 and TD counterparts validated all previous 'customer requirements' for and worked through the 'NSA Way' process to completion. SV and OGC are also 'customers' of this application and along with ODoC, had visibility into the entire revamping process. This engagement continues to address any issues noted after release. (b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Nonetheless, the legacy system's deficiency allowed a DIA to query on a selector that should have no longer been retained in as RAS approved. It should be noted however, the DIA could still have queried on that selector as part of their 'data integrity' duties --- within the bounds of the order and without RAS approval.

(U//~~FOUO~~) Explanatory Remarks related to Recommendation 1:

a) ~~(S//NF)~~ Any selector being reviewed for RAS that is a US identifier or is believed to be in use by a US person cannot be RAS approved without an OGC First Amendment review. As the nomination is entered into a field to note whether the selector is foreign or domestic must be populated for the nomination to be processed. When the domestic field is populated, sends the nomination to OGC for review and no further action can be taken until that review is completed. (b)(3)-P.L. 86-36

b) ~~(TS//SI//NF)~~ As a selector is approved within the selector management system, a revalidation date is set tied to the date of approval

and whether it is US or foreign. HSAC [Homeland Security Advisory Council] internal management guidelines are that all US selectors will be revalidated every 90 days and foreign selectors at 180 days. This protocol should preclude any instance of exceeding FISC mandated timeframes. [redacted] will automatically move these selectors into a pending status 15 days from the projected 'expiration'. If any selector in this status has not been revalidated by the cut-off date, [redacted] moves the selector into an expired state. The selector is no longer noted as 'RAS approved' in the system [redacted] and [redacted] is informed of this action in order to ensure this selector can no longer be queried in the [redacted] BRF or PR/TT repositories.

(b)(3)-P.L. 86-36

c) ~~(C//REL TO USA, FVEY)~~ 'Time Bounded Query' restrictions have their own icon which prompts an analyst to check a selector's record within the [redacted] system. This record notates the time restriction and informs analysts of the specific timeframe they must focus on during the review of query results. Information outside of those boundaries must not be used in the pursuit of their targets. [redacted]

POC: [redacted] Chief, S2I4, CT Homeland Security Analysis, [redacted] 969-0224

Approved by: DDAP, [redacted] 3 Aug 10

(b)(3)-P.L. 86-36

Quick Reaction Draft Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C)

RECOMMENDATION 2: ~~(TS//SI//NF)~~ Clearly define and separate the duties of Data Integrity Analysts (DIA) and Foreign Intelligence Analysts. Specifically, implement controls to prevent an individual from querying BR metadata for data integrity and foreign intelligence purposes and issue formal guidance to differentiate such queries.

S3 Input: ~~(TS//SI//NF)~~ S3 has accepted responsibility for performing the functions of the Data Integrity Analysts and determined this mission will be performed within the [redacted] Based on S3 direction, it is expected that [redacted] will have an interim procedure to perform DIA functions in place within three weeks, working toward a permanent procedure to be in place within three months.

(b)(1)
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20350901

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records May 2010 Test Results

(ST-10-0004D)

30 June 2010

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assesses whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

30 June 2010
IG-11174-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – May 2010 Test Results (ST-10-0004D)

1. (U) This report summarizes the results of our May 2010 testing using the continuous auditing methodology.

2. ~~(TS//SI//NF)~~ **Audit Objectives** We are conducting monthly testing of NSA controls to comply with the Foreign Intelligence Surveillance Court (FISC) Business Records (BR) Order to determine whether these controls are operating as intended.

3. (U//~~FOUO~~) **Monthly Test Results and Objectives** We found no instances of non-compliance for the month of May 2010. However, significant scope limitations remained in testing Office of General Counsel (OGC) reviews of selectors associated with U.S. persons because of control weaknesses reported in the Pilot Test Report issued on 12 May 2010 (IG-11154-10). See page 4 for details of May 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (e.g., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?
- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?
- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator (HMC)?
- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report serialized dissemination of BR metadata outside NSA?
- ~~(TS//SI//NF)~~ *Dissemination of Serialized SIGINT Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

4. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted], or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight

DISTRIBUTION:

D21 [redacted]
SV42 [redacted]
S12 [redacted]
S2I4 [redacted]
T1222 [redacted]
DoJ [redacted]

(b)(6) (b)(3)-P.L. 86-36

cc:

D4 (J. DeLong)
Acting GC (P. Reynolds)
SV [redacted]
S1 [redacted]
S2 [redacted]
S2I [redacted]
T12 [redacted]
T122 [redacted]
T1222 [redacted]
OGC IG POC [redacted]
SID IG POC [redacted]
TD IG POC [redacted]
D1 [redacted]
D12
D13
D14

(U) This page left intentionally blank

(U) May 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the BR Order, with noted scope limitations, between 1-31 May 2010. The rating definitions are included on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All queries from and queries from the were made by authorized individuals.	None	**Compliant**
2. RAS Approval of Queried Selectors	Of the queries performed in the seed selectors of were validated as approved. The remaining queries were for data integrity purposes or were "ident lookups."[1] The seed selectors of queries were RAS approved. The remaining queries were for data integrity purposes.	None	**Compliant**
3. OGC Review of U.S. Person Selectors	All RAS-approved U.S. person seed selectors queried in were reviewed by OGC for First Amendment concerns as required. U.S. person seed selectors were queried in the each was reviewed by OGC for First Amendment concerns, as required.	Because of a control weakness reported in the Pilot Test Report, we had to limit testing to seed selectors presumed to be associated with U.S. persons We did not review approvals of foreign selectors associated with U.S. persons, because the existing database does not track this information.	**Compliant, with scope limitations**
4. Chaining	All queries from and the were chained to no more than three hops from the seed selector.	None	**Compliant**
5. Revalidation of Queried Selectors	The seed selectors queried for foreign intelligence purposes were approved by authorized HMCs within the Court's timeframes. The seed selectors that were not RAS approved were queried for data integrity or "ident lookups"	None	**Compliant**
6. Weekly Dissemination Reports	Weekly Dissemination Reports completely and accurately reported the serialized SIGINT reports issued.	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**
7. Dissemination of Serialized SIGINT Reports with BR Metadata	The Chief or Acting Chief of Information Sharing Services (S12) approved the serialized SIGINT reports issued.	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[1] ~~(C//REL TO USA, FVEY)~~ "Ident lookups" refers to querying a selector to determine the approval status of a selector. In such cases, the Emphatic Access Restriction controls prevent chaining of a selector that is not marked as approved for querying and return an error message to the analyst. There is no violation of the Order, because the selector was not actually chained.

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records June 2010 Test Results

(ST-10-0004E)

20 July 2010

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20350709

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

19 July 2010
IG-11179-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – June 2010 Test Results (ST-10-0004E)

1. (U) This report summarizes the results of our June 2010 testing using the continuous auditing methodology.

2. ~~(TS//SI//NF)~~ **Audit Objectives** We are conducting monthly testing of NSA controls to comply with the Foreign Intelligence Surveillance Court (FISC) Business Records (BR) Order to determine whether these controls are operating as intended.

3. ~~(C//REL TO USA, FVEY)~~ **Monthly Test Results and Objectives** We found no instances of non-compliance for the month of June 2010. However, for the five test objectives related to querying, we limited the testing of data from [redacted] to 1-25 June 2010 as a result of the 25 June 2010 [redacted] implementation. In addition, significant scope limitations remained in testing Office of General Counsel (OGC) reviews of selectors associated with U.S. persons because of control weaknesses reported in the Pilot Test Report issued on 12 May 2010 (IG-11154-10). See page 5 for details of June 2010 monthly test results for the following objectives:

(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (e.g., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20350709

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator (HMC)?

- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report serialized dissemination of BR metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized SIGINT Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

4. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted], or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight

DISTRIBUTION:
D21
SV42
S12
S2I4
T1222
DoJ

(b)(6)

cc:
Director
SIGINT Director
D4 (J. DeLong)
GC (M. Olsen)
SV
SV4
S1
S2
S2I
T12
T122
T1222
OGC IG POC
SID IG POC
TD IG POC
D1
D12
D13
D14

(b)(3)-P.L. 86-36

This page intentionally left blank.

(U) June 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with 1) the querying requirements of the BR Order, with noted scope limitations, between 1-25 June 2010, and 2) the dissemination requirements of the BR Order for the entire month. The rating definitions are included on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All queries from and queries from the were made by authorized individuals.	None	**Compliant**
2. RAS Approval of Queried Selectors	Of the queries performed in the seed selectors of were validated as approved. The remaining queries were for data integrity purposes or were "ident lookups".[1] The seed selectors of queries were RAS approved. The remaining queries were for data integrity purposes.	None	**Compliant**
3. OGC Review of U.S. Person Selectors	All RAS-approved U.S. person seed selectors queried in were reviewed by OGC for First Amendment concerns as required. U.S. person seed selectors were queried in the each was reviewed by OGC for First Amendment concerns as required.	Based on a control weakness reported in the Pilot Test Report, we limited testing to seed selectors presumed to be associated with U.S. persons We did not review approvals of foreign selectors associated with U.S. persons, because the existing database does not track this information.	**Compliant, with scope limitations**
4. Chaining	All queries from and the were chained to no more than three hops from the seed selector.	None	**Compliant**
5. Revalidation of Queried Selectors	The seed selectors queried for foreign intelligence purposes were approved by authorized HMCs within the Court's timeframes. The seed selectors that were not RAS approved were queried for data integrity or "ident lookups".	None	**Compliant**
6. Weekly Dissemination Reports	Weekly Dissemination Reports completely and accurately reported the serialized SIGINT reports issued.	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**
7. Dissemination of Serialized SIGINT Reports with BR Metadata	The Acting Chief or Acting Deputy Chief of Information Sharing Services (S12) approved the serialized SIGINT reports issued.	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[1](TS//SI//NF) "Ident lookups" refers to querying a selector to determine the approval status of a selector. In such cases, the Emphatic Access Restriction controls prevent chaining of a selector that is not marked as approved for querying and return an error message to the analyst. There is no violation of the BR Order, because the selector was not actually chained.

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records July 2010 Test Results

(ST-10-0004F)

18 August 2010

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20350805

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

18 August 2010
IG-11188-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – July 2010 Test Results (ST-10-0004F)

1. ~~(TS//SI//NF)~~ **Background** This report summarizes the results of our July 2010 testing using the continuous auditing methodology. The OIG is using this methodology as a means of complying with the oversight responsibilities assigned to it in the Business Records (BR) Court Order. Specifically, we are conducting monthly testing of NSA controls to comply with the Foreign Intelligence Surveillance Court (FISC) BR Order to determine whether these controls are operating as intended.

2. ~~(C//REL TO USA, FVEY)~~ **Monthly Test Results and Objectives** We found no instances of non-compliance for the month of July 2010. For the five test objectives related to querying, July testing included data from [redacted] for 26–30 June 2010. We excluded this data from June testing because of the implementation of [redacted] on 25 June 2010. [redacted] also resolved a significant scope limitation in our testing of Office of General Counsel (OGC) reviews of selectors associated with U.S. persons, as all U.S. selectors are now tracked. **(b)(3)-P.L. 86-36**

(U) See page 5 for details of July 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (e.g., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20350805

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator (HMC)?

- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report disseminations of BR metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized SIGINT Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

[redacted]
Assistant Inspector General
for Intelligence Oversight

(b)(3)-P.L. 86-36

DISTRIBUTION:
D21
SV42
S12
S2I4
T1222
DoJ

(b)(6) cc:
Director
SIGINT Director
D4 (J. DeLong)
GC (M. Olsen)
SV
SV4
S1
S2
S2I
T12
T122
T1222
OGC IG POC
SID IG POC
TD IG POC
D1
D12
D13
D14

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) July 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with 1) the querying requirements of the BR Order between 26 June – 31 July 2010, and 2) the dissemination requirements of the BR Order for the entire month. The rating definitions are included on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All queries from and queries from the were made by authorized individuals.	None	Compliant
2. RAS Approval of Queried Selectors	Of the queries performed in the seed selectors of were validated as approved. The remaining queries were for data integrity purposes. The seed selectors of queries were RAS approved. The remaining queries were for data integrity purposes.	None	Compliant
3. OGC Review of U.S. Person Selectors	The RAS-approved U.S. person seed selectors queried in were reviewed by OGC for First Amendment concerns as required. U.S. person seed selectors were queried in the each was reviewed by OGC for First Amendment concerns as required.	None	Compliant
4. Chaining	In accordance with our test plan, we did not test July 2010 data for this objective. Because we have noted no exceptions for the last six months of testing, we will not test this objective again until October 2010 (using September data) and January 2011 (using December data).		
5. Revalidation of Queried Selectors	The seed selectors queried for foreign intelligence purposes were approved by authorized HMCs within the Court's timeframes. The seed selectors that were not RAS approved were queried for data integrity purposes.	None	Compliant
6. Weekly Dissemination Reports	Weekly Dissemination Reports completely and accurately reported the serialized SIGINT reports issued.	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	Compliant
7. Dissemination of Serialized SIGINT Reports with BR Metadata	The Deputy Chief of Information Sharing Services (S12) approved the serialized SIGINT reports issued.	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	Compliant

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-Compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records August 2010 Test Results

ST-10-0004G
28 September 2010

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assesses whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

28 September 2010
IG-11202-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – August 2010 Test Results (ST-10-0004G)

1. ~~(TS//SI//NF)~~ **Background** This report summarizes the results of our August 2010 testing, using the continuous auditing methodology, of NSA's compliance with the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR). The Office of the Inspector General (OIG) is using this methodology to fulfill the oversight responsibilities assigned to it in the FISC BR Order. Specifically, from January to December 2010, we are conducting monthly tests of NSA's compliance with certain requirements of the FISC BR Order. Once monthly testing is complete, the OIG will make an overall assessment of whether the controls that are in place to ensure such compliance are operating as intended.

2. ~~(C//REL TO USA, FVEY)~~ **Monthly Test Results and Objectives** We found no instances of non-compliance for the month of August 2010. The implementation of [redacted] on 25 June 2010 resolved a significant scope limitation in our testing of Office of General Counsel (OGC) reviews of selectors associated with U.S. persons because all U.S. selectors are now tracked.

(b)(3)-P.L. 86-36

(U) See page 5 for details of August 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (i.e., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20350916

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator?

- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report disseminations of BR metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized Signals Intelligence (SIGINT) Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight

DISTRIBUTION:

D21 [redacted]
SV42 [redacted]
S12 [redacted]
S2I4 [redacted]
T1222 [redacted]
DoJ [redacted]

(b)(6)

cc:
Director
SIGINT Director
D4 (J. DeLong)
GC (M. Olsen)
SV [redacted]
SV4 [redacted]
S1 [redacted]
S2 [redacted]
S2I [redacted]
T12 [redacted]
T122 [redacted]
T1222 [redacted]
OGC IG POC [redacted]
SID IG POC [redacted]
TD IG POC [redacted]
D1 [redacted]
D12
D13
D14

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) August 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR) between 1 and 31 August 2010. The ratings are defined on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All queries from and queries from the were made by authorized individuals.	None	Compliant
2. Reasonable articulable suspicion (RAS) approval of queried selectors	Of the queries performed in the seed selectors of were validated as approved. The remaining queries were for data integrity purposes. The seed selectors of all queries were RAS approved.	None (b) (3)-P.L. 86-36	Compliant
3. Office of General Counsel (OGC) review of U.S. person selectors	The RAS-approved U.S. person seed selectors queried in were reviewed by OGC for First Amendment concerns, as required.	None	Compliant
(b) (1) (b) (3)-P.L. 86-36 4. Chaining	In accordance with our test plan, we did not test August 2010 data for this objective. Because we have not noted any exceptions for the past six months of testing, we will not test this objective again until October 2010 (using September data) and January 2011 (using December data).		
5. Revalidation of queried selectors	The seed selectors queried for foreign intelligence purposes were approved by authorized Homeland Mission Coordinators within the Court's timeframes. The seed selectors that were not RAS approved were queried for data integrity purposes.	None	Compliant
6. Weekly dissemination reports		We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	Compliant
7. Dissemination of serialized SIGINT reports with BR metadata		We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	Compliant

~~(TS//SI//NF)~~

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records September 2010 Test Results

(ST-10-0004H)

28 October 2010

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20351020

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

28 October 2010
IG-11213-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – September 2010 Test Results (ST-10-0004H)

1. ~~(TS//SI//NF)~~ **Background** This report summarizes the results of our September 2010 testing, using the continuous auditing methodology, of NSA's compliance with the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR). The Office of the Inspector General (OIG) is using this methodology to fulfill the oversight responsibilities assigned to it in the FISC BR Order. Specifically, from January to December 2010, we are conducting monthly tests of NSA's compliance with certain requirements of the FISC BR Order. Once monthly testing is complete, the OIG will make an overall assessment of whether the controls that are in place to ensure such compliance are operating as intended.

(b)(3)-P.L. 86-36 2. ~~(C//REL TO USA, FVEY)~~ **Monthly Test Results and Objectives** We found no instances of non-compliance for the month of September 2010. The implementation of [redacted] on 25 June 2010 resolved a significant scope limitation in our testing of Office of General Counsel (OGC) reviews of selectors associated with U.S. persons because all U.S. selectors are now tracked.

(U) See page 5 for details of September 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (i.e., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20351020

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator?

- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report disseminations of BR metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized Signals Intelligence (SIGINT) Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight

DISTRIBUTION:
D21
SV42
S12
S2I4
T122 Technical Director
DoJ
(b)(6)

cc:
Director
SIGINT Director
D4 (J. DeLong)
GC (M. Olsen)
SV
SV4
S1
S2
S2I
T12
T122
T1222
OGC IG POC
SID IG POC
TD IG POC
D1
D12
D13
D14

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) September 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR) between 1 and 30 September 2010. The ratings are defined on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	Authorized individuals made all [redacted] Chain [redacted] queries from [redacted]	None	**Compliant**
2. Reasonable articulable suspicion (RAS) approval of queried selectors	Of the [redacted] Chain [redacted] queries performed in [redacted] all seed selectors were validated as RAS approved.	None	**Compliant**
3. Office of General Counsel (OGC) review of U.S. person selectors	The [redacted] RAS-approved U.S. person seed selectors queried in [redacted] were reviewed by OGC for First Amendment concerns, as required.	None (b)(3)-P.L. 86-36	**Compliant**
4. Chaining	All [redacted] Chain [redacted] queries were chained to no more than three hops from the seed selector.	None	**Compliant**
5. Revalidation of queried selectors	The [redacted] seed selectors queried for foreign intelligence purposes were approved by authorized Homeland Mission Coordinators within the Court's timeframes.	None	**Compliant**
6. Weekly dissemination reports (WDRs)	WDRs completely and accurately reported the [redacted] serialized Signals Intelligence (SIGINT) reports issued.	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**
7. Dissemination of serialized SIGINT reports with BR metadata	The Chief of Information Sharing Services (S12) approved the [redacted] serialized SIGINT reports issued.	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

[1] ~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records October 2010 Test Results

ST-10-0004I

01 December 2010

DERIVED FROM: NSA/CSS Manual 1-52
DATED: 08 January 2007
DECLASSIFY ON: 20320108

(U) NSA OFFICE OF THE INSPECTOR GENERAL

(U) The NSA Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA activities are conducted in compliance with the law. The OIG also serves as an ombudsman, assisting Agency employees, civilian and military, with complaints and questions.

(U) Intelligence Oversight

(U) The OIG Office of Intelligence Oversight reviews NSA's most sensitive and high-risk programs for compliance with the law.

(U) Audits

(U) The OIG Office of Audits within the OIG provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether NSA operations comply with federal policies. Information Technology audits determine whether IT solutions meet customer requirements, while conforming to information assurance standards. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) Investigations and Special Inquiries

(U) The OIG Office of Investigations administers a system for receiving and acting on requests for assistance and complaints about fraud, waste, and mismanagement. Investigations and special inquiries may be undertaken as a result of such requests and complaints (including anonymous tips), at the request of management, as the result of questions that surface during inspections and audits, or at the initiative of the Inspector General.

(U) Field Inspections

(U) The Office of Field Inspections conducts site reviews as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with an assessment of compliance with federal policy. The Office partners with Inspectors General of Service Cryptologic Components and other Intelligence Community Agencies to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

1 December 2010
IG-11229-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – October 2010 Test Results (ST-10-0004I)

1. ~~(TS//SI//NF)~~ **Background** This report summarizes the results of our October 2010 testing, using the continuous auditing methodology, of NSA's compliance with the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR). The Office of the Inspector General (OIG) is using this methodology to fulfill the oversight responsibilities assigned to it in the FISC BR Order. Specifically, from January to December 2010, we are conducting monthly tests of NSA's compliance with certain requirements of the FISC BR Order. Once monthly testing is complete, the OIG will make an overall assessment of whether the controls that are in place to ensure such compliance are operating as intended.

2. ~~(TS//SI//NF)~~ **Monthly Test Results and Objectives** For the month of October 2010, we found that one weekly dissemination report mistakenly listed as a serialized dissemination that was not derived from BR metadata. Although the error did not violate the BR Order, it underscores a weakness in the largely manual process to track and report BR disseminations that we noted in our *Advisory Report on the Audit of NSA Controls to Comply with the FISC Order Regarding Business Records*, dated 12 May 2010. The error is currently being corrected.

(U) See pages 5 and 6 for details of October 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (i.e., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20351115

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator?

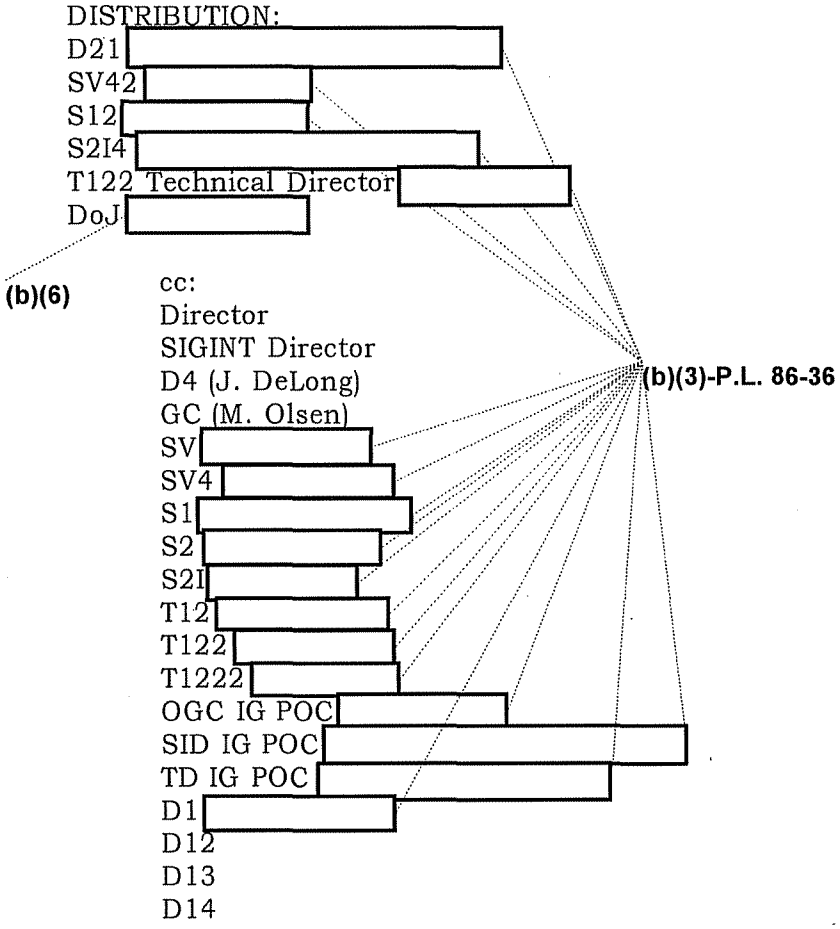
- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report disseminations of BR metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized Signals Intelligence (SIGINT) Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight


DISTRIBUTION:
D21
SV42
S12
S2I4
T122 Technical Director
DoJ
(b)(6)
cc:
Director
SIGINT Director
D4 (J. DeLong)
GC (M. Olsen)
SV
SV4
S1
S2
S2I
T12
T122
T1222
OGC IG POC
SID IG POC
TD IG POC
D1
D12
D13
D14
(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) October 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR) between 1 and 31 October 2010, with the exception of accurate and complete weekly dissemination reports. The ratings are defined on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All [ ] Chain [ ] queries from [ ] and [ ] queries from the [ ] were made by authorized individuals.	None	Compliant
2. Reasonable articulable suspicion (RAS) approval of queried selectors	Of the [ ] Chain [ ] queries performed in [ ] the seed selectors of [ ] were validated as approved. The remaining queries were for data integrity purposes [ ] or were "ident lookups" [ ][2]. The seed selectors of all [ ] queries were RAS approved.	None (b)(3)-P.L. 86-36	Compliant
3. Office of General Counsel (OGC) review of U.S. person selectors	The [ ] RAS-approved U.S. person seed selectors queried in [ ] and the [ ] were reviewed by OGC for First Amendment concerns, as required.	None	Compliant
4. Chaining	A total of [ ] Chain [ ] queries from [ ] and the [ ] were chained to no more than three hops from the seed selector. One chain query from [ ] was chained beyond the three-hop limit but was for testing purposes and allowable under the BR 10-49 Declaration.	None	Compliant
5. Revalidation of queried selectors	The [ ] seed selectors queried for foreign intelligence purposes were approved by authorized Homeland Mission Coordinators within the Court's timeframes. The [ ] seed selectors that were not RAS approved were queried for data integrity [ ] or were "ident lookups" [ ]	None	Compliant

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[1] ~~(TS//SI//NF)~~ [ ]

[2] ~~(TS//SI//NF)~~ "Ident lookup" refers to querying a selector using [ ] to determine the approval status. In such cases, the Emphatic Access Restriction controls prevent chaining of a selector that is not marked as approved for querying and return an error message to the analyst. There is no violation of the BR Order because the selector was not actually chained. (b)(3)-P.L. 86-36

Area	Test Results	Scope Limitations	Rating
6. Weekly dissemination reports (WDRs)		We limited testing to serialized Signals Intelligence (SIGINT) reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**
7. Dissemination of serialized SIGINT reports with BR metadata		We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

1 December 2010
IG-11229-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – October 2010 Test Results (ST-10-0004I)

1. ~~(TS//SI//NF)~~ **Background** This report summarizes the results of our October 2010 testing, using the continuous auditing methodology, of NSA's compliance with the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR). The Office of the Inspector General (OIG) is using this methodology to fulfill the oversight responsibilities assigned to it in the FISC BR Order. Specifically, from January to December 2010, we are conducting monthly tests of NSA's compliance with certain requirements of the FISC BR Order. Once monthly testing is complete, the OIG will make an overall assessment of whether the controls that are in place to ensure such compliance are operating as intended.

2. ~~(TS//SI//NF)~~ **Monthly Test Results and Objectives** For the month of October 2010, we found that one weekly dissemination report mistakenly listed as a serialized dissemination that was not derived from BR metadata. Although the error did not violate the BR Order, it underscores a weakness in the largely manual process to track and report BR disseminations that we noted in our *Advisory Report on the Audit of NSA Controls to Comply with the FISC Order Regarding Business Records*, dated 12 May 2010. The error is currently being corrected.

(U) See pages 5 and 6 for details of October 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (i.e., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20351115

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator?

- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report disseminations of BR metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized Signals Intelligence (SIGINT) Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight

DISTRIBUTION:
D21
SV42
S12
S2I4
T122 Technical Director
DoJ

(b)(6)

cc:
Director
SIGINT Director
D4 (J. DeLong)
GC (M. Olsen)
SV
SV4
S1
S2
S2I
T12
T122
T1222
OGC IG POC
SID IG POC
TD IG POC
D1
D12
D13
D14

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) October 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR) between 1 and 31 October 2010, with the exception of accurate and complete weekly dissemination reports. The ratings are defined on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	All [redacted] Chain [redacted] queries from [redacted] and [redacted] queries from [redacted] were made by authorized individuals.	None	**Compliant**
2. Reasonable articulable suspicion (RAS) approval of queried selectors	Of the [redacted] Chain [redacted] queries performed in [redacted] the seed selectors of [redacted] were validated as approved. The remaining queries were for data integrity purposes [redacted] or were "ident lookups." [redacted][2] The seed selectors of all [redacted] queries were RAS approved.	None	**Compliant**
3. Office of General Counsel (OGC) review of U.S. person selectors	The [redacted] RAS-approved U.S. person seed selectors queried in [redacted] and the [redacted] were reviewed by OGC for First Amendment concerns, as required.	**(b)(3)-P.L. 86-36** None	**Compliant**
4. Chaining	A total of [redacted] Chain [redacted] queries from [redacted] and the [redacted] were chained to no more than three hops from the seed selector. One chain query from [redacted] was chained beyond the three-hop limit but was for testing purposes and allowable under the BR 10-49 Declaration.	None	**Compliant**
5. Revalidation of queried selectors	The [redacted] seed selectors queried for foreign intelligence purposes were approved by authorized Homeland Mission Coordinators within the Court's timeframes. The [redacted] seed selectors that were not RAS approved were queried for data integrity [redacted] or were "ident lookups" [redacted]	None	**Compliant**

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[1] ~~(TS//SI//NF)~~ [redacted]

[2] ~~(TS//SI//NF)~~ "Ident lookup" refers to querying a selector using [redacted] to determine the approval status. In such cases, the Emphatic Access Restriction controls prevent chaining of a selector that is not marked as approved for querying and return an error message to the analyst. There is no violation of the BR Order because the selector was not actually chained. **(b)(3)-P.L. 86-36**

Area	Test Results	Scope Limitations	Rating
6. Weekly dissemination reports (WDRs)		We limited testing to serialized Signals Intelligence (SIGINT) reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**
7. Dissemination of serialized SIGINT reports with BR metadata		We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	**Compliant**

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records November 2010 Test Results

(ST-10-0004J)

20 December 2010

DERIVED FROM: NSA/CSS Manual 1-52
DATED: 08 January 2007
DECLASSIFY ON: 20320108

(U) NSA OFFICE OF THE INSPECTOR GENERAL

(U) The NSA Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA activities are conducted in compliance with the law. The OIG also serves as an ombudsman, assisting Agency employees, civilian and military, with complaints and questions.

(U) Intelligence Oversight

(U) The OIG Office of Intelligence Oversight reviews NSA's most sensitive and high-risk programs for compliance with the law.

(U) Audits

(U) The OIG Office of Audits within the OIG provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether NSA operations comply with federal policies. Information Technology audits determine whether IT solutions meet customer requirements, while conforming to information assurance standards. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) Investigations and Special Inquiries

(U) The OIG Office of Investigations administers a system for receiving and acting on requests for assistance and complaints about fraud, waste, and mismanagement. Investigations and special inquiries may be undertaken as a result of such requests and complaints (including anonymous tips), at the request of management, as the result of questions that surface during inspections and audits, or at the initiative of the Inspector General.

(U) Field Inspections

(U) The Office of Field Inspections conducts site reviews as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with an assessment of compliance with federal policy. The Office partners with Inspectors General of Service Cryptologic Components and other Intelligence Community Agencies to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

20 December 2010
IG-11238-10

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – November 2010 Test Results (ST-10-0004J)

1. ~~(TS//SI//NF)~~ **Background** This report summarizes the results of our November 2010 testing, using the continuous auditing methodology, of NSA's compliance with the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR). The Office of the Inspector General (OIG) is using this methodology to fulfill the oversight responsibilities assigned to it in the FISC BR Order. Specifically, from January to December 2010, we are conducting monthly tests of NSA's compliance with certain requirements of the FISC BR Order. Once monthly testing is complete, the OIG will make an overall assessment of whether the controls that are in place to ensure such compliance are operating as intended.

2. ~~(TS//SI//NF)~~ **Monthly Test Results and Objectives** We found no instances of non-compliance with the BR Order for six of the seven objectives tested in November 2010. We did not test the seventh objective—compliance with weekly dissemination reporting requirements—because the new BR Order [BR 10-70, signed 29 October 2010] changed the weekly dissemination reporting requirement to a monthly reporting requirement. Because the first report covers the period 9 October to 19 November 2010, not the entire month of testing, we can only conclude that from 1 to 19 November 2010, NSA was in full compliance with the BR Order regarding the accurate and complete reporting of serialized dissemination of BR FISA metadata.

(U) See page 5 for details of November 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (i.e., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20351214

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator?

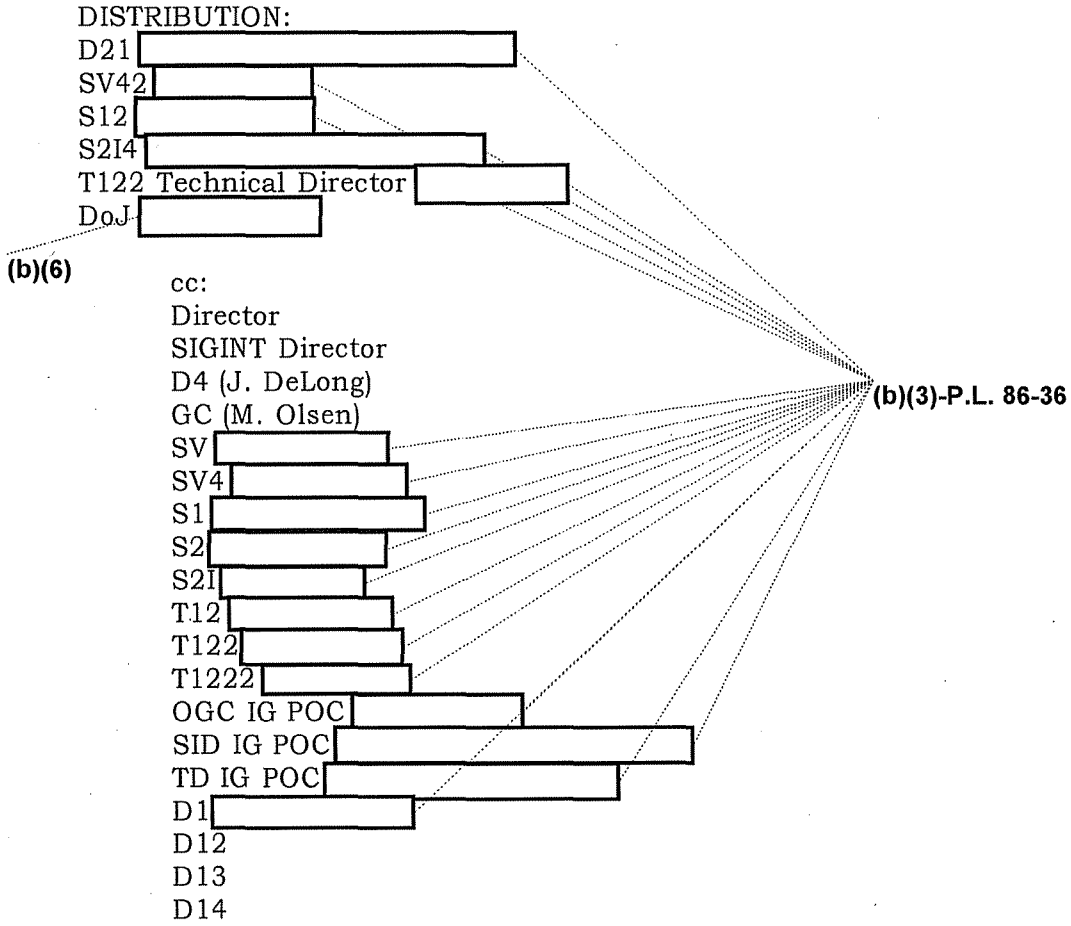
- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report disseminations of BR metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized Signals Intelligence (SIGINT) Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight


DISTRIBUTION:
D21
SV42
S12
S2I4
T122 Technical Director
DoJ
(b)(6)
cc:
Director
SIGINT Director
D4 (J. DeLong)
GC (M. Olsen)
SV
SV4
S1
S2
S2I
T12
T122
T1222
OGC IG POC
SID IG POC
TD IG POC
D1
D12
D13
D14
(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) November 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR) between 1 and 30 November 2010. The ratings are defined on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	Authorized individuals made all [redacted] Chain [redacted] from [redacted]	None	Compliant
2. Reasonable articulable suspicion (RAS) approval of queried selectors	Of the [redacted] Chain [redacted] queries performed in [redacted] the seed selectors of [redacted] were validated as approved. The remaining queries were for data integrity purposes [redacted] or were "ident lookups" [redacted][2]	None (b)(3)-P.L. 86-36	Compliant
3. Office of General Counsel (OGC) review of U.S. person selectors	The [redacted] U.S. person seed selectors queried in [redacted] were reviewed by OGC for First Amendment concerns, as required.	None	Compliant
4. Chaining	In accordance with our test plan, we did not test November 2010 data for this objective. Because there were no noted exceptions for past testing of this objective, we will not test this objective again until January 2011 (using December 2010 data).		
5. Revalidation of queried selectors	The [redacted] seed selectors queried for foreign intelligence purposes were approved by authorized Homeland Mission Coordinators within the Court's timeframes. The [redacted] seed selectors that were not RAS approved were queried for data integrity purposes [redacted] or "ident lookup" [redacted]	None	Compliant
6. Weekly dissemination reports (WDRs)	WDRs are no longer a requirement of the BR Order; therefore, this is no longer a testable objective.		
7. Dissemination of serialized SIGINT reports with BR metadata	[redacted]	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	Compliant

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[1] ~~(TS//SI//NF)~~ [redacted]

[2] ~~(TS//SI//NF)~~ "Ident lookup" refers to querying a selector using [redacted] to determine the approval status. In such cases, the Emphatic Access Restriction controls prevent chaining of a selector that is not marked as approved for querying and return an error message to the analyst. There is no violation of the BR Order because the selector was not actually chained.

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records December 2010 Test Results

(ST-10-0004K)

12 January 2011

Derived From: NSA/CSS Classification Manual 1-52
Dated: 20090804
Declassify On: 20360106

(U) NSA OFFICE OF THE INSPECTOR GENERAL

(U) The NSA Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA activities are conducted in compliance with the law. The OIG also serves as an ombudsman, assisting Agency employees, civilian and military, with complaints and questions.

(U) Intelligence Oversight

(U) The OIG Office of Intelligence Oversight reviews NSA's most sensitive and high-risk programs for compliance with the law.

(U) Audits

(U) The OIG Office of Audits within the OIG provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether NSA operations comply with federal policies. Information Technology audits determine whether IT solutions meet customer requirements, while conforming to information assurance standards. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) Investigations and Special Inquiries

(U) The OIG Office of Investigations administers a system for receiving and acting on requests for assistance and complaints about fraud, waste, and mismanagement. Investigations and special inquiries may be undertaken as a result of such requests and complaints (including anonymous tips), at the request of management, as the result of questions that surface during inspections and audits, or at the initiative of the Inspector General.

(U) Field Inspections

(U) The Office of Field Inspections conducts site reviews as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with an assessment of compliance with federal policy. The Office partners with Inspectors General of Service Cryptologic Components and other Intelligence Community Agencies to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

12 January 2011
IG-11243-11

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – December 2010 Test Results (ST-10-0004K)

1. ~~(TS//SI//NF)~~ **Background** This report summarizes the results of our December 2010 testing, using the continuous auditing methodology, of NSA's compliance with the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR). The Office of the Inspector General (OIG) is using this methodology to fulfill the oversight responsibilities assigned to it in the FISC BR Order. Specifically, from January to December 2010, we are conducting monthly tests of NSA's compliance with certain requirements of the FISC BR Order. Once monthly testing is complete, the OIG will make an overall assessment of whether the controls that are in place to ensure such compliance are operating as intended.

2. ~~(TS//SI//NF)~~ **Monthly Test Results and Objectives** We found no instances of non-compliance with the BR Order for six of the seven objectives tested in December 2010. We did not test the seventh objective—compliance with weekly dissemination reporting requirements—because the new BR Order [BR 10-70, signed 29 October 2010] changed the weekly dissemination reporting requirement to a monthly reporting requirement. Because the report covers the period 20 November to 17 December 2010, not the entire month of testing, we can only conclude that from 1 to 17 December 2010, NSA was in full compliance with the BR Order regarding the accurate and complete reporting of serialized dissemination of BR FISA metadata.

(U) See page 5 for details of December 2010 monthly test results for the following objectives:

- ~~(TS//SI//NF)~~ *Access*: Were all queries to the BR metadata made by authorized individuals (i.e., intelligence analysts and data integrity analysts)?
- (U//~~FOUO~~) *Reasonable Articulable Suspicion (RAS) Approval of Queried Selectors*: Did all queries use RAS-approved seed selectors?

Derived From: NSA/CSS Classification Guide 2-48
Dated: 20090804
Declassify On: 20360106

- (U//~~FOUO~~) *OGC Review of U.S. Person Selectors*: Did OGC verify that RAS determinations of all queried seed selectors associated with U.S. persons had not been based solely on activities protected by the First Amendment to the Constitution?

- ~~(C//REL TO USA, FVEY)~~ *Chaining*: Were all queries chained to no more than three hops?

- (U//~~FOUO~~) *Revalidation of Queried Selectors*: Were all queried foreign and U.S. person seed selectors revalidated within the Court's timeframes—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator?

- ~~(TS//SI//NF)~~ *Weekly Dissemination Reports*: Did NSA accurately and completely report disseminations of BR metadata outside NSA?

- ~~(TS//SI//NF)~~ *Dissemination of Serialized Signals Intelligence (SIGINT) Reports with BR Metadata*: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or one of the five other authorized individuals?

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] on 963-2988(s) or via e-mail at [redacted] or [redacted] on 952-2171(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

[redacted]
Assistant Inspector General
for Intelligence Oversight

DISTRIBUTION:
D21
SV42
S12
S2I4
T122 Technical Director
DoJ

(b)(6)

cc:
Director
SIGINT Director
D4 (J. DeLong)
GC (M. Olsen)
SV
SV4
S1
S2
S2I
T12
T122
T1222
OGC IG POC
SID IG POC
TD IG POC
D1
D12
D13
D14

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) December 2010 Test Results

~~(TS//SI//NF)~~ Test results show that NSA complied with the requirements of the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR) between 1 and 31 December 2010. The ratings are defined on the last page of this report.

~~(TS//SI//NF)~~

Area	Test Results	Scope Limitations	Rating
1. Access	Authorized individuals made all [redacted] Chain [redacted] queries from [redacted] and the [redacted]	None	Compliant
2. Reasonable articulable suspicion (RAS) approval of queried selectors	Of the [redacted] Chain [redacted] queries performed in [redacted] the seed selectors of [redacted] were validated as approved. The remaining [redacted] queries were for data integrity purposes. [redacted] in the [redacted] was for data integrity purposes.	None	Compliant
3. Office of General Counsel (OGC) review of U.S. person selectors	The [redacted] U.S. person seed selectors queried in [redacted] were reviewed by OGC for First Amendment concerns, as required.	None (b)(3)-P.L. 86-36	Compliant
4. Chaining	All [redacted] queries from [redacted] and the [redacted] were chained to no more than three hops from the seed selector.	None	Compliant
5. Revalidation of queried selectors	The [redacted] seed selectors queried for foreign intelligence purposes were approved by authorized Homeland Mission Coordinators within the Court's timeframes. The [redacted] seed selectors that were not RAS approved were queried for data integrity purposes.	None	Compliant
6. Weekly dissemination reports (WDRs)	WDRs are no longer a requirement of the BR Order; therefore, this is no longer a testable objective.		
7. Dissemination of serialized SIGINT reports with BR metadata	[redacted]	We limited testing to serialized SIGINT reports because briefings, litigation, and other types of dissemination were not easily testable using the continuous auditing methodology.	Compliant

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Rating System

~~(TS//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the BR Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses.	**Compliant**
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	**Compliant, with scope limitations**
A rating of red indicates that one or more instances of non-compliance with the BR Order were identified during testing.	**Non-compliant**

~~(TS//SI//NF)~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

Further dissemination of this report outside NSA is *PROHIBITED* without the approval of the Inspector General.

~~(TS//SI//NF)~~ Audit Report on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records

ST-10-0004L

25 May 2011

DERIVED FROM: NSA/CSS Manual 1-52
DATED: 08 January 2007
DECLASSIFY ON: 20320108

(U) NSA OFFICE OF THE INSPECTOR GENERAL

(U) The NSA Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA activities are conducted in compliance with the law. The OIG also serves as an ombudsman, assisting Agency employees, civilian and military, with complaints and questions.

(U) Intelligence Oversight

(U) The OIG Office of Intelligence Oversight reviews NSA's most sensitive and high-risk programs for compliance with the law.

(U) Audits

(U) The OIG Office of Audits within the OIG provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether NSA operations comply with federal policies. Information Technology audits determine whether IT solutions meet customer requirements, while conforming to information assurance standards. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) Investigations and Special Inquiries

(U) The OIG Office of Investigations administers a system for receiving and acting on requests for assistance and complaints about fraud, waste, and mismanagement. Investigations and special inquiries may be undertaken as a result of such requests and complaints (including anonymous tips), at the request of management, as the result of questions that surface during inspections and audits, or at the initiative of the Inspector General.

(U) Field Inspections

(U) The Office of Field Inspections conducts site reviews as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with an assessment of compliance with federal policy. The Office partners with Inspectors General of Service Cryptologic Components and other Intelligence Community Agencies to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

25 May 2011
IG-11287-11

TO: DISTRIBUTION

~~(TS//SI//NF)~~ SUBJECT: Audit Report on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004L) — ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This report summarizes the results of our yearlong review of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records. Although we determined that the querying and dissemination controls we tested were adequate to provide reasonable assurance of compliance with the terms of the Order, two recommendations were made to strengthen the existing control framework.

2. (U//~~FOUO~~) As required by NSA/CSS Policy 1-60, *NSA/CSS Office of the Inspector General*, actions on OIG audit recommendations are subject to monitoring and follow-up until completion. Therefore, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." If you propose that a recommendation be considered closed, please provide sufficient information to show that actions have been taken to correct the deficiency. If a planned action will not be completed by the original target completion date, please state the reason for the delay and provide a revised target completion date. Status reports should be sent to [redacted] Assistant Inspector General for Follow-up, at OPS 2B, Suite 6247, within 15 calendar days after each target completion date.

(b)(3)-P.L. 86-36

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. For additional information, please contact [redacted] on 963-0922(s) or via e-mail at [redacted]

George Ellard

George Ellard
Inspector General

ST-10-0004L

(U) DISTRIBUTION:
DIRNSA
DOC (J. DeLong)
SID (T. Shea)
TD (L. Anderson)
OGC (M. Olsen)

cc:
OGC
ST
SV
SV4
SV42
S12
S2
S2I
S2I4
S309
S3209
S332
T1
T12
T122
T1222
D4 IG POC
D4
OGC IG POC
SID IG POC
TD IG POC
DL SIDIGLIAISON
DL TD_REGISTRY

DOJ NSD

IG
D/IG
D1
D11
D12
D13
D14

(b)(3)-P.L. 86-36

(b)(6)

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

ST-10-0004L

(U) EXECUTIVE SUMMARY

(U) OVERVIEW

~~(TS//SI//NF)~~ This report summarizes the results of our audit of National Security Agency (NSA) controls to comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (BR). From January through December 2010, we conducted monthly tests of NSA compliance with seven provisions of the BR Order to determine whether controls were in place and operating as intended. Five of the provisions were related to querying and two to dissemination.

(U) HIGHLIGHTS

(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ Querying controls were adequate to provide reasonable assurance of compliance with the five provisions of the Order that we tested. NSA's June 2010 release of [redacted] a new selector-tracking application, corrected control weaknesses that we identified in our Pilot Test Report (IG-111545-10). Tests of controls resulted in a low error rate of [redacted] One error occurred before [redacted] release; none occurred after. NSA management must remain diligent in monitoring these controls and ensuring that they remain effective.

(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ Manual controls over the dissemination of serialized Signals Intelligence (SIGINT) reports and the compilation of the Weekly Dissemination Report were inherently risky. However, risks of non-compliance with the two provisions of the Order that we tested were manageable given the amount of information disseminated [redacted] during 2010). Tests of controls revealed no instances of non-compliance. All [redacted] serialized SIGINT reports derived from BR metadata had been approved by an authorized official and included in Weekly Dissemination Reports.

(b)(1)
(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ The manual dissemination controls will be increasingly difficult to manage if the amount of information disseminated outside NSA increases. A recent change to the BR Order that removes the limit on the number of analysts authorized to access BR metadata will likely increase BR-related dissemination if implemented. As part of a two-phase plan to [redacted] query BR metadata, the Counterterrorism Production Center (S2I) began training analysts in [redacted] Recognizing the analytic limitations, NSA plans to seek relief on foreign dissemination tracking requirements through a motion to amend, which in turn will lessen the compliance burden and risk in this area.

(b)(3)-P.L. 86-36

(U) **Management action**

(U//~~FOUO~~) The SIGINT Director concurred with the Office of the Inspector General recommendations. In addition, the Office of the Director of Compliance, Technology Directorate, and Office of General Counsel concurred with the recommendations assigned to them as the secondary action officers. The planned actions meet the intent of the recommendations.

(U) This page intentionally left blank.

I. (U) BACKGROUND

~~(TS//SI//NF)~~ The Business Records (BR) Order

~~(TS//SI//NF)~~ Pursuant to a series of Orders issued by the Foreign Intelligence Surveillance Court (FISC) beginning in May 2006, the National Security Agency (NSA) has been analyzing certain call detail records or telephony metadata from [redacted] telecommunications providers. NSA refers to the Orders collectively as the "BR Order" or "BR FISA."

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ The BR Order provides NSA access to bulk call detail records that primarily include records of telephone calls between the United States and abroad or wholly within the United States; [redacted] This collection of information is not wholly available to NSA through its other foreign intelligence information collection. It is valuable to NSA analysts tasked with identifying potential threats to the U.S. homeland and interests abroad because it enhances analysts' ability to identify, prioritize, and track terrorist operatives and their support networks in the United States and abroad, primarily using call chaining analysis techniques.

~~(TS//SI//NF)~~ Provisions of the BR Order

~~(TS//SI//NF)~~ The Order defines a series of requirements that NSA must follow to protect the privacy rights of U.S. persons (USPs). To access this data, a designated approval authority must conclude that, because of factual and practical considerations of everyday life on which reasonable and prudent persons act, facts give rise to a reasonable articulable suspicion (RAS) that an identifier [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ The provisions of the Orders issued for the first 10 months of our review remained constant. On 29 October 2010, substantial changes were made to the BR Order to be consistent with the terms of the new Pen Register Trap and Trace Order issued in July 2010. The most significant changes related to our review were the elimination of restrictions on the number of analysts allowed to access the BR metadata and a requirement for monthly rather than weekly reports of BR-related dissemination. We adjusted our test procedures for November and December 2010 data to accommodate the changes that affected our monthly control tests.

(U) Tests of Controls Using Continuous Auditing

~~(TS//SI//NF)~~ To assess the effectiveness of NSA controls for complying with the BR Order, the Office of the Inspector General used the continuous auditing methodology, performing monthly tests of NSA's compliance with select requirements for 12 months. Continuous auditing is one of many tools used

within the audit profession to provide reasonable assurance that the control structure surrounding an operational environment is suitably designed, established, and operating as intended. Details on the scope and methodology we used to test controls are in Appendix A.

II. (U) FINDINGS AND RECOMMENDATIONS

(b)(3)-P.L. 86-36

(U) FINDING ONE: Querying Controls

~~(TS//SI//NF)~~ NSA controls over querying were adequate to provide reasonable assurance of compliance with the five provisions of the Order that we tested. Although our Pilot Test Report (IG-111545-0) found an isolated instance of non-compliance for the revalidation of queried selectors, NSA's June 2010 release of [redacted] a new selector-tracking application, corrected the control weakness. No additional errors were noted for the queries reviewed since [redacted] release.

(b)(3)-P.L. 86-36

(U) Criteria Used to Assess Querying Controls

~~(TS//SI//NF)~~ The BR Order includes a series of requirements that limit access to the metadata and limit the selectors that NSA is authorized to query. We evaluated against *Standards of Internal Control in the Federal Government* the adequacy of controls to ensure compliance with the following BR requirements.

1. (U//~~FOUO~~) **RAS Approval of Queried Selectors:** All queries for intelligence analysis purposes must use RAS-approved seed selectors.

2. (U//~~FOUO~~) **Office of General Counsel (OGC) Review of USP Selectors:** OGC must verify that RAS determinations of all seed selectors proposed for querying associated with USPs are not based solely on activities protected by the First Amendment to the Constitution.

3. (U//~~FOUO~~) **Revalidation of Queried Selectors:** The RAS justifications for all queried foreign and USP seed selectors must be revalidated within the Court's periods—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator.

4. ~~(TS//SI//NF)~~ **Access:** All queries to BR metadata must be made by authorized individuals (e.g., intelligence analysts and Data Integrity Analysts.

5. ~~(C//REL TO USA, FVEY)~~ **Chaining:** All queries must be constrained to chains of no more than three hops.

(U//~~FOUO~~) We tested the effectiveness of these controls monthly from January through December 2010.

~~(TS//SI//NF)~~ Databases, Applications, and Controls to Manage the Querying of BR Metadata

~~(TS//SI//NF)~~ The following describes the various databases, applications, and controls that were in place to manage querying of BR metadata.

ST-10-0004L

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ Storing BR Metadata

~~(TS//SI//NF)~~ [redacted] NSA's corporate contact chaining system, stores metadata from multiple sources and stores BR metadata in a separate physical [redacted] performs data quality, preparation, and sorting functions and [redacted] Audit logs document queries and chains made to the metadata.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ Tracking Selectors and Controls over Querying BR Metadata

~~(TS//SI//NF)~~ **The BR FISA Database** was used until 25 June 2010 to track the approvals of selectors and supporting documentation for RAS justifications.

~~(TS//SI//NF)~~ In February 2009, NSA implemented the Emphatic Access Restriction (EAR), a software-restrictive measure written into [redacted] middleware. At that time, the EAR used data contained in the BR FISA Database to prevent querying of non–RAS-approved selectors in [redacted] and to limit the number of hops. However, as noted in our Pilot Test Report, limitations of the BR FISA Database precluded the use of automated controls to prevent queries of expired selectors or to identify selectors associated with USPs.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ In June 2009, the NSA BR FISA Compliance Review Team completed a comprehensive systems engineering and process review of the instrumentation and implementation of the BR FISA authorization and reported that the [redacted] did not have sufficient controls over querying. [redacted] was decommissioned and its functionality reconstituted in [redacted] where all analytic queries are under the architectural controls of [redacted] thereby affording the same compliance safeguards afforded to the [redacted] (e.g., EAR restrictions).

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ [redacted] is the new selector-tracking application that replaced the BR FISA database on 25 June 2010. After [redacted] release, the EAR was reconfigured to use data from [redacted] to prevent queries of selectors in [redacted] that were not RAS approved, including USP selectors that were not marked as having been reviewed by OGC. Finally, [redacted] added a control to change automatically the RAS approval of expired selectors to "not approved" so that those selectors could not be queried.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Tracking Personnel Authorized to Query BR Metadata

~~(TS//SI//NF)~~ [redacted] provides identity and authorization access control services to authorized NSA Enterprise programs and projects. NSA

management uses [redacted] to manage access to BR metadata. The Signals Intelligence Directorate's (SID) FISA Authorities Division (SV4) also maintains a master list of accesses.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Controls were in place in [redacted] to ensure that only cleared personnel were able to access BR metadata. These controls compared [redacted] log-ins with [redacted] groups and prevented access to those not cleared [redacted]

(U//~~FOUO~~) **Weaknesses in querying controls have been corrected**

(TS//SI//NF) During pilot testing, we identified weaknesses that precluded the use of automated controls to ensure compliance with two of the five requirements that we tested: OGC review of USP selectors and revalidation of selectors. Specifically, the BR FISA Database that NSA used to track the approval status and justifications of BR selectors was not designed to tag and track selectors associated with USPs and selector revalidation dates as separate and distinct fields.[1] As a result, NSA increased its risk of non-compliance with these requirements, and the scope of testing on selectors associated with USPs was limited.

~~(TS//SI//NF)~~ On 25 June 2010, NSA corrected these weaknesses by replacing the BR FISA Database with [redacted] a new selector-tracking application. (b)(3)-P.L. 86-36 [redacted] created the required data fields, allowing NSA to implement automated controls that prevent analysts from querying for foreign intelligence purposes 1) USP selectors without an OGC review and 2) expired selectors without revalidation.

~~(TS//SI//NF)~~ We found no weaknesses in automated controls over the remaining three of the five querying requirements that we tested: access to BR metadata, RAS approvals, and chaining.

(U//~~FOUO~~) **Querying controls were adequate to provide reasonable assurance of compliance with the Order**

~~(TS//SI//NF)~~ Querying controls were adequate to provide reasonable assurance of compliance with the Order for the five requirements that we tested. Monthly tests of 2010 queries of BR metadata in [redacted] (b)(3)-P.L. 86-36 [redacted] One error occurred before [redacted] release, and none occurred after. We found one error in the [redacted] queries made in 2010 for one of the five BR requirements tested. We had a significant scope limitation in testing compliance with OGC reviews of USP selectors before [redacted] release and no limitations after.

(b)(1)
(b)(3)-P.L. 86-36

(U) **RAS approvals**

~~(TS//SI//NF)~~ We found no errors in our tests of controls over RAS approvals. All selectors queried were documented as RAS-approved at the time of the query

[1] ~~(TS//SI//NF)~~ During pilot testing, we identified a third control weakness not directly related to our testing: the BR FISA Database was not designed to track time-restricted selectors so that analysts could be made aware of the time for which the RAS determination applied as mandated by the Order. [redacted] also resolved this control (b)(3)-P.L. 86-36 weakness. We did not include time-restricted selectors in our monthly testing because the provisions of the Order allow for the application of analytic judgment to queries on time-restricted selectors, which is subjective and makes objective assessment of compliance difficult.

in the BR FISA Database or [redacted] We therefore judged these controls adequate to provide reasonable assurance of compliance with the Order.

(b)(3)-P.L. 86-36

(U) **OGC reviews of USP selectors**

~~(TS//SI//NF)~~ We found no errors in our tests of controls over OGC reviews of USP selectors. After [redacted] release, all selectors queried that had been documented in [redacted] as being associated with USPs were reviewed by OGC, as documented in [redacted] However, before June 2010, there was a significant scope limitation in our testing of OGC approvals. Because the BR FISA Database did not identify selectors associated with USPs, we did not know whether our tests included all U.S. selectors. Because [redacted] corrected this control weakness and we found no instances of non-compliance after its release, we determined these controls adequate to provide reasonable assurance of compliance with the Order.

(U) **Revalidation of selectors**

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ We found no errors in our tests of controls to revalidate selectors after [redacted] was released. All selectors queried had been revalidated within the prescribed period, as documented in [redacted] Before [redacted] release, we found one error that was a breakdown in controls, which the Department of Justice (DoJ) National Security Division later reported as a compliance incident pursuant to Rule 10(c) of the FISC Rules of Procedures.[2] [redacted]

(b)(3)-P.L. 86-36

[redacted] Because this control weakness was subsequently resolved with the release of [redacted] and we found no other errors, we judged these controls adequate to provide reasonable assurance of compliance with the Order.

(b)(3)-P.L. 86-36

(U) **Access**

~~(TS//SI//NF)~~ We found no errors in our tests of controls over access to BR metadata. Only authorized personnel, as documented in [redacted] and the Special FISA Division's (SV42) list of authorized accesses, queried the BR metadata for foreign intelligence or technical analysis (e.g., data integrity) purposes. We therefore judged these controls adequate to provide reasonable assurance of compliance with the Order.

(b)(3)-P.L. 86-36

(U) **Chaining**

~~(TS//SI//NF)~~ We found no errors in our tests of controls over chaining. According to the [redacted] audit logs, no selectors had been chained to more than three hops, except for selectors queried for data integrity purposes as permitted by the Order. In following our test procedures, we did not test these controls from July through November 2010 because we found no errors within the first six months of testing. We therefore judged these controls adequate to provide reasonable assurance of compliance with the Order.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Periodic monitoring of querying controls is needed**

(U//~~FOUO~~) Although our evaluation and tests of controls determined that controls were adequate to provide reasonable assurance of compliance with the Order, management must continue to monitor the effectiveness of these controls in a manner commensurate with risk and value added.

[2](U//~~FOUO~~) Because of amendment to the FISC rules, 10(c) incidents are now referred to as 13(b) incidents.

(U//~~FOUO~~) Monitoring is the final standard for internal control in the federal government. Agency internal control monitoring assesses the quality of performance over time by putting in place procedures to monitor internal control as part of the process of carrying out regular activities. Monitoring includes ensuring that managers know their responsibilities for internal control and control monitoring. In addition, separate evaluations of internal control should be performed periodically and the deficiencies investigated. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as reviews of control design and direct testing of internal control.

~~(TS//SI//NF)~~ At the time of our review, SV42 was monitoring the effectiveness of controls by conducting weekly manual reviews of audit logs to ensure compliance with three of the provisions of the Order that we tested. Given the strength of the automated controls since [redacted] release, management should reassess the timing and extent of these reviews. In particular, we recommend that management base the type, duration, and frequency of monitoring on risk and value added. For example, in lieu of weekly and 100 percent reviews of audit logs, management should consider such options as periodic testing, sampling, event-driven reviews, or automated exception reporting. **(b)(3)-P.L. 86-36**

(U) RECOMMENDATION 1
(U//~~FOUO~~) Develop a comprehensive plan to provide long-term monitoring of the effectiveness of querying controls. The plan should be commensurate with risk and value added and include the means to manage changes in factors such as personnel, Information Technology systems, software applications, and legal authorities. **(ACTION: SIGINT Director with TD and ODOC)**

(U) Management Response **(b)(3)-P.L. 86-36**

CONCUR ~~(TS//SI//NF)~~ Currently, Oversight and Compliance (SV) manually monitors querying compliance with a weekly 100 percent audit of all queries. SV has found no errors in querying since the Emphatic Access Restriction (EAR) was implemented [redacted] which technologically limits the selectors used in a query. SV is in the process of developing a long-term querying compliance strategy aligning the weekly 100 percent auditing with SID's Auditing Modernization Strategy. SV will work with D4 to develop a "Sampling Rigor" to identify a sampling standard by the end of August 2011. In addition, SV will continue to work with [redacted] developers to fully automate auditing procedures such as a web-based interface to perform the audits. [redacted] **(b)(3)-P.L. 86-36**

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

(U) OIG Comment

(U//~~FOUO~~) The planned actions meet the intent of the recommendation.

(U) This page intentionally left blank.

(b)(1)
(b)(3)-P.L. 86-36

(U) FINDING TWO: Dissemination Controls

~~(TS//SI//NF)~~ Manual controls over the dissemination of serialized SIGINT reports and the compilation of the Weekly Dissemination Report (WDR) were inherently risky. However, risks of non-compliance with the two provisions of the Order that we tested were manageable [redacted] Although we found no instances of non-compliance, monthly testing identified one error in which a WDR incorrectly included a report that was not derived from BR metadata. This error was not a violation of the Order but underscores that the largely manual process for tracking serialized SIGINT dissemination and compiling WDRs is inherently risky and would require management attention should the amount of dissemination increase. [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

(U) Criteria Used to Assess Dissemination Controls

~~(TS//SI//NF)~~ To protect the privacy rights of USPs, the BR Order includes a series of requirements to track and control information shared outside NSA. With the exception of exculpatory material used in litigation, the BR Order requires that all disseminations of USP information derived from BR metadata made outside NSA, whether in formal reporting or in response to requests for information or other forms of communication, be approved by one of five NSA officials. One of the five officials must determine that the information identifying the USP is in fact related to Counterterrorism (CT) information and that it is necessary to understand the CT information or assess its importance. The BR Order does not state that the authority may be delegated. Until BR 10-70 was issued on 29 October 2010, the Order also required that NSA provide the FISC a weekly report of all dissemination. BR 10-70 changed the weekly reporting requirement to every 30 days.

~~(TS//SI//NF)~~ We evaluated the adequacy of controls to ensure compliance with two BR requirements against *Standards of Internal Control in the Federal Government* and tested the effectiveness of these controls monthly from January through December 2010.

1. ~~(TS//SI//NF)~~ **Weekly Dissemination Reports:** NSA must accurately and completely report disseminations of BR metadata outside NSA.

2. ~~(TS//SI//NF)~~ **Dissemination of Serialized SIGINT Reports with BR Metadata:** All information disseminated through serialized SIGINT reports must be approved by the Chief of Information Sharing Services (S12) or one of the four other authorized individuals.

~~(TS//SI//NF)~~ Process to Track and Disseminate BR Serialized SIGINT Reports

~~(TS//SI//NF)~~ The process to track serialized SIGINT dissemination is largely manual and maintained outside the infrastructure used to handle normal

reports involving the release of U.S. identities. Homeland Security Analysis Center (S2I4) policy was that serialized reporting and S12-approved responses to Requests for Information were the only acceptable forms of dissemination outside NSA. Therefore, e-mails and other informal types of dissemination were not permitted, and any information derived from BR metadata required S12 approval. In particular, S2I4 procedures required that reports derived from BR metadata use the [redacted] format normally used to disseminate SIGINT information that responds to the special requirements of the [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted]

~~(TS//SI//NF)~~ The Chief and Senior Editor of S2I4 track BR-related reports and submit requests to disseminate information outside NSA to the Chief of S12, via e-mail. S12 documents approvals to disseminate through one-time dissemination authorization memos. The Chief of S12 signs the memos and retains a copy for the record.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ S2I4 manually tracks BR-related dissemination for inclusion in WDRs to the FISC, and SV42 maintains a spreadsheet to track report dissemination authorizations.

~~(TS//SI//NF)~~ [redacted] a management information system for SIGINT production contains statistical information and customer feedback about serialized reports. Within [redacted] dissemination based on BR analysis can be identified [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted]

(U//~~FOUO~~) The Manual Process to Disseminate and Track Serialized SIGINT Reports Was Inherently Risky but Manageable Given the Amount of Information Disseminated

~~(C//REL to USA, FVEY)~~ During pilot testing, we noted that the process to obtain and document dissemination authorizations for serialized SIGINT reports signed by the Chief of S12 and the process to compile WDRs were largely manual and, therefore, dependent on the diligence of the staff and the strength of standard operating procedures. During monthly testing, we found one error that underscored this weakness but found no instances of non-compliance with the Order. The largely manual process to disseminate and track serialized SIGINT reports was therefore inherently risky but manageable given the relatively small amount of information disseminated [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Weekly Dissemination Reports

~~(TS//SI//NF)~~ In our tests of controls over the accuracy of the 44 WDRs covering 2010 dissemination, we found that a WDR mistakenly listed a serialized dissemination that was not derived from BR metadata. Although the error did not violate the BR Order, it underscores a weakness in the largely manual process to track and report BR disseminations that we noted in our Pilot Test Report (IG-111545-10).

~~(TS//SI//NF)~~ We did not test NSA compliance with weekly dissemination reporting requirements in November and December 2010 because the BR Order [redacted] changed the reporting requirement from weekly to every 30 days. Because the 30-day reports did not correspond with our

(b)(3)-P.L. 86-36

monthly testing, we were unable to draw a conclusion about whether NSA was in full compliance with the BR Order regarding the accurate and complete reporting of serialized dissemination of BR FISA metadata for the period from 1 November 2010 to 17 December 2010.

(U//~~FOUO~~) We judged the manual process to compile WDRs to be inherently risky but manageable given the small amount of information disseminated.

(U//~~FOUO~~) Dissemination of Serialized SIGINT Reports

~~(TS//SI//NF)~~ We found no errors in our tests of controls over approvals of serialized SIGINT reports. All [redacted] reports issued in 2010 had been approved by the Chief of S12 or one of the four other authorized individuals. We judged the manual process to track serialized reports as inherently risky but manageable given the small amount of information disseminated.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Manual Processes Will Not Be Manageable if the Amount of Dissemination Increases

~~(TS//SI//NF)~~ We noted in our Pilot Test Report that management should consider automating dissemination approvals and tracking if BR-related dissemination increases. A change to the provisions of the Order signed on 29 October 2010 (BR 10-70) might significantly increase the amount of information disseminated. Specifically, BR 10-70 removes the limit of 125 analysts authorized to query BR metadata but maintains requirements for NSA to report to the FISC all dissemination outside NSA. Before issuance of BR 10-70, only [redacted] persons had query access to the metadata, well below the 125 limit. The Chief of S2I4 estimated that if NSA implements this change, S2I4's query access might expand to the [redacted] personnel already authorized to view query results and to the more than [redacted] analysts with [redacted] CT responsibilities. Manual processes would not be manageable if the amount of dissemination increases with the number of analysts authorized to query.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ S2I issued a Staff Processing Form (SPF) [redacted] announcing plans to expand BR and Pen Register and Trap and Trace (PR/TT) access to query results [redacted]

(b)(3)-P.L. 86-36

The Chief of S2I4 stated that the expansion relies on training and controls, such as the EAR and [redacted] to ensure compliance. The SPF states that training [redacted]

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ NSA OGC recognized that increasing the number of analysts authorized to query BR metadata and expanding access to BR query results might increase the risk that informal disseminations would not be documented and therefore, would be untracked and ultimately out of compliance with the Court Order. Specifically, the BR Order requires formal, documentable tracking of foreign-target BR disseminations, a practice that runs counter to traditional NSA analytic process and hence requires additional, non-standard training to accomplish. This practice also constrains the full analysis of bulk metadata. NSA OGC is therefore drafting a motion to amend the BR (and PR/TT) Order. A draft of the motion, [redacted] states that NSA seeks relief from the

(b)(3)-P.L. 86-36

requirement to include in a 30-day report "a statement of the number of instances since the preceding report in which NSA has shared, in any form, information obtained or derived from the metadata with anyone outside NSA," only to the extent that the dissemination applies to non-USP information obtained or derived from metadata. NSA OGC expects to file the motion soon, but there is no definite period, and it is uncertain whether the FISC will grant the motion.

(U) RECOMMENDATION 2

~~(TS//SI//NF)~~ Develop a plan to mitigate the risk of non-compliance with the Order in disseminating information derived from BR metadata when expanding access to BR querying and results.

(ACTION: SIGINT Director with ODOC and OGC)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Management Response

CONCUR ~~(TS//SI//NF)~~ SID acknowledges that BR Order compliance, in terms of tracking and controlling the dissemination of BR-derived information, is indeed essential as the Signals Intelligence Directorate expands BR and Pen Register/Trap and Trace (PR/TT) access to query results [redacted] will be incrementally executed in a methodical manner to mitigate the risk of non-compliance. Expansion of access and use of the BR and PR/TT authorities will be conducted apace of the requisite compliance and oversight infrastructure to minimize the risk of incidents and violations.

(b)(3)-P.L. 86-36

Training serves as one of the key elements for success and much progress has been made. [redacted] SID expects the launch of the National Cryptologic School course OVSC 1205. This course incorporates required Office of the General Counsel (OGC) indoctrinations for both BR and PR/TT with analyst focused material. Completion of OVSC 1205 will be the basis for granting the [redacted] credentials and constitutes a prerequisite for the granting of the [redacted] upon nomination by a production element manager based on a valid mission justification.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ In addition, SID fully understands the Office of the Inspector General's concerns regarding tracking disseminations of BR-derived information and continues to evaluate approval and dissemination processes to optimize current procedure, where possible. When planning to disseminate information derived from BR FISA, USP information must be identified and its dissemination (with a report) must be reviewed and approved by the Chief or D/Chief S12 (or one of the other officials as noted in the BR Order). [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

Although non-USP disseminations do not require prior approval from S12, known disseminations shall continue to be documented as they occur and

reported, along with disseminations of USP info, every 30 days to the FISC. As BR is expanded [redacted] process shall be expanded to ensure the same degree of controls and oversight. Expansion will be gradual to ensure requisite training is conducted and control and compliance processes are in place, and SID shall consider further controls/process enhancements (such as further automation) as the situation warrants. S2I shall ensure expansion remains aligned with current scalable processes that have resulted in substantive compliance with the Court's order to date.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

* (U) Refer to Appendix E, Pages 3 through 5 for full text of SID's management action plan for Recommendation 2.

(U) OIG Comment

(U//~~FOUO~~) The planned actions meet the intent of the recommendation.

(U) This page intentionally left blank.

III. (U) ABBREVIATIONS AND ORGANIZATIONS

~~(TS//SI//NF)~~ BR	Business Records
(U) BDA	Blanket Dissemination Authorization
(U) CT	Counterterrorism
(U) CTEE	Counterterrorism Extended Enterprise
(U) DIA	Data Integrity Analyst
(U) DoJ	Department of Justice
~~(TS//SI//NF)~~ EAR	Emphatic Access Restriction
(U) FISA	Foreign Intelligence Surveillance Act
(U) FISC	Foreign Intelligence Surveillance Court
(U) MRG	Math Research Group
(U) NSA	National Security Agency
(U) ODOC	Office of the Director of Compliance
(U) OGC	Office of General Counsel
~~(TS//SI//NF)~~ PR/TT	Pen Register and Trap and Trace
(U) RAS	reasonable articulable suspicion
(U) S12	Information Sharing Services
(U) S2I	Counterterrorism Production Center
(U) S2I4	Homeland Security Analysis Center
(U) SID	Signals Intelligence Directorate
(U) SIGINT	Signals Intelligence
(U) SPF	Staff Processing Form
(U) SV	Oversight and Compliance
(U) SV4	FISA Authorities Division
(U) SV42	Special FISA Oversight and Processing
(U) TD	Technology Directorate
(U) USP	U.S. person
(U) WDR	Weekly Dissemination Report

(U) This page intentionally left blank.

(U) APPENDIX A

(U) About the Audit

(U) This page intentionally left blank.

(U) ABOUT THE AUDIT

(U) Objective

~~(TS//SI//NF)~~ The overall objective of this audit was to test whether controls to ensure National Security Agency (NSA) compliance with key terms of the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR) are operating as intended. To do so, we conducted a pilot test of the audit in which our objective was to determine NSA compliance and assess the feasibility and reasonableness of including in monthly testing six objectives related to querying and dissemination. We then conducted monthly testing of NSA's compliance with seven requirements of the BR Order.

(U) Scope and Methodology

(U) We conducted pilot testing from January to March 2010; monthly testing of January through December 2010 data was conducted from March 2010 through January 2011.

~~(TS//SI//NF)~~ For tests related to querying, we compared all selectors that were documented in [redacted] as having been queried each month against access lists, reasonable articulable suspicion approvals documented in the Foreign Intelligence Surveillance Act BR database or [redacted] and Office of General Counsel (OGC) reviews documented in the [redacted] or [redacted] We also counted the number of hops chained for each selector in the [redacted] audit logs. We researched anomalies to make a final determination of compliance.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) For tests related to dissemination, we verified that serialized SIGINT reports issued in 2010 were supported by dissemination authorizations. We also reviewed Weekly Dissemination Reports and supporting documentation.

(U//~~FOUO~~) We met with individuals from OGC, the Office of the Director of Compliance (ODOC), the Signals Intelligence Directorate (SID), and the Technology Directorate, including the SID Office of Oversight and Compliance, Information Sharing Services, Homeland Security Analysis Center, SID Issues Support Staff, Analytic Capabilities, [redacted] and [redacted] Operations.

(b)(3)-P.L. 86-36

ST-10-0004L

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions according to our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions according to our audit objectives.

(U//~~FOUO~~) Reports Issued

~~(TS//SI//NF)~~ *Advisory Report on the Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004)*, 12 May 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records –January to March 2010 Test Results (ST-10-0004A)*, 1 June 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – April 2010 Test Results (ST-10-0004B)*, 10 June 2010

~~(TS//SI//NF)~~ *Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C)*, 29 September 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – May 2010 Test Results (ST-10-0004D)*, 30 June 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – June 2010 Test Results (ST-10-0004E)*, 20 July 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – July 2010 Test Results (ST-10-0004F)*, 18 August 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – August 2010 Test Results (ST-10-0004G)*, 28 September 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – September 2010 Test Results (ST-10-0004H)*, 28 October 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – October 2010 Test Results (ST-10-0004I)*, 1 December 2010

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – November 2010 Test Results (ST-10-0004J)*, 20 December 2010

ST-10-0004L

~~(TS//SI//NF)~~ *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – December 2010 Test Results (ST-10-0004K)*, 12 January 2011

(U) This page intentionally left blank.

(U) APPENDIX B

(U) Summary of Recommendations

(U) This page intentionally left blank.

(U) SUMMARY OF RECOMMENDATIONS

(U) RECOMMENDATION 1

(U//~~FOUO~~) Develop a comprehensive plan to provide long-term monitoring of the effectiveness of querying controls. The plan should be commensurate with risk and value added and include the means to manage changes in factors such as personnel, Information Technology systems, software applications, and legal authorities.

(U) ACTION: SIGINT Director with TD and ODOC
(U) Status: OPEN/Concur
(U) Target Completion Date: [redacted]

(b)(3)-P.L. 86-36

(U) RECOMMENDATION 2

~~(TS//SI//NF)~~ Develop a plan to mitigate the risk of non-compliance with the Order in disseminating information derived from BR Metadata when expanding access to BR querying and results.

(U) ACTION: SIGINT Director with ODOC and OGC
(U) Status: OPEN/Concur
(U) Target Completion Date: [redacted]

(U) This page intentionally left blank.

ST-10-0004L

(U) APPENDIX C

(U) Monthly Test Results of Querying Controls

(U) This page intentionally left blank.

ST-10-0004L

(U) MONTHLY TEST RESULTS OF QUERYING CONTROLS

~~(TS//SI//NF)~~

BR Requirement Tested	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total Errors	Error Rate	Auditor Conclusion
1. RAS Approval	0	0	0	0	0	0	0	0	0	0	0	0	**0**		**Adequate**
2. OGC Review	0	0	0	0	0	0	0	0	0	0	0	0	**0**		**Adequate**
3. Revalidation	0	0	1	0	0	0	0	0	0	0	0	0	**1**		**Adequate**
4. Access	0	0	0	0	0	0	0	0	0	0	0	0	**0**		**Adequate**
5. Chaining	0	0	0	0	0	0	Not tested *	Not tested *	Not tested *	Not tested *	Not tested *	0	**0**		**Adequate**
Total No. of Queries														**(b)(1) (b)(3)-P.L. 86-36**	

*(U//~~FOUO~~) Not tested per test plan.

~~(TS//SI//NF)~~

(b)(3)-P.L. 86-36

KEY	No test errors	Scope limitation	Test error(s)

(U) This page intentionally left blank.

ST-10-0004L

(U) APPENDIX D

(U) Monthly Test Results of Dissemination Controls

ST-10-0004L

(U) This page intentionally left blank.

ST-10-0004L

(U) MONTHLY TEST RESULTS OF DISSEMINATION CONTROLS

~~(TS//SI//NF)~~

BR Requirement Tested	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total Errors	Error Rate	Auditor Conclusion
1. Weekly Dissemination Reports	0	0	0	0	0	0	0	0	0	1	Not tested*	Not tested*	1		Manageable
2. Dissemination of serialized SIGINT	0	0	0	0	0	0	0	0	0	0	0	0	0		Manageable
Total No. of WDRs															
Total No. of Serialized SIGINT Dissemination														(b)(1) (b)(3)-P.L. 86-36	

~~*(TS//SI//NF)~~ Not tested because the reporting requirement changed from weekly to every 30 days.

~~(TS//SI//NF)~~

(b)(3)-P.L. 86-36

KEY	No test errors	Scope limitation	Test error(s)

(U) This page intentionally left blank.

ST-10-0004L

(U) APPENDIX E

(U) Full Text of Management Responses

(U) This page intentionally left blank.

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

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
OIG	2011-3073	

THRU	ACTION	EXREG SUSPENSE
	☐ APPROVAL	15 Apr 11
SUBJECT	☐ SIGNATURE	KCC SUSPENSE
(U) SID's Management Response to the DRAFT IG Report for ST-10-0004L.	☐ INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION
S, S02, S023, S1, S2, S3, ST, SV, D2, D4

SUMMARY

PURPOSE: ~~(TS//SI//NF)~~ To provide the Signals Intelligence Directorate's (SID's) response to the DRAFT Inspector General Audit Report on *NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR) (ST-10-0004L).*

BACKGROUND: ~~(TS//SI//NF)~~ SID received the DRAFT audit report which summarized the results of the Inspector General's year-long review of NSA Controls to Comply with the FISC Order Regarding BR. Although the querying and dissemination controls tested were adequate to provide reasonable assurance of compliance with the terms of the order, two recommendations with SID Lead were documented in the report.

DISCUSSION: (U//~~FOUO~~) SID reviewed the document for factual accuracy and concurs with the document and recommendations as written. SID Oversight and Compliance (SV) will lead the effort for Recommendation 1, with SID's [redacted] spearheading the effort for Recommendation 2. The Office of General Counsel agreed to be a secondary action officer to assist SID in its development of a management action plan for Recommendation 2. The SIGINT Directorate's coordinated response is attached.

Encl: a/s

(b)(3)-P.L. 86-36

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
SID DIR	5/6/11		S3	/2May11	
S02	5/6/11		ST	/4May11	
S0232	/May 11		SV	28Apr11	
S1	2May11		D2	/2May11	
S2	3May11		D4	/29Apr11	

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
SID IG Liaison	S0232	966-5590	04 May 2011

FORM A6796 REV NOV 96
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SECURITY CLASSIFICATION
~~TOP SECRET//COMINT//NOFORN~~

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

~~(TS//SI//NF)~~ DRAFT AUDIT REPORT ON NSA CONTROLS TO COMPLY WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER REGARDING BUSINESS RECORDS (ST-10-0004L)

RECOMMENDATION 1

(U//~~FOUO~~) Develop a comprehensive plan to provide long-term monitoring of the effectiveness of querying controls. The plan should be commensurate with risk and value added and include the means to manage changes in factors such as personnel, information technology systems, software applications, and legal authorities.

SID Action Element: SID Lead SV
(ACTION: SIGINT Director with TD and ODoC)

Concur/Non-concur: **CONCUR as written**

SID Response (May 2011): ~~(TS//SI//NF)~~ Currently, SV manually monitors querying compliance with a weekly 100 percent audit of all queries. SV has found no errors in querying since the Emphatic Access Restriction (EAR) was implemented [redacted] which technologically limits the selectors used in a query. SV is in the process of developing a long-term querying compliance strategy aligning the weekly 100 percent auditing with SID's Auditing Modernization Strategy. SV will work with D4 [redacted] In addition, SV will continue to work with [redacted] developers to fully automate auditing procedures such as a web-based interface to perform the audits. This long-term plan will take into consideration the expansion of BR and PRTT [redacted]

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

Estimated Completion Date: (U [redacted]

SID POC: (U//~~FOUO~~) [redacted] Deputy Chief, SV4, NSTS: 969-5383

(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

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

RECOMMENDATION 2

~~(TS//SI//NF)~~ Develop a plan to mitigate the risk of non-compliance with the Order in disseminating information derived from BR metadata when expanding access to BR querying and results.

(b)(3)-P.L. 86-36

(ACTION: SIGINT Director with ODoC and OGC)
SID Lead

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

Concur/Non-concur: CONCUR as written

SID Response (April 2011): ~~(TS//SI//NF)~~ SID acknowledges that BR Order compliance, in terms of tracking and controlling the dissemination of BR-derived information, is indeed essential as the Signals Intelligence Directorate expands BR and Pen Register/Trap and Trace (PR/TT) access to query results This mission expansion to the will be incrementally executed in a methodical manner to mitigate the risk of non-compliance. Expansion of access and use of the BR and PR/TT authorities will be conducted apace of the requisite compliance and oversight infrastructure to minimize the risk of incidents and violations. Training serves as one of the key elements for success and much progress has been made. For instance, by mid September 2011, SID expects the launch of the National Cryptologic School (NCS) course OVSC 1205. This course incorporates required Office of the General Counsel (OGC) indoctrinations for both BR and PR/TT with analyst focused material. The current regimen represented in OVSC 1204 is strictly BR centric while 1205 addresses both programs. Completion of OVSC 1205 will be the basis for granting the credentials and constitutes a prerequisite for the granting of the upon nomination by a production element manager based on a valid mission justification. Beyond training, management oversight will be critical. The BR Order has no provision for the delegation of dissemination approval authority beyond those individuals and positions named in the order. OVSC1205, specifically on this topic (dissemination), reflects the language of the order clearly in Module 4 and as the planned expansion progresses, have the responsibility for educating their workforce and providing the appropriate level of oversight to ensure compliance. has a sound business practice that will serve as a model to emulate as SID moves forward with this important mission expansion. SID has been collaborating with key players and SID/S12 remains committed to guiding and overseeing the

(b)(1)
(b)(3)-P.L. 86-3

(b)(3)-P.L. 86-36

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

(b)(1)
~~(b)(3)-P.L. 86-36~~
(b)(3)-50 USC 3024(i)

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

mission rollout and implementation of procedures governing U.S. person dissemination issues.

~~(TS//SI//NF)~~ Finally, SID fully understands the IG's concerns regarding tracking disseminations of BR-derived information and continues to evaluate approval and dissemination processes to optimize current procedure, where possible. When planning to disseminate information derived from BR FISA, USP information must be identified and its dissemination (with a report) must be reviewed and approved by the Chief or D/Chief S12 (or one of the other officials as noted in the BR Order). As with the unmasked dissemination of any USP identities in products, this is accomplished using [redacted] The S12 URS Centers are [redacted] responsible for preparing and submitting the [redacted] on behalf of Product Line reporters [redacted] Although non-USP disseminations do not require prior approval from S12, known disseminations shall continue to be documented as they occur and reported, along with disseminations of USP info, every 30 days to the FISC. As BR is expanded [redacted] shall be expanded to ensure the same degree of controls and oversight. Expansion will be gradual to ensure requisite training is conducted and control and compliance processes are in place, and SID shall consider further controls/process enhancements (such as further automation) as the situation warrants. S2I shall ensure expansion remains aligned with current scalable processes that have resulted in substantive compliance with the Court's order to date.

(b)(3)-P.L. 86-36

(U) Estimated Completion Date: [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- (U) OVSC 1205 fully fielded
- ~~(TS//SI//NF)~~ Appropriate populations [redacted] representing the cross sections of SID and TD elements involved in BR and PR/TT at NSA-W fully credentialed and aware of program background as well as current environment with the FISC
- ~~(TS//SI//NF)~~ [redacted] production element managers credentialed [redacted] based on recommendations of the former
- ~~(TS//SI//NF)~~ SV oversight protocol for auditing, DOJ spot checks, and 30 day reports revamped to include unique challenges that could arise based on [redacted] access and use
- ~~(TS//SI//NF)~~ ODoC in progress review of each incremental step to ensure compliance remains apace of implementation

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

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

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

(U//~~FOUO~~) SID Points of Contact:

(U//~~FOUO~~) SID Lead –
(U//~~FOUO~~) S1 – 966-3919
(U//~~FOUO~~) S2 – 969-0224
(U//~~FOUO~~) S3 – 969-0699
(U//~~FOUO~~) SV – 969-5383

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Coordinated with: ODOC – Assistant Director for Special Compliance Activities, D4, 963-1705

(U//~~FOUO~~) OGC concurs with Recommendation 2 and will work with both SID and ODOC to prepare a management action plan.

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

[redacted] NSA-D11 USA CIV

From: [redacted] NSA-D4 USA CIV
Sent: Thursday, March 31, 2011 9:14 AM
To: [redacted] NSA-D11 USA CIV; [redacted] NSA-D11 USA CIV
Cc: [redacted] NSA-D4 USA CIV; [redacted] NSA-D4 USA CIV; [redacted] NSA-D4 USA CIV; [redacted] NSA-D4 USA CIV; [redacted] NSA-D4 USA CIV; [redacted] NSA-D4 USA CIV
Subject: FW: (U) Draft Report - ST-10-0004L - For Management Response
Attachments: Draft Report - ST-10-0004L - 11-16-2009.pdf; ST-10-0004L Action Response.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

(b)(3)-P.L. 86-36

Classification: ~~TOP SECRET//COMINT//NOFORN~~

[redacted]

ODOC (D4) concurs with Recommendations 1 and 2 (see attached form).

Recommendation 1:
Action: [redacted] as D4 POC
Concur/Non-concur: Concur - *with clarification* that SID has the lead
Mgmt response: The D4 POC will work with SID (who has the lead for the action) in the development of an Action Plan
Completion date: For SID (as action lead) to define

(b)(3)-P.L. 86-36

Recommendation 2:
Action: [redacted]
Concur/Non-concur: Concur - *with clarification* that SID has the lead
Mgmt response: The D4 POC will work with SID (who has the lead for the action) in the development of an Action Plan
Completion date: For SID (as action lead) to define

Thank you.

[redacted]

(U//~~FOUO~~)

[redacted]
Office of the Director of Compliance, D4
OPS 2B, Rm. 2B8054, Suite 6242
963-2199 / [redacted]

[redacted] NSA-D11 USA CIV

From: [redacted] NSA-T021 USA CIV
Sent: Tuesday, April 19, 2011 3:54 PM
To: [redacted] NSA-D11 USA CIV; [redacted] NSA-D11 USA CIV
Cc: DL td_registry (ALIAS) T021; [redacted] NSA-TE6 USA CIV; DL t1_actionofficer (ALIAS) T1; [redacted] NSA-T USA CIV; [redacted] NSA-TE6 USA CIV
Subject: (U) Draft Report - ST-10-0004L - For Management Response-2011-2987

Follow Up Flag: Follow up
Flag Status: Flagged

(b)(3)-P.L. 86-36

Classification: ~~CONFIDENTIAL~~

(U//~~FOUO~~) [redacted] apologize for the delay, I was out yesterday. T1, TD DoC and TE6 have reviewed the report and all concur and do not recommend any changes. Specifically to REC 1, they all concur as well.

REC No - REC 1

Action - SIGINT DIR with TD and ODOC

Concur with the recommendation

Mgmt Response - TD has no comments to present on the audit.

Completion Date - To be determined by all parties as the actions within REC 1 begin to take place.

POC - T1 - [redacted]
TD DoC - [redacted]
TE6 - [redacted]

(b)(3)-P.L. 86-36

Thank you, [redacted]

[redacted] NSA-D11 USA CIV (b)(3)-P.L. 86-36

From: [redacted] NSA-D2 USA CIV
Sent: Monday, May 02, 2011 4:10 PM
To: [redacted] NSA-D11 USA CIV
Cc: [redacted] NSA-D11 USA CIV; [redacted] NSA-D2 USA CIV; [redacted] NSA-D21 USA CIV; [redacted] NSA-D21 USA CIV; [redacted] NSA-D2 USA CIV
Subject: RE: (U) Draft Report - ST-10-0004L - For Management Response

Follow Up Flag: Follow up
Flag Status: Flagged

Classification: ~~TOP SECRET//COMINT//NOFORN~~

Hi [redacted]

Please use this email as confirmation that OGC wants to be added to Recommendation 2. OGC concurs with Recommendation 2 and will work with both SID and ODOC to prepare a management action plan.

Please let me know if you need anything further.

Thanks.

(U) This page intentionally left blank.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Report on the Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Retention

ST-11-0011
20 October 2011

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities compl y with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provide s independent assessment s of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC compon ents must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

20 October 2011
IG-11345-12

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Report on the Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Retention (ST-11-0011) — ACTION MEMORANDUM

1. (U) This report summarizes the results of our audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Retention and incorporates management's response to the draft report.

2. (U//~~FOUO~~) As required by NSA/CSS Policy 1-60, *NSA/CSS Office of the Inspector General,* actions on OIG audit recommendations are subject to monitoring and follow-up until completion. Therefore, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." If you propose that a recommendation be considered closed, please provide sufficient information to show that actions have been taken to correct the deficiency. If a planned action will not be completed by the original target completion date, please state the reason for the delay and provide a revised target completion date. Status reports should be sent to [redacted] Assistant Inspector General for Follow-up, at OPS 2B, Suite 6247, within 15 calendar days after each target completion date.

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. For additional information, please contact [redacted] on 963-0922(s) or via e-mail at [redacted]

(b)(3)-P.L. 86-36

George Ellard

George Ellard
Inspector General

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

ST-11-0011

(U) DISTRIBUTION:
DIRNSA
SID (T. Shea)
TD (L. Anderson)

cc: EXDIR (F. Fleisch)
COS (D. Bonanni)
DOC (J. DeLong)
D4
OGC
ST
SV
SV4
SV42
S31323
S353
TE
TE6
T1
T12
T122
T1222
T131
T1313
D4 IG POC
SID IG POC
TD IG POC
DL SIDIGLIAISON
DL TD_REGISTRY

DOJ NSD

IG
D/IG
D1
D11
D12
D13
D14

(b)(3)-P.L. 86-36

(b)(6)

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

(U) EXECUTIVE SUMMARY

(U) Overview

~~(TS//SI//NF)~~ This report summarizes the results of our audit of National Security Agency (NSA) controls to comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (BR) Retention. From April through June 2011, we performed testing and procedural reviews to assess the Agency's compliance. On the basis of the information reviewed, we found no instances of non-compliance with the terms of the Order for BR retention for calendar year (CY) 2011. However, we noted three areas for future improvement: (1) develop a plan and written procedures to document the Agency's BR retention process, (2) develop a process to research quarantined records, and (3) accurately document parser configurations.

(U) Highlights

~~(TS//SI//NF)~~ The Agency should document the key initiatives and procedures that will be used to comply with the Order for BR retention in the future.

- ~~(TS//SI//NF)~~ **No formal BR retention plan or procedures**
  ~~(TS//SI//NF)~~ The Agency does not have a coordinated plan that documents the major initiatives for the BR retention process. Furthermore, the organizations responsible for maintaining BR systems, databases, and backups do not have written procedures to document their processes.

- (U//~~FOUO~~) **No process to research quarantined records**
  ~~(TS//SI//NF)~~ The Agency does not have a formal process to research quarantined records for reasonableness before their introduction into the Agency's BR repositories.

- (U//~~FOUO~~) **Inaccurate parser documentation**
  ~~(TS//SI//NF)~~ Documentation was not accurately maintained for the current parser configurations used to filter BR metadata.

(U) **Management Action**
(U//~~FOUO~~) Technology Directorate and Signals Intelligence Directorate personnel agreed with the Inspector General recommendations. The planned actions meet the intent of the recommendations.

(U) This page intentionally left blank.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

I. (U) BACKGROUND

~~(TS//SI//NF)~~ The Business Records (BR) Order

~~(TS//SI//NF)~~ Pursuant to a series of Orders issued by the Foreign Intelligence Surveillance Court (FISC) beginning in May 2006, the National Security Agency (NSA) has been receiving certain call detail records or telephony metadata from [redacted] telecommunication providers. NSA refers to the Business Records (BR) Orders collectively as the -BR Order‖ or -BR FISA.‖

~~(TS//SI//NF)~~ The BR Order provides NSA access to bulk call detail records that include records of telephone calls between the United States and abroad or wholly within the United States, [redacted] This collection of information is not wholly available to NSA through its other foreign intelligence information collection. It is valuable to NSA analysts tasked with identifying potential threats to the U.S. homeland and interests abroad because it enhances analysts' ability to identify, prioritize, and track terrorist operatives and their support networks in the United States and abroad, using call chaining analysis techniques.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ Provisions of the BR Order for Retention

~~(TS//SI//NF)~~ The Order requires that BR metadata be destroyed no later than five years (60 months) after its initial collection.[1] The Office of General Counsel (OGC) reviewed the Order and concluded that BR retention compliance should be determined using the date when records are received from providers, and not the call communication date.

- ~~(TS//SI//NF)~~ **Record receipt date** is the actual date when telecommunication carriers electronically provide BR metadata to NSA. Although record receipt dates have no analytical value, the Agency uses this information to determine BR retention compliance. Record receipt dates are separate and distinct from call communication dates.

- ~~(TS//SI//NF)~~ **Call communication date** is the date when a telephone call is made from one person (Selector A) to another person

[1] ~~(TS//SI//NF)~~ BR Order 11-57, dated 13 April 2011, defines telephone metadata as comprehensive communications routing information (e.g., originating and terminating telephone number), trunk identifier, telephone calling card numbers, and the time and duration of calls. Telephony metadata does not include the substantive content of a communication or the name, address, or financial information of a subscriber or customer.

(Selector B).[2] This date is important for intelligence analysis because it establishes a call association for a particular time between two selectors.

(U) **Timing differences with call communication dates and record receipt dates**

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

[redacted] Because of these differences, the Agency must track receipt dates for BR metadata to document compliance with the Order.

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ NSA Repositories that Store BR Metadata

~~(TS//SI//NF)~~ BR metadata [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- ~~(TS//SI//NF)~~ [redacted] is the Agency's corporate contact chaining database that accepts metadata from multiple sources [redacted]

(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ [redacted] s the corporate database repository that [redacted]

[2] ~~(S//SI//REL TO USA, FVEY)~~ A selector is an identifier used in dialed number recognition (e.g., telephone number) or in digital network intelligence [redacted] In this report, the terms Selector A and Selector B are used to identify different persons in telephone calls.

(b)(1)
(b)(3)-P.L. 86-36

[3] ~~(C//REL TO USA, FVEY)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- ~~(TS//SI//NF)~~ is the contingency database for
- ~~(TS//SI//NF)~~ is the system backup that stores an
- ~~(TS//SI//NF)~~ **Backup tapes** are maintained at

~~(TS//SI//NF)~~ Figure 1 illustrates the BR dataflows within the Agency and the various BR repositories.

~~(TS//SI//NF)~~ Figure 1. Business Records Dataflow

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

~~(C//REL TO USA, FVEY)~~ How information is stored [redacted] (b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] are the main databases used to store BR metadata for intelligence analysis. [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(C//REL)~~ Figure 2. [redacted] Architecture s (b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

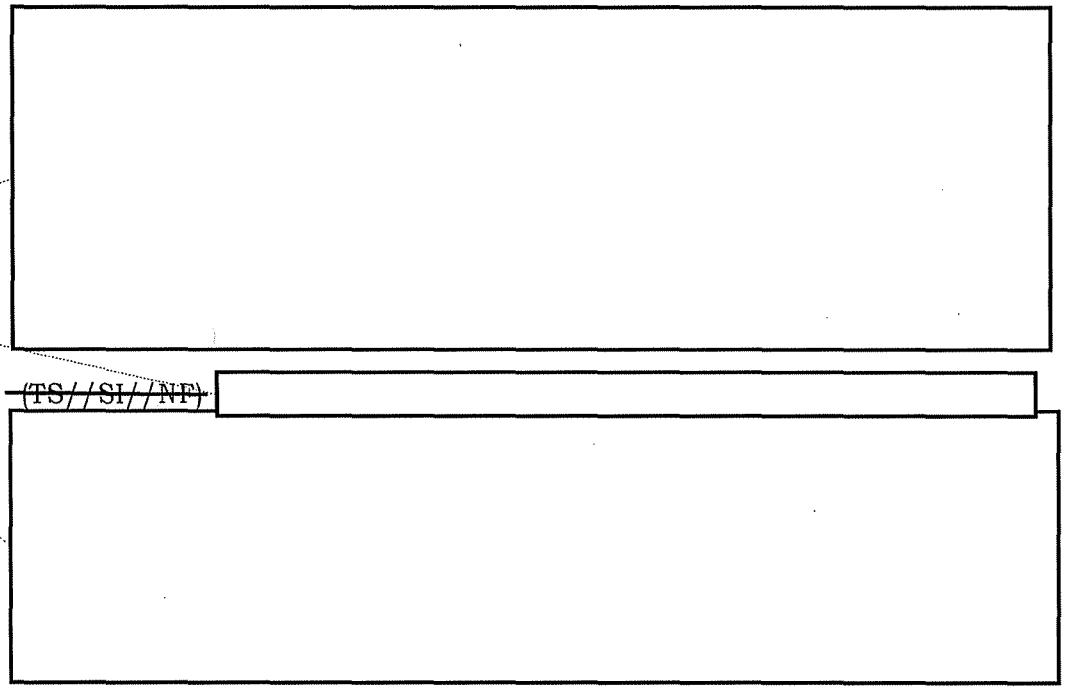
~~(TS//SI//NF)~~

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)



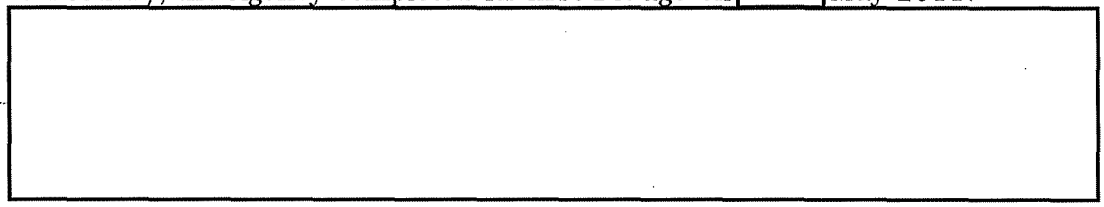
~~(TS//SI//NF)~~

~~(TS//SI//NF)~~ NSA's BR Age-Off Process

(b)(3)-P.L. 86-36

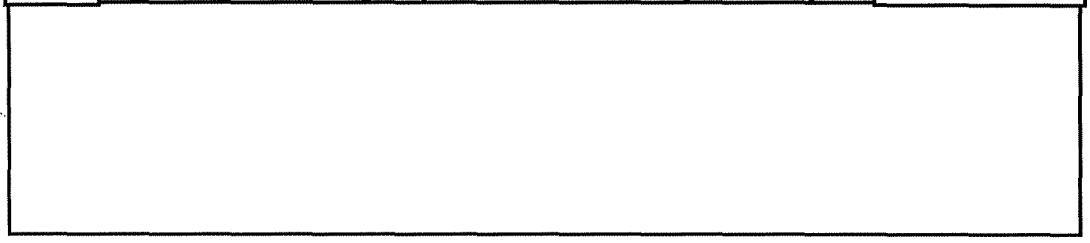
~~(TS//SI//NF)~~ To remain compliant with the terms of the Order (which states that BR metadata must be destroyed no later than five years after its initial collection), the Agency completed its first BR age-off [redacted] May 2011.

(b)(1)
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ For the CY 2011 age-off, BR metadata [redacted] was deleted from Agency databases and tape backups.[5] [redacted]



[4] (U//~~FOUO~~) A relational database stores data in tables using a standardized data format. This allows similar information to be organized and queried on the basis of specific data fields.

[5] ~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ Table 1 shows the procedural timeline used to complete the CY2011 BR age-off effort.

~~(TS//SI//NF)~~ **Table 1. Procedures Used to Complete the BR Age-Off**

~~(TS//SI//NF)~~

(b)(3)-P.L. 86-36

Dates	Procedure
	replaced as the Agency's official BR database. During the transition, BR transactions were historically downloaded into
	All hard drives that previously stored BR transactions were submitted for secure destruction.
	backup tapes that contained BR metadata were submitted for secure destruction.
	files were deleted. The remaining files in
	was taken out of service during the rebuild.
	SID analysts were redirected from to the backup database
	SID analysts were redirected back to
	The continuous flow of BR metadata was restored so that it again updated the Agency's BR repositories automatically. BR metadata received during the rebuild was downloaded into the Agency's BR databases.
	BR transactions manually saved to will be deleted and reloaded with the post-rebuild transactions

(b)(1)
(b)(3)-P.L. 86-36

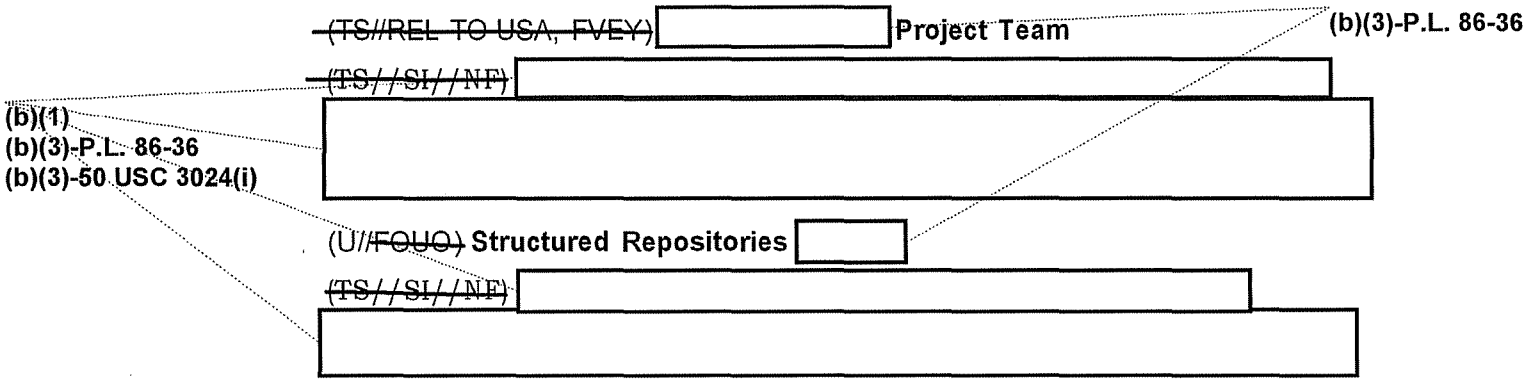
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

(U) Organization



(U) Audit Universe

(U) **General control environment assessment**

(TS//SI//NF) The audit scope focused on the manual and automated controls used to maintain compliance with the terms of the Order for BR retention for the Agency's BR repositories, system backups, and backup tapes. The BR repositories reviewed included the operational component of [redacted] We also observed the process for deleting BR files [redacted] and the physical storage and destruction procedures [redacted] We excluded from review BR information disseminated in Signals Intelligence reports.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) **Reviews to assess Agency compliance with the terms of the Order**

(TS//SI//NF) We performed five levels of review and observation to determine the Agency's compliance with the terms of the Order for BR retention. We also determined whether the Agency has a plan and organizational procedures to document the systems, resources, and organizations involved with the BR retention efforts.

- (U) Review 1: Tape, disk, and system backup data destruction
- (U) Review 2: Quarantined records
- (U) Review 3: System parser controls
- (U) Review 4: Selector pair testing
- (U) Review 5: Metrics analysis

(U//FOUO) A summary of the audit test results for the five levels are in Table 2 in the Finding and Recommendations Section. A detailed summary of the audit methodology and results for the selector pair testing and metrics analysis are in Appendix B.

II. (U) FINDING AND RECOMMENDATIONS

~~(TS//SI//NF)~~ BR Retention Practices Must Be Documented

~~(TS//SI//NF)~~ We found no instances of non-compliance with the terms of the Order for BR retention for CY2011. However, the Agency does not have a formal plan or written organizational procedures to document the systems, resources, and practices used to maintain compliance with the Order. Furthermore, documentation of the [redacted] was not accurately maintained. As a result, the Agency has an increased risk of non-compliance in the future.

(U) Criteria Used to Assess the Agency's Compliance with the Order

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ The BR Order requires that BR metadata be destroyed no later than five years after its initial collection. To maintain compliance, TD and SID decided to delete annually from Agency databases and tape storage BR metadata whose record receipt date is [redacted] For CY2011, the Agency deleted BR metadata received [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ We performed five levels of review to assess the adequacy of controls and to determine whether the Agency was in compliance with the terms of the BR Order. In addition, we determined whether the Agency has a formal plan and organizational procedures to document the key processes and the roles and responsibilities for the organizations involved in the BR rebuild. A majority of the audit focused on [redacted] and the tape and system backups because they stored BR metadata from the date of the original Order (May 2006).

(b)(3)-P.L. 86-36

1. ~~(TS//SI//NF)~~ ***Tape, disk, and system backup destruction practices for BR metadata received before*** [redacted] We evaluated the secure storage and destruction procedures for the [redacted] backup tapes [redacted] used to store BR metadata. We also observed the process for deleting the [redacted] system backup files and reviewed for compliance the data stored in the [redacted] COOP backup system.

2. ~~(TS//SI//NF)~~ ***Quarantined records*** [redacted] to develop a system quarantine process to document the records that

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted] We reviewed the quarantine process to determine whether an adequate audit trail was maintained to document the Agency's compliance with the Order.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ ***System parser controls*** System parsers are used to filter BR metadata of unwanted data before records are saved to Agency databases. To determine whether the parsers were working as intended, we performed testing in a simulated environment to verify that parsers (1) quarantined records with call communication dates [redacted] and (2) deleted suspected credit card information before processing records. We also reviewed whether documentation of the parser configurations used to filter BR metadata was accurately maintained.

(b)(3)-P.L. 86-36

3. ~~(TS//SI//NF)~~ ***Selector pair testing*** [redacted] call dates before [redacted] System testing was performed to determine whether these records were correctly processed with one of the following outcomes after the BR rebuild was complete:

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- (U//~~FOUO~~) *Deleted:* Performed for records that had call communication dates and receipt dates before [redacted]
- ~~(C//REL TO USA, FVEY)~~ *Modified:* Performed for records that had successive call dates that occurred on or after [redacted]

4. ~~(C//REL TO USA, FVEY)~~ ***Metrics analysis*** Summary metrics were obtained [redacted] (but before the quarantined records were introduced) as another check to verify that no records had first call dates before [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Audit Summary Results

(U//~~FOUO~~) Although we found no instances of non-compliance with the terms of the Order, we noted three areas for future improvement:

1. (U) Develop a plan and written procedures to document the rebuild.
2. (U) Establish a process to research quarantined records.
3. (U) Accurately document parser configurations.

(U//~~FOUO~~) These deficiencies are discussed in detail in the next section. Table 2 shows the summary results for the five areas reviewed.

(U) Table 2. Audit Summary Results

~~(TS//SI//NF)~~

Review Area	Summary Assessment
Tape, disk, and system backup destruction practices	**Compliant:** We found no instances of non-compliance with the Order for BR retention. • The [redacted] backup tapes were submitted for secure destruction. The backup tapes were securely stored in a locked cabinet inside a restricted access room [redacted] • [redacted] files [redacted] were deleted. • The [redacted] hard drives were erased and submitted for secure destruction. • The [redacted] backup was deleted of all BR metadata and repopulated [redacted]
Quarantined records	**Compliant *(with an exception noted)*:** We found no instances of non-compliance with the Order for BR retention. However, T1222's process for reviewing and researching quarantined records must be documented. • Adequate documentation was maintained for the approximately [redacted] records [redacted]
System parser controls	**Compliant *(with an exception noted)*:** We found no instances of non-compliance with the Order for BR retention. However, the Agency must ensure that configuration documentation accurately reflects the current operating parser configurations in use. • We performed [redacted] tests in a simulated environment that confirmed parsers correctly processed transactions [redacted] quarantined records [redacted] and deleted suspected credit card information from records.
Selector pair testing	**Compliant:** We found no instances of non-compliance with the Order for BR retention. • Sample testing verified that the integrity of the data (received before the rebuild began) could be relied on to conduct our selector testing. In total, [redacted] records [redacted] were randomly selected to verify that it met our criteria for testing. (Note: We could not perform a statistical verification because of the size of the sample universe [redacted] • The [redacted] records were found to be correctly deleted or modified (with [redacted] after the [redacted] rebuild was complete.
Metrics analysis	**Compliant:** We found no instances of non-compliance with the Order for BR retention. • The metrics analysis verified that no records [redacted] after the [redacted] rebuild was complete. This validation was performed before the [redacted] quarantined files were re-introduced.
(U) See Appendix B for a detailed explanation of the testing methodology and results for the selector pair test and metrics analysis. Only the areas with exceptions noted are presented in this section.	

~~(TS//SI//NF)~~

(b)(3)-P.L.

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L.

~~(TS//SI//NF)~~ BR Retention Practices Must Be Better Documented

(U) **The Agency does not have a process to research quarantined records**

(U//~~FOUO~~) We found no instances of non-compliance associated with the newly developed quarantine process. However, the Agency must establish a formal process to research quarantined records before their introduction into Agency repositories.

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(U) RECOMMENDATIO N 1

~~(TS//SI//NF)~~ Establish a process to research quarantined records before they are removed from quarantine and included in the Agency's BR repositories.

(ACTION: [redacted])

(U) Management Response **(b)(3)-P.L. 86-36**

CONCUR ~~(TS//SI//NF)~~ [redacted] will write a process to research and analyze any quarantined records in order to determine if any records should be included in the Agency's BR repositories.

(U) OIG Comment

(U//~~FOUO~~) The planned actions meet the intent of the recommendation.

(U) **Documentation did not accurately reflect parser configurations**

~~(TS//SI//NF)~~ Although we found no instances of non-compliance for the system controls used to filter BR metadata, the Agency must ensure that documentation accurately reflects the current parser configurations.

~~(TS//SI//NF)~~ The Agency receives raw BR metadata from [redacted] **(b)(3)-P.L. 86-36** telecommunication providers [redacted] Parsers are used to filter the BR metadata of unwanted information before it is saved to Agency databases. [redacted] Data Integrity Analysts (DIAs) stated that they have been actively working to document the parser configurations [redacted] However, the DIAs confirmed that the supporting documentation has not been consistently updated to

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted]

(U) **Action taken**

(U//~~FOUO~~) [redacted] DIAs finished their update of the parsers' configurations. This documentation was subsequently provided to the Office of the Inspector General.

(b)(3)-P.L. 86-36

(U) RECOMMENDATION 2

(U//~~FOUO~~) Update parser documentation to reflect accurately the current configurations in use. This documentation should be updated as new configuration changes are made to the parsers.

(ACTION: [redacted] and DIAs)

(b)(3)-P.L. 86-36

(U) Management Response

CONCUR (U//~~FOUO~~) [redacted] completed its update of the parser configurations [redacted] and will continue to update the documentation as configuration changes are made to the parsers. [redacted] will also review the documentation on a quarterly basis to verify it is up-to-date. **(b)(3)-P.L. 86-36**

(U) OIG Comment

(U//~~FOUO~~) Status: CLOSED. The actions addressed the recommendation.

~~(TS//SI//NF)~~ The Agency does not have a formal plan and organizational procedures to document its BR retention practices

~~(TS//SI//NF)~~ The Agency does not have a formal plan to document the BR retention requirements, the methodology used to maintain compliance for the enterprise, the systems and databases and other storage media that store BR data, the organizations responsible for carrying out the plan, and the milestones for completing future rebuilds. Furthermore, the organizations responsible for maintaining BR systems, databases, and backups [redacted] do not have written procedures to document their roles and responsibilities and processes to maintain BR retention compliance. As a result, the Agency has an increased risk for non-compliance in the future. [redacted] **(b)(3)-P.L. 86-36**

[redacted] **(b)(3)-P.L. 86-36**

(U) RECOMMENDATION 3

~~(TS//SI//NF)~~ Prepare a plan that documents the Agency's major initiatives for complying with the terms of the Order. This plan should be flexible and updated to reflect changes in the terms of the Order and in the systems and databases that store BR metadata, and the plan should identify organizational resources and milestones for completing future aging-off of BR metadata. Ensure that BR retention rules defined in the Order are documented in the Compliance Standard for Retention.

(ACTION: Chief, TD Office of Compliance with Deputy Director, T1)

(U) Management Response

CONCUR ~~(TS//SI//NF)~~ In June 2011, at the request of the Compliance Steering Group, the TD Office of Compliance (TV) and SID Office of Oversight and Compliance (SV) jointly authored an approach to developing compliance standards, deriving applicable technical requirements, and publishing the requirements for compliance certification. Consistent with the documented approach, the draft retention standard, including BR data, has been submitted to TV, which is documenting and vetting the technical requirements for retention (age-off). These requirements are expected to be published in October for developers' reference. At such time, T1 and other

developer organizations will be provided requirements specific to retention issues.

(U) OIG Comment

(U//~~FOUO~~) The planned actions meet the intent of the recommendation.

(U) RECOMMENDATION 4
~~(TS//SI//NF)~~ **Prepare written procedures that document the roles and responsibilities of the organizations involved in the BR retention effort. These procedures should also document the process for researching quarantined records and the requirements for maintaining accurate documentation for parser configurations as outlined in Recommendations 1 and 2.** **(ACTION: Chief, TD Office of Compliance and Deputy Director, T1)**

(U) Management Response

CONCUR ~~(TS//SI//NF)~~ TD Compliance will outline the roles and responsibilities for organizations involved in the BR process. T1 will describe the procedures for researching quarantine records. [redacted] will document their procedures to include roles, responsibilities and procedures for handling the BR data. We have requested the document be completed by the end of October. [redacted] will write procedures documenting [redacted] roles and responsibilities with regards to BR retention.

(b)(3)-P.L. 86-36

(U) OIG Comment

(U//~~FOUO~~) The planned actions meet the intent of the recommendation.

(U) This page intentionally left blank.

IV. (U) SUMMARY OF RECOMMENDATIONS

(U) RECOMMENDATION 1

~~(TS//SI//NF)~~ **Establish a process to research quarantined records before they are removed from quarantine and included in the Agency's BR repositories.**

(U) ACTION: [redacted]
(U) Status: OPEN/Concur
(U) Target Completion Date: [redacted] **(b)(3)-P.L. 86-36**

(U) RECOMMENDATION 2

(U//~~FOUO~~) Update parser documentation to reflect accurately the current configurations in use. This documentation should be updated as new configuration changes are made to the parsers.

(U) ACTION: [redacted] **and DIAs** **(b)(3)-P.L. 86-36**
(U) Status: CLOSED/Concur
(U) Completion Date: [redacted]

(U) RECOMMENDATION 3

~~(TS//SI//NF)~~ **Prepare a plan that documents the Agency's major initiatives for complying with the terms of the Order. This plan should be flexible and updated to reflect changes in the terms of the Order and in the systems and databases that store BR metadata, and the plan should identify organizational resources and milestones for completing future aging-off of BR metadata. Ensure that BR retention rules defined in the Order are documented in the Compliance Standard for Retention.**

(ACTION: Chief, TD Office of Compliance [redacted] **)** **(b)(3)-P.L. 86-36**
(U) Status: OPEN/Concur
(U) Target Completion Date: [redacted]

(U) RECOMMENDATION 4

~~(TS//SI//NF)~~ **Prepare written procedures that document the roles and responsibilities of the organizations involved in the BR retention effort. These procedures should also**

document the process for researching quarantined records and the requirements for maintaining accurate documentation for parser configurations as outlined in Recommendations 1 and 2.

(ACTION: Chief, TD Office of Compliance [redacted]
(U) Status: OPEN/Concur
(U) Target Completion Date: [redacted] **(b)(3)-P.L. 86-36**

V. (U) ACRONYMS AND ORGANIZATIONS

(U) BR	Business Records
(U) CY	Calendar Year
(U) DIA	Data Integrity Analyst
(U) FISA	Foreign Intelligence Surveillance Act
(U) FISC	Foreign Intelligence Surveillance Court
(U) COOP	Continuity of Operations
(U) OGC	Office of General Counsel
(U) MRG	Math Research Group
(U) NAS	Network Attached Storage
(U) NSA	National Security Agency
(U) SID	Signals Intelligence Directorate
(U)	
(U)	(b)(3)-P.L. 86-36
(U) TD	Technology Directorate
(U) T1	Mission Capabilities
(U) T1222	Knowledge Services
(U) T1313	Structured Repositories
(U) TV	Technology Directorate Office of Compliance

(U) This page intentionally left blank.

(U) APPENDIX A

(U) About the Audit

(U) This page intentionally left blank.

(U) ABOUT THE AUDIT

(U) Objectives

~~(TS//SI//NF)~~ The overall audit objective was to determine whether Agency controls are adequate to provide reasonable assurance of NSA compliance with the terms of the Foreign Intelligence Surveillance Court (FISC) Order regarding Business Records (BR) retention.

(U) Scope and Methodology

(U//~~FOUO~~) From April through June 2011, we performed testing and procedural walkthroughs to assess the adequacy of controls and to determine the Agency's compliance with the terms of the Order. Five levels of review were performed.

1. ~~(TS//SI//NF)~~ ***Tape, disk, and system backup destruction practices for BR metadata received before*** [redacted] We evaluated the secure storage and destruction procedures for the [redacted] backup tapes [redacted] used to store BR metadata. We also observed the process for deleting [redacted] Network Attached Storage (NAS) system backup files and reviewed for compliance the data stored in the [redacted] Continuity of Operations backup system.

(b) (3) -P.L. 86-36

2. ~~(TS//SI//NF)~~ ***Quarantined records*** We reviewed the quarantine process to determine whether an adequate audit trail documented the records that had call communication dates before [redacted] but were received on or after [redacted]

3. ~~(TS//SI//NF)~~ ***System parser controls*** To determine whether the parsers were working as intended, we performed testing in a simulated environment to verify that parsers (1) quarantined records with call communication dates before [redacted] and (2) deleted suspected credit card information before processing of records. We also reviewed whether documentation of the current parser configurations was accurately maintained.

(b) (1)
(b) (3) -P.L. 86-36
(b) (3) -50 USC 3024(i)

4. ~~(TS//SI//NF)~~ ***Selector pair testing*** [redacted]

5. ~~(C//REL TO USA, FVEY)~~ ***Metrics analysis*** Summary metrics were obtained [redacted] (but before the quarantined records were introduced) as another check to verify that no records had first call dates before [redacted] (b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

~~(TS//SI//NF)~~ We also determined whether the Agency has a formal plan and organizational procedures to document the key processes and the roles and responsibilities for the various organizations involved in the BR rebuild.

(U//~~FOUO~~) We corresponded with management and personnel from the Technology Directorate, the Signals Intelligence Directorate, the Office of the Director of Compliance, and the Office of General Counsel.

(U//~~FOUO~~) We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions according to our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions according to our audit objectives.

(U) Use of Computer-Processed Data

(b) (3)-P.L. 86-36

~~(C//REL TO USA, FVEY)~~ To perform this audit, we used data that originated from the [redacted] system. We used this information to perform our selector pair testing [redacted]

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

[redacted] records to verify the integrity of the data and to provide minimum assurance that it met our criteria for testing.

(U) Prior Coverage

~~(TS//SI//NF)~~ The NSA Office of the Inspector General (OIG) has not performed a previous audit or review of the Agency controls to assess compliance with the terms of the Order for BR retention. The NSA OIG completed on 21 December 2007 the Audit of Retention of Domestic Communications Collected Under the Foreign Intelligence Surveillance Act (ST-06-0007); however, that audit focused on inadvertent collection of Foreign Intelligence Surveillance Act domestic communications and whether the Agency was in compliance with the U.S. Signals Intelligence Directive (USSID) SP0018 special minimization procedures. In addition, the Audit on the Assessment of Management Controls for Implementing the FISC Order (ST-06-0018), completed on 5 September 2006, focused on the adequacy of management controls for processing and disseminating U.S. person information. Most recently, the BR Capstone Audit (ST-10-0004), 25 May 2011, evaluated the BR querying and dissemination controls.

(U) Management Control Program

~~(TS//SI//NF)~~ As part of the audit, we assessed the organization's control environment pertaining to the audit objective, as set forth in NSA/CSS Policy 7-3, *Internal Control Program*, 14 April 2006. The 2010 Vulnerability and Process Assessment completed by [redacted] did not report concerns applicable to BR retention.

(b) (3) -P.L. 86-36

(U) This page intentionally left blank.

(U) APPENDIX B

(U) Testing Methodologies and Results

(U) This page intentionally left blank.

(U) Testing Methodology and Results

(U) Selector Testing Methodology and Results

(U) **Selector pair methodology**

(b) (3) -P.L. 86-36

~~(TS//SI//NF)~~ The purpose of selector pair testing was to determine whether the contact chains [redacted] were compliant with the terms of the Order for BR retention. The Order requires that BR metadata be destroyed no later than five years (60 months) after its initial collection. To maintain compliance, the Technology Directorate and Signals Intelligence Directorate decided to delete annually from Agency databases and tape storage BR metadata whose record receipt date [redacted] For CY 2011, the Agency deleted BR metadata received before [redacted]

(b)(3)-P.L. 86-36

(U) The following methodology was used to complete the selector pair testing:

~~(C//REL TO USA, FVEY)~~ **Step 1** – Identify the contact chains [redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

[redacted]

~~(C//REL TO USA, FVEY)~~ [redacted]
these above criteria.

(U) **Step 2** – Verify that the data received in the Before and Span listings contained only selector pairs that met the criteria in Step 1.

- (U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

[redacted]

~~(C//REL TO USA, FVEY)~~ [redacted]

[redacted]

- ~~(C//REL TO USA, FVEY)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

(U) **Step 3** – Establish a test methodology and criteria for the selector pair testing.

(U) Before listing:

- ~~(C//REL TO USA, FVEY)~~
- ~~(C//REL TO USA, FVEY)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- ~~(C//REL TO USA, FVEY)~~

(U) Span listing:

(b)(1)
(b)(3)-P.L. 86-36

- ~~(C//REL TO USA, FVEY)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- ~~(C//REL TO USA, FVEY)~~

(b)(1)
(b)(3)-P.L. 86-36

~~(C//REL TO USA, FVEY)~~

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Step 4** – Verify that would work as intended for the selector pair testing.

- (U//~~FOUO~~)

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Step 5

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(C//REL TO USA, FVEY)~~ Step 6

(b)(1)
(b)(3)-P.L. 86-36

(U) **Selector pair test results**

(U//~~FOUO~~) We found no instances of non-compliance during the selector pair testing. Our testing found no error cases during the selector pair test.

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(C//REL)~~ Table B1. Rebuild (before and after metrics comparison)

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

Category	Before Rebuild	After Rebuild
		0
		0
Quarantined records added back (after rebuild)		
Total records		
Expected total records		
Actual total records		
Net records excluded by parsers during rebuild		

* ~~(TS//SI//NF)~~
† ~~(TS//SI//NF)~~
‡ ~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

(U) Metrics Analysis Methodology and Results

(U) **Metrics analysis**

(U//~~FOUO~~) We found no instances of non-compliance during our metric analysis. However, we were unable to perform both parts of the metrics analysis as originally planned in the Audit Guide.

~~(TS//SI//NF)~~ The intended purpose of the metrics analysis was twofold: (1) confirm that all records before [redacted] were removed from the [redacted] database, and (2) verify that the total number of records could be accounted for before and after the [redacted] rebuild was complete. Although we were able to verify the first part, in that the selector pair testing confirmed that the [redacted] records with first call dates before [redacted] could be accounted for (i.e., deleted or modified, or excluded by parsers on the basis of current configurations), we were unable to verify the second part of the metrics analysis because the net number of records decreased by approximately [redacted] (see Table B1). However, [redacted] officials anticipated that there would be some differences before the rebuild effort began, and their explanations seem reasonable.

(b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36
(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Specifically, [redacted] concluded that the decrease of [redacted] records happened because the rebuild had been performed using the most current parser configurations, which had been refined over time to capture more precisely records with a Counterterrorism value. As a result, the current parsers allowed fewer records in aggregate to be downloaded into [redacted] than the total sum of the records previously allowed during the parsers' five-year span.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Examples of modifications made to the parser configurations designed to prevent certain types of records from being processed include instances in which:

- ~~(TS//SI//NF)~~ [redacted] were excluded because they had little or no Counterterrorism value,
- ~~(TS//SI//NF)~~ [redacted] was excluded,
- ~~(TS//SI//NF)~~ [redacted] was excluded, and
- ~~(TS//SI//NF)~~ records were rejected [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) APPENDIX C

(U) Full Text of Management Response

(U) This page intentionally left blank.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
OIG	10690-11	

THRU	ACTION	EXREG SUSPENSE
	[ ] APPROVAL	
SUBJECT: (U//~~FOUO~~) SIGINT Directorate Response to the OIG Draft Report on the Audit of NSA Control to Comply with the FISC Order Regarding Business Record Retention (ST-11-0011)	[ ] SIGNATURE	KCC SUSPENSE
	[X] INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION: SID, S02, S3

SUMMARY

PURPOSE: (U//~~FOUO~~) To provide the SIGINT Directorate's (SID) response to the Office of the Inspector General (OIG) Draft Report on the Audit of NSA Control to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Record (BR) Retention (ST-11-0011).

BACKGROUND: (U//~~FOUO~~) From April through June 2011 the NSA OIG performed testing and procedural reviews to assess the Agency's compliance with BR retention. On the basis of the information reviewed, the OIG found no instances of non-compliance for the CY2011 terms. However, three areas were noted for future improvement: (1) develop a plan and written procedures to document the Agency's BR retention process, (2) develop a process to research quarantined records, and (3) accurately document parser configurations. As a result, a single recommendation (Recommendation 2) was assigned to the [redacted] and it states, *"(U//~~FOUO~~) Update parser documentation to reflect accurately the current configurations in use. Going forward, this documentation should be updated as new configuration changes are made to the parsers."*

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Recommendation 2 was subsequently tasked to SID for written acknowledgement on the validity of the issue and identification of planned corrective actions.

DISCUSSION: (U//~~FOUO~~) SID concurs on Recommendation 2. [redacted] completed its update of the parser configurations [redacted] and will continue to update the documentation as configuration changes are made to the parsers. [redacted] will also review the documentation on a quarterly basis to verify it is up-to-date.

(U) SID requests OIG closure of Recommendation 2.

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
SID	[redacted] 9/22/11		S3	[redacted] 20 Sep 11	966-6831
S02	[redacted] 9/22/11				
S0232	[redacted] 22 Sep 11				

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
[redacted] SID IG Liaison	S023	966-2464	21 September 2011

FORM A6796

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360607

(b)(3)-P.L. 86-36

SECURITY CLASSIFICATION
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

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

TD Response to ST-11-0011

Factual Accuracy: T1 comments

1. The term "Call receipt date" could be misleading. Suggest using the term "Record Receipt Date". NSA does not receive "calls" from the providers, we receive metadata records.

Recommendation #1: ~~(TS//SI//NF)~~ Establish a process to research quarantined records before they are removed from quarantine and included in the Agency's BR repositories.

LEAD ACTION: Chief, [redacted]

CONCUR/NON-CONCUR: Concur with recommendation. [redacted] will write a process to Research and Analyze any quarantined records in order to determine if any records should be included in the Agency's BR repositories.

ESTIMATED COMPLETION DATE: [redacted] **(b)(3)-P.L. 86-36**

Approved by [redacted] Chief T1

Recommendation #3: ~~(TS//SI//NF)~~ Prepare a plan that documents the Agency's major initiatives for complying with the terms of the Order. This plan should be flexible and updated to reflect changes in terms of the Order, systems and databases that store BR metada, and identify the organizational resources and milestones for completing future aging-off efforts of BR metada. Furthermore, ensure BR retention rules as defined in the Order are documented in the Compliance Standard for Retention.

LEAD ACTION: Chief TD Office of Compliance and Deputy Director, T1)

CONCUR/NONCONCUR: Concur: In June 2011, at the request of the Compliance Steering Group, TV and SV jointly authored the approach to developing compliance standards, deriving applicable technical requirements, and publishing the requirements for compliance certification. Consistent with the documented approach, the draft Retention standard, to include BR data, has been submitted to TV. And TV is currently documenting and

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20361001

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

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

vetting the technical requirements for retention (age-off). These requirements are expected to be published in October for developers' reference. At such time, T1 and other developer organizations will be provided requirements specific to retention issues.

ESTIMATED COMPLETION DATE: Compliance certifications will include a verification of retention procedures/code as of [redacted]

(b)(3)-P.L. 86-36

Recommendation #4: ~~(TS//SI//NF)~~ Prepare written procedures that document the roles and responsibilities for the organization involved in the BR retention effort. These procedures should also document the process for researching quarantined records and the requirements for maintaining accurate documentation for parser configurations as outlined in Recommendations 1 and 2, respectively. **(ACTION:** Recommend Changing Office Responsibility for this action to Chief TD Office of Compliance and Deputy Director, T1 "Vice" [redacted]**)**

CONCUR/NON-CONCUR: Concur with modified recommendation. TD Compliance will outline the roles and responsibilities for organizations involved in the BR process. T1 will describe the procedures for researching quarantine records. The [redacted] development team [redacted] will document their procedures to include roles, responsibilities and procedures for handling the BR data. We have requested the document be completed by [redacted] [redacted] will write procedures documenting [redacted] roles and responsibilities with regards to BR retention.

ESTIMATED COMPLETION DATE: [redacted]

General Comments:

(b)(3)-P.L. 86-36

- The first two pages of the OIG document have the classification set to TOP SECRET//SI//**NORFORN** instead of NOFORN.
- Recommend that the final version of this report be provided to the [redacted] team for use in developing requirements for the BR-FISA portion of [redacted] The organization is [redacted]

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

(U) This page intentionally left blank

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

~~(TS//SI//NF)~~ Report on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Collection

ST-12-0003
01 August 2012

Derived From: NSA/CSS Manual 1-52
Dated: 08 January 2007
Declassify On: 20370108

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

ST-12-0003

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

01 August 2012
IG-11437-12

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Report on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Collection (ST-12-0003)—ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This report summarizes our review on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Collection and incorporates management's response to the draft report.

2. (U//~~FOUO~~) As required by NSA/CSS Policy 1-60, *NSA/CSS Office of the Inspector General,* actions on OIG recommendations are subject to monitoring and follow-up until completion. Consequently, we ask that you provide a written report concerning each "OPEN" recommendation in the following circumstances: when your action plan has been fully implemented; when your action plan has changed; or if the recommendation is no longer valid. The report should provide sufficient information to show that corrective actions have been completed. If a planned action will not be completed by the original target completion date, please state the reason for the delay and give a revised target completion date. Reports should be sent to [redacted] Assistant Inspector General for Follow-up, at OPS 2B, Suite 6247 or by email at [redacted] (b)(3)-P.L. 86-36

3. (U) We appreciate the courtesy and cooperation extended to our staff throughout the review. For additional information, please contact [redacted] at 963-0936(s) or by e-mail at [redacted]

George Ellard

GEORGE ELLARD
Inspector General

ST-12-0003

(U//~~FOUO~~) DISTRIBUTION:
DL SIDIGLIAISON
DL TD_REGISTRY

cc:
DOC (J. Delong)
D4
OGC
ST
SV
SV4
SV42
S3132
S31323
S353
S3531
TV
T12
T121
T122
T1222
T131
T1313

(b)(3)-P.L. 86-36

DOJ NSD

(b)(6)

IG
D/IG
D1
D11
D12
D13
D14

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

(U) EXECUTIVE SUMMARY

(U) Overview

~~(TS//SI//NF)~~ This report summarizes the results of our special study of National Security Agency (NSA) controls to comply with the Foreign Intelligence Surveillance Court Order regarding business records (BR) collection. From December 2011 through March 2012, we performed testing and procedural reviews to assess the Agency's compliance. Other than one incident NSA reported during our review, we found no other instance of non-compliance with the terms of the Order for BR collection during calendar year 2011. However, we noted areas for improvement.

(U) Highlights

~~(TS//SI//NF)~~ The Agency should improve BR processes to strengthen controls and help reduce the risk of non-compliance.

- ~~(TS//SI//NF)~~ **Program material** BR FISA program material is not centrally located or accessible to stakeholders.
- ~~(TS//SI//NF)~~ **Meeting notes** Meeting notes of mandatory quarterly meetings with Department of Justice National Security Division are not kept.
- ~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- ~~(TS//SI//NF)~~ **Management oversight** Management does not have a process to review sampling.
- (U//~~FOUO~~) **Structure code test** There is no process for periodic reviews of the structure code test used in sampling.

(U) **Management Action**

(U//~~FOUO~~) Signals Intelligence Directorate personnel agreed with the Inspector General recommendations. The planned actions meet the intent of the recommendations.

(U) This page intentionally left blank.

I. (U) BACKGROUND

~~(TS//SI//NF)~~ Business Records (BR) Order

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ Pursuant to a series of Orders issued by the Foreign Intelligence Surveillance Court (FISC) beginning in May 2006 to comply with the Foreign Intelligence Surveillance Act of 1978 (FISA), the National Security Agency (NSA) has been receiving certain call detail records (CDRs) or telephony metadata from [redacted] telecommunication s providers. NSA refers to these BR Orders collectively as the "BR Order" or "BR FISA."

~~(TS//SI//NF)~~ The BR Order provides NSA access to records of telephone calls between the United States and abroad or wholly within the United States. [redacted] This collection of information is not available to NSA through its other foreign intelligence information collection. It is valuable to NSA analysts tasked with identifying potential threats to the U.S. homeland and interests abroad because it enhances analysts' ability to identify, prioritize, and track terrorist operatives and their support networks in the United States and abroad, primarily using call chaining analysis.

~~(TS//SI//NF)~~ Collection provisions of the BR Order

~~(TS//SI//NF)~~ The BR Order requires providers to provide daily an electronic copy of all records or telephony metadata. The Order defines telephony metadata as comprehensive communications routing information, including but not limited to session-identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity number, International Mobile Station Equipment Identity number, trunk identifier, telephone calling card numbers, and time and duration of call). Telephony metadata does not include the substantive content of communication s or the name s, address es, and financial information of customer s.

~~(TS//SI//NF)~~ **Exhibit B** For each renewal of requested authority, NSA must file with the FISC a report that describes, among other things, proposed significant changes to the way in which the CDRs are received from providers and significant changes to the controls NSA has in place to receive, store, process, and disseminate BR metadata.

~~(TS//SI//NF)~~ **Exhibit C** At least once during the authorization period of an Order, NSA's Office of General Counsel (OGC), its Office of the Director of Compliance (ODOC), the Department of Justice's National Security Division (DoJ NSD), and other appropriate NSA representatives must meet to assess compliance with the FISC Orders. Traditionally, this meeting must include a review of a sample of records obtained to ensure that only approved metadata is being acquired. The results of this meeting must be submitted

to the FISC in writing as part of any application to renew or reinstate the authority requested. Exhibit C of the application summarizes the quarterly meeting [redacted] the requirement of the Order to review a sample of records obtained changed to a review of NSA's monitoring and assessment to ensure that only approved metadata are being acquired.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ **BR collection process**

~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ [redacted]

[redacted] The FISC Order does not require [redacted] to produce telephony metadata for communications originating and terminating in foreign countries.

~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~ Criteria to Assess Agency Compliance with the BR Order

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ BR Order

~~(TS//SI//NF)~~ Minimization procedures in FISC BR Order require that NSA and DoJ NSD conduct oversight of NSA's activities. The Order states that at least once during the authorization period:

> ~~[TS//SI//NF]~~ NSA's OGC, Office of Director of Compliance (ODOC), NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with the Court's Order. Included in this meeting will be a review of a sample of the call detail records obtained to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein. the requirement of the Order to review a sample of records obtained, changed to a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. For each renewal of requested authority, NSA must file with the FISC a report that describes, among other things, a description of any proposed significant changes in the way in which records would be received from the Providers and any significant changes to controls NSA has in place to receive, store, process, and disseminate the BR metadata.

(b)(1)
(b)(3)-P.L. 86-36

(U) Internal controls

(U) NSA/CSS Policy 7-3, *Managers' Internal Control Program*, 14 February 2012, implements the Government Accountability Office's *Standards for Internal Control in the Federal Government*, November 1999. Policy 7-3 requires managers "to institute the needed controls." According to the policy, internal control is

[1] ~~(C//REL TO USA, FVEY)~~

[2] ~~(TS//SI//NF)~~ On the basis of factual and practical considerations of everyday life on which reasonable and prudent persons act, there is a RAS that the selection term to be queried is

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[U] a system of guidance, instructions, policies, regulations, procedures, rules or other organizational instructions intended to determine the methods to be employed to carry out mission or operational actions or objectives, and ensure that programs achieve intended results.

~~(TS//SI//NF)~~ Table 1 depicts NSA/CSS Policy 7-3 categories of internal controls, which we applied to the BR FISA Program to evaluate the risk of non-compliance .

(U) Table 1: NSA/CSS Policy 7-3 Categories of Internal Controls

(U)

Control	Description
Documentation	(U) Established written procedures that are complete, accurate, and available for examination. Consists of regulations, policies, procedures, and/or standard operating procedures.
Record	(U) A written description of what has happened.
Structure	(U) Key duties and responsibilities in authorizing, processing, recording, and reviewing official NSA/CSS transactions should be separated among individuals. Managers should exercise appropriate oversight to ensure that individuals do not exceed or abuse their assigned authorities.
Authorization	(U) Procedures are in place to prevent people from exceeding their authority or misusing government resources.
Management	(U) Consists of the assignment, review, and approval of work. This control requires that management provide guidance and training to reduce loss of resources and increase achievement of results.
Security	(U) Any method or device that can be used to restrict access to government resources. This control may utilize safes, vaults, locked rooms, locked desk drawers, computer log-on identification , and passwords.

(U)

II. (U) FINDING AND RECOMMENDATIONS

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ FINDING: BR Program Processes Must Be Improved

~~(TS//SI//NF)~~ Other than the compliance incident described, we found no other instance of non-compliance with the Order for BR Retention during CY2011. However, the Agency must centralize program documentation and make it accessible to all stakeholders. Notes of mandatory quarterly meetings with DoJ NSD personnel should be kept. [redacted] ***Management reviews of sampling that*** [redacted] ***personnel perform is required. The structure code used in sampling*** [redacted] ***should be reviewed and updated periodically. Improving BR processes will strengthen the controls already in place and help reduce risk of non-compliance.***

(U) Non-Compliance Incidents

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ During our review, NSA filed with the FISC [redacted] a Notice of Compliance Incident in accordance with paragraph 13(b) of the FISC Rules of Procedure explaining that [redacted] records [redacted] contained credit card information. Notification to the FISC was not provided upon recognition because it was OGC's understanding that this must be reported only when credit card information was viewable by analysts in [redacted] Subsequently, OGC learned that DoJ maintains a different view: Identification of credit card information, regardless of whether the credit card information was viewable by intelligence analysts, must be reported to the Court. According to [redacted] analysts, credit card information never entered [redacted] because the parser rules prevented the fields from being ingested. [redacted] is responsible for updating parser rules and performs daily and weekly sampling of records to identify non-compliant data.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Program Documentation

~~(TS//SI//NF)~~ The BR FISA program has two SharePoint sites that contain historical information on the program. One site is maintained by the [redacted] and contains e-mails from a former BR FISA Program Manager. The second site is sporadically maintained by personnel from Oversight and Compliance (SV). [redacted]

(b)(3)-P.L. 86-36

[redacted]

~~(TS//SI//NF)~~ The BR FISA Program Lead is concerned that program documentation is in different locations and is not updated on the SharePoint site. He believes that all program material should be maintained centrally and be easily accessible. He stated that a recent response to a Congressional "Question for the Record" might not have been consistent with a previous response because the historical information was not included on the SharePoint site for reference.

~~(TS//SI//NF)~~ In addition to a weekly compliance meeting with NSA stakeholders, there is a Court-mandated quarterly compliance meeting of DoJ NSD, NSA OGC, NSA ODOC, and other NSA personnel. Representatives of the OIG attended a quarterly compliance meeting on 1 February 2012, and questions regarding previous quarterly meetings were raised. The OIG observed NSA participants recollecting decisions and discussions from previous meetings. NSA does not maintain notes of discussions and decisions made during these mandatory meetings.

~~(TS//SI//NF)~~ Part of the reason that program documentation is not updated centrally and meeting notes are not maintained is that the BR FISA Program no longer has a Program Management Office (PMO). The Program Lead has no staff and relies on individuals from various organizations. [redacted]

(b)(3)-P.L. 86-36

[redacted]

(U//~~FOUO~~) **Effect** Lack of complete and final historical documentation in a central location accessible to stakeholders could lead to misinformed decisions and reporting on the program.

RECOMMENDATION 1
~~(TS//SI//NF)~~ **Consolidate and maintain all final BR FISA Program material in a central location accessible to NSA stakeholders.** **(ACTION: BR FISA Program Lead)**

(U) Management Response

(U) **AGREE** All final program material will be maintained on the existing SV SharePoint site by 28 September 2012.

(U) OIG Comment

(U) Planned action meets the intent of the recommendation. Upon confirmation that all final program material is consolidated on the SV SharePoint site, the OIG will close this recommendation.

RECOMMENDATION 2
~~(TS//SI//NF)~~ **Maintain meeting notes of quarterly compliance meetings with DoJ NSD.** **(ACTION: BR FISA Program Lead)**

(U) Management Response

(U) **AGREE** Management will maintain quarterly compliance meeting documentation on the SV SharePoint site.

(U) OIG Comment

(U) Planned action meets the intent of the recommendation. Upon confirmation that management maintains quarterly compliance meeting notes on the SV SharePoint site, the OIG will close this recommendation.

(U) Reconciling Data from Providers

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ **Effect** Reconciling [redacted] would identify problem s with provider [redacted]

(b)(1)
(b)(3)-P.L. 86-36

RECOMMENDATION 3

~~(TS//SI//NF)~~ **Reconcile periodically** [redacted] **NSA receives.**

(ACTION: [redacted]

(U) Management Response

(U) **AGREE** For each provider, management will establish a reasonable periodicity for reconciliation that is technically feasible, yet meets OIG's recommendation.

(U) OIG Comment

(U) Planned action meets the intent of the recommendation. Upon confirmation that management has begun reconciling the number of BRs that providers send with the number NSA receives, the OIG will close this recommendation.

(U) Management Reviews and Structure Code

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] management receives weekly BR FISA compliance reports and biweekly status reports and attend s monthly project review meetings on the BR FISA compliance work performed by [redacted] personnel. However, [redacted] management does not review [redacted] personnel 's daily and weekly sampling of records received from providers.

(U//~~FOUO~~) GAO's *Standards for Internal Control in the Federal Government* include monitoring: Internal controls should generally be designed to ensure that ongoing monitoring occurs in the course of normal operations. This includes regular management and supervisory activities, comparisons, reconciliations, and other actions that personnel should take in performing their duties.

~~(TS//SI//NF)~~ [redacted] personnel run daily and weekly queries on CDRs to answer five questions , as part of the sampling process controls to verify NSA's compliance with the Order:

1. ~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36

2. ~~(TS//SI//NF)~~ [redacted]

(b)(3)-P.L. 86-36 3. (U//~~FOUO~~) [redacted] adhere to expectations?

4. ~~(TS//SI//NF)~~ Did [redacted] adhere to expectations? (b)(1) (b)(3)-P.L. 86-36

5. ~~(TS//SI//NF)~~ Did [redacted] adhere to expectations?

~~(TS//SI//NF)~~ The results of [redacted] sampling are submitted to ODOC in weekly BR FISA compliance reports. ODOC compiles the information with other compliance reports and provides it to the Director of Compliance for review. ODOC summarize s the weekly BR FISA compliance reports for DoJ NSD's review before quarterly compliance review meetings.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Each day, [redacted] runs manual scripts on all records for [redacted] that carry calling card numbers. NSA is not authorized to receive customer financial information; therefore, [redacted] checks these feeds [redacted] for credit card number s [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ **Effect** Management's review of the sampling of records that [redacted] personnel perform will provide a layer of oversight and help ensure compliance with the Order. [redacted]

(b)(3)-P.L. 86-36

[redacted]

RECOMMENDATION 4

(U//~~FOUO~~) Implement a management review process of the sampling that [redacted] personnel perform.

(ACTION: [redacted]

(U) Management Response

(U) **AGREE** Management implemented a review process in June 2012 to review the sampling during the team's monthly project review meeting.

(U) OIG Comment

(U) Planned action meets the intent of the recommendation. This recommendation is closed.

RECOMMENDATION 5
(U//~~FOUO~~) Implement a process to conduct periodic reviews of the structure code. (ACTION:)

(U) Management Response

(U) **AGREE** has implemented a process to review the structure code quarterly to verify that software remains up-to-date.

(b)(3)-P.L. 86-36

(U) OIG Comment

(U) Planned action meets the intent of the recommendation. This recommendation is closed.

III. (U) OBSERVATIONS

(U) Parameters for Defining Significant Changes

~~(TS//SI//NF)~~ Guidelines have not been established to define significant changes in the way that records are received or in the controls NSA has in place for BR metadata.

~~(TS//SI//NF)~~ For each renewal of authority, NSA must file with the FISC a report, Exhibit B, that describes significant changes proposed to the way records are received from providers and to the controls NSA has in place to receive, store, process, and disseminate records.

~~(TS//SI//NF)~~ The OIG asked stakeholders for the definition of "significant" or agreed-on guidelines for determining significance, but a common definition could not be identified. [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted] OGC believes that items that could be considered significant would be discussed during the weekly BR FISA meetings. NSA OGC and DoJ NSD ultimately determine what is reported as significant.

OBSERVATION
~~(TS//SI//NF)~~ **Nonexistent guidelines for determining significant changes might cause inconsistent reporting. BR FISA program stakeholders should consider defining "significant."**

~~(TS//SI//NF)~~ NSA has been inconsistent in its Exhibit B reports to the FISC about whether there have been significant changes. The OIG reviewed all Exhibit B reports for CY2011 to identify the information included in these reports and determine whether significant changes to controls had been reported. Of the [redacted] Exhibit B filings in CY2011, only one did not mention whether NSA is proposing significant changes to the way records are received from providers or significant changes to controls.

(b)(3)-P.L. 86-36

OBSERVATION
~~(TS//SI//NF)~~ **Inconsistent reporting in Exhibit B might cause confusion about whether significant changes have occurred. Establishing consistent criteria in Exhibit B reporting should be considered.**

~~(TS//SI//NF)~~ Disclosures in Exhibit C Filings

~~(TS//SI//NF)~~ Exhibit C filings to the FISC summarize meetings between NSA and DoJ NSD to assess compliance with the FISC Orders. These representatives must meet at least once during the authorization period (usually every 90 days), and the results of this meeting must be submitted to the FISC in writing.

~~(TS//SI//NF)~~ Information reported in the Exhibit C filings is inconsistent. For example, BR 11-07 Exhibit C, 20 January 2011, reported that, on 8 December 2010, DoJ NSD, NSA OGC, NSA ODOC, and NSA Signals Intelligence Directorate personnel met to discuss implementation of the FISC authorization in a manner that complies with that authorization. However, there was no specific statement that NSA was in compliance with the FISC's Order and no mention of the results of OGC's sampling of BR to ensure that NSA was not receiving unauthorized data. By comparison, BR 11-57 Exhibit C, 13 April 2011, stated that on 23 February 2011 representatives reviewed a sample of CDRs and concluded, on the basis of this review and representations of responsible personnel, that only approved metadata was being acquired.

OBSERVATION
~~(TS//SI//NF)~~ Although DoJ NSD personnel submit Exhibit C and are responsible for its content, NSA OGC personnel review the submission. NSA OGC should recommend that DoJ NSD address the terms of the Order consistently in Exhibit C reports.

IV. (U) SUMMARY OF RECOMMENDATIONS

RECOMMENDATION 1

~~(TS//SI//NF)~~ **Consolidate and maintain all final BR FISA Program material in a central location accessible to NSA stakeholders.**

(U) ACTION: BR FISA Program Lead
(U) Status: OPEN
(U) Target Completion Date: [redacted]

(b)(3)-P.L. 86-36

RECOMMENDATION 2

~~(TS//SI//NF)~~ **Maintain meeting notes of quarterly compliance meetings with DoJ NSD.**

(U) ACTION: BR FISA Program Lead
(U) Status: OPEN
(U) Target Completion Date: [redacted]

(b)(1)
(b)(3)-P.L. 86-36

RECOMMENDATION 3

~~(TS//SI//NF)~~ **Reconcile periodically** [redacted] **NSA receives.**

(U) ACTION: [redacted]
(U) Status: OPEN
(U) Target Completion Date: [redacted]

RECOMMENDATION 4

(U//~~FOUO~~) Implement a management review process of the sampling that [redacted] **personnel perform.**

(U) ACTION: [redacted]
(U) Status: Closed

(b)(3)-P.L. 86-36

RECOMMENDATION 5

(U//~~FOUO~~) Implement a process to conduct periodic reviews of the structure code.

(U) ACTION: [redacted]
(U) Status: Closed

(U) This page intentionally left blank.

V. (U) ABBREVIATIONS AND ORGANIZATIONS

(U) BR	Business Records
(U) CDR	Call Detail Record
(U) DoJ	Department of Justice
(U) FISA	Foreign Intelligence Surveillance Act
(U) FISC	Foreign Intelligence Surveillance Court
(U) FTP	File Transfer Protocol
(U) GAO	Government Accountability Office
(U) NSD	National Security Division
(U) ODOC	Office of the Director of Compliance
(U) OGC	Office of General Counsel
(U) [redacted]	[redacted]
(U) PMO	Program Management Office
(U) RAS	Reasonable Articulable Suspicion
(U) SCIF	Sensitive Compartmented Information Facility
(U) [redacted]	[redacted]
(U) [redacted]	[redacted]

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) APPENDIX A

(U) About the Special Study

(U) This page intentionally left blank.

(U) ABOUT THE SPECIAL STUDY

(U) Objectives

~~(TS//SI//NF)~~ The overall objective of this study was to determine whether Agency controls are adequate to provide reasonable assurance that NSA complies with the terms of the Foreign Intelligence Surveillance Court (FISC) Order for Business Records (BR) for collection of BR metadata.

1. ~~(TS//SI//NF)~~ **Objective 1:** Determine the controls the Agency has implemented for collection of BR metadata in accordance with the Order.
2. ~~(TS//SI//NF)~~ **Objective 2:** Determine whether Agency personnel are following the requirements of the Order by meeting and reviewing samples of records.
3. ~~(TS//SI//NF)~~ **Objective 3:** Determine whether Agency personnel are following the requirements of the Order by filing the required information with the FISC every 30 days.

(U) Scope and Methodology

(U) Scope

~~(TS//SI//NF)~~ The review focused on the manual and automated controls for collection of BR. We verified whether procedures have been implemented to provide a level of assurance that non-compliant data will not be collected or if inadvertently collected will be swiftly expunged and not made available for analysis. We tested whether NSA is compliant with the Order by meeting at least once during each authorization period and reviewing samples of call detail records (CDRs) to ensure that only approved metadata is acquired. We verified that every 30 days, NSA files with the FISC a report that describes significant changes to the way CDRs are received and to the controls in place for receiving CDRs.

(U) Methodology

(U//~~FOUO~~) We reviewed the following documentation:

- ~~(TS//SI//NF)~~ All [redacted] Exhibit C filings for CY2011 to ensure that NSA is compliant with the reporting requirements of the Order.

(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ All [redacted] Exhibit B reports for CY2011 to ensure NSA's compliance with the reporting requirements in the Order by identifying whether NSA reported significant changes in controls and the way CDRs are received.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- ~~(TS//SI//NF)~~ The [redacted] parser rules for the [redacted] feeds. We compared the rules [redacted] and observed [redacted] personnel run daily and weekly queries and the results of those queries used for sampling CDRs.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ In addition, we interviewed personnel from [redacted] Counterterrorism, Office of General Counsel, Office of the Director of Compliance, and SID Oversight and Compliance to document the roles and responsibilities of each organization in relation to the requirements of the Order.

(U) Prior Coverage

~~(TS//SI//NF)~~ The Office of the Inspector General's (OIG) *Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court Order: Telephony Business Records* (ST-06-0018), 5 September 2006, concluded that control procedures for collecting telephony metadata under the Order had not been formally designed and clearly documented. As a result, management controls did not provide reasonable assurance that NSA would comply with the Order. We recommended that, at a minimum, procedures be established to:

- (U//~~FOUO~~) Monitor incoming data regularly,
- (U//~~FOUO~~) Suppress from analysts' view unauthorized data that is discovered , and
- (U//~~FOUO~~) Eliminate unauthorized data from the incoming data stream.

(U//~~FOUO~~) The report's formal recommendation was for Agency management to design procedures to provide a higher level of assurance that non-compliant data will not be collected or if inadvertently collected will be swiftly expunged and not made available for analysis.

~~(TS//SI//NF)~~ Management concurred with the OIG's finding and recommendation and stated that it had partially implemented the recommended procedures to block questionable data from providers' incoming dataflow.

~~(TS//SI//NF)~~ The OIG's *Report on the Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Retention* (ST-11-0011), 20 October 2011, concluded that documentation was not accurately maintained for the current parser configurations used to filter BR metadata of unwanted information before it is saved to Agency databases. Before the issuance of the report, [redacted] completed its update of parser configurations .

(b)(3)-P.L. 86-36

(U) Management Control Program

~~(TS//SI//NF)~~ As part of our study, we obtained and reviewed the Vulnerability and Process Assessments for the organizations under review, as set forth in NSA/CSS Policy 7-3, *Internal Control Program*, 14 February 2012. The 2011 Vulnerability and Process Assessment completed by [redacted] (b)(3)-P.L. 86-36 did not report any concerns applicable to the collection of BR.

(U) This page intentionally left blank.

(U) APPENDIX B

~~(TS//SI//NF)~~ Business Records Systems

(U) This page intentionally left blank.

~~(TS//SI//NF)~~ BUSINESS RECORDS (BR) SYSTEMS

~~(TS//SI//NF)~~ **BR Systems** BR data is stored on Agency networks in [redacted] and off-line using backup tapes. (b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ [redacted] is the Agency's corporate contact chaining database [redacted] Foreign Intelligence Surveillance Act (FISA) BR. [redacted] (b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)
- ~~(TS//SI//NF)~~ [redacted] is the corporate database repository that stores BR FISA transactions. [redacted] provides analysts with detailed BR transaction information that supports the contact chain summaries found in [redacted] replaced the [redacted] Transaction Database in January 2011.
- ~~(TS//SI//NF)~~ [redacted] is the contingency database for [redacted] Because of system limitations, the [redacted] system contains [redacted] During the [redacted] rebuild, analysts were redirected to the [redacted]
- ~~(TS//SI//NF)~~ [redacted] is the system backup that stores an exact (unformatted) copy of the raw BR metadata received from telecommunications providers. (b)(3)-P.L. 86-36
- ~~(TS//SI//NF)~~ **Backup tapes** are maintained [redacted] The raw BR metadata electronically stored in [redacted] is saved [redacted] to tape backup.
- ~~(TS//SI//NF)~~ [redacted] is software that runs on a [redacted] system that contains [redacted] servers. The system currently holds [redacted]

(U) This page intentionally left blank.

(U) APPENDIX C

~~(TS//SI//NF)~~ Agency Foreign Intelligence Surveillance Act Business Records Collection Stakeholders

(U) This page intentionally left blank.

~~(TS//SI//NF)~~ AGENCY FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) BUSINESS RECORDS (BR) COLLECTION STAKEHOLDERS

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ The following organizations are the primary stakeholders for BR FISA collection.

(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ **Program Management Division** manages the relationship with the telecommunication providers
- ~~(TS//SI//NF)~~ is responsible for NSA's repository of bulk metadata collected under the BR FISA metadata collection process. centrally manages the database,

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

maintains Storage system backup and tape backups, and ensures that are provided to for update to

- ~~(TS//SI//NF)~~ develops and implements structured database strategies consistent with the Agency's Enterprise Architecture. manages the database and provides continuous monitoring of BR transactions received through the interface.
- ~~(TS//SI//NF)~~ performs the function of Data Integrity Analyst. develops and modifies parser rules to ensure that only compliant data is ingested into performs daily and weekly tests on the raw call detail records to identify non-compliant data. also completes the weekly BR FISA Compliance Report for the Office of the Director of Compliance.

(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ **Office of the Director of Compliance (ODOC; D4)**, through its Monitoring Assessments and Special Compliance Activities divisions, is responsible for monitoring the Agency's activities for compliance with the terms of the Order. ODOC reviews the requirements of the Order and what NSA reports to the FISC, develops training, identifies end-to-end processes, and liaises with stakeholders. ODOC reviews the Weekly Compliance Report prepared by

(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ **Office of General Counsel – Intelligence Law (D21)** is responsible for completing authorization renewals, filing information with the FISC, interpreting the Order to the NSA workforce, and requesting modifications to the Order when necessary.

- ~~(TS//SI//NF)~~ **BR FISA Lead (ST)** is the Signals Intelligence Directorate representative for the BR FISA program. The BR FISA Lead manages the direction of the program and ensures that the program functions properly. The BR FISA Lead signs the declaration that accompanies the FISA BR application to the FISC.
- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] is responsible for the development of [redacted] —software that runs on a [redacted] system that contains [redacted] servers. [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(3)-P.L. 86-36

(U) APPENDIX D

(U) Full Text of Management Response

(U) This page intentionally left blank.

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

SIGNALS INTELLIGENCE DIRECTORATE memorandum

FROM: S02 16 July 2012

TO: Office of the Inspector General (OIG)

SUBJ: ~~(TS//SI//NF)~~ Signals Intelligence Directorate (SID) Response to the Draft Report on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Collection (ST-12-0003)

(U//~~FOUO~~) SID reviewed the subject draft report in its entirety and agrees with the recommendations. SID's complete response, to include three requests for closure, is attached.

(U) Please contact [redacted] SID IG Liaison, on 963-2014s if you have any questions or concerns.

(b)(3)-P.L. 86-36 [redacted]

Deputy Chief of Staff for
SIGINT Policy and Corporate Issues

Encl: a/s

CLASSIFIED BY: NSA/CSSM 1-52
DATED: 20070108
DECLASSIFY ON: 20370717

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

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

~~(TS//SI//NF)~~ SID Response to the Draft Report on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Collection (ST-12-0003)

(U) SID Recommendations and Planned Corrective Actions

Recommendation 1

~~(TS//SI//NF)~~ *Consolidate and maintain all final BR FISA Program material in a central location accessible to NSA stakeholders.*
(ACTION: BR FISA Program Lead)

(U) Agree
(U) Estimated Completion Date:
~~(TS//SI//NF)~~ **SID Comment:** All final program material will be maintained on the existing SV SharePoint site. While a good portion of the final program data exists on the site today, collection and storage of outstanding documents should be accomplished
(U//~~FOUO~~) POC: 963-0711s

Recommendation 2

~~(TS//SI//NF)~~ *Maintain official meeting notes of quarterly compliance meetings with DoJ NSD.*
(ACTION: BR FISA Program Lead)

(U) Agree with comment
(U) Estimated Completion Date:
~~(TS//SI//NF)~~ **SID Comment:** SID requests that the word "official" be removed. Quarterly compliance meetings create suggested actions; however, these actions do not become *official* until they are presented to and ratified by the Foreign Intelligence Surveillance Court. NSA will maintain meeting documentation on the SharePoint site referenced above.
(U//~~FOUO~~) POC: 963-0711s

Recommendation 3

~~(TS//SI//NF)~~ *Reconcile periodically*
(ACTION:

(U) Agree
(U) Estimated Completion Date: Requesting closure.
~~(TS//SI//NF)~~ **SID Comment:**

~~(TS//SI//NF)~~

(U//~~FOUO~~) 769-4014s; S35309; 769-4T66s

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3(

(b)(3)-P.L.

CLASSIFIED BY: NSA/CSSM 1-52
DATED: 20070108
DECLASSIFY ON: 20370717

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

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

(b)(3)-P.L. 86-36

Recommendation 4

(U//~~FOUO~~) Implement a management review process of the sampling that [redacted] personnel perform.

(ACTION: [redacted]

(U) Agree

(U) Estimated Completion Date: Requesting closure.

(U//~~FOUO~~) SID Comment: [redacted] implemented a management review process to address this recommendation. [redacted] management now reviews [redacted] sampling each month at the team's project review meeting. This procedure (see chart below) is part of a controlled collection of html-formatted files that only team members have access to. SID respectfully requests that this item be considered satisfied and closed.

Monthly Tasks

Task	Directions
Monthly project review with [redacted] management	(U//~~FOUO~~) Management will: 1. Verify that the daily logs are being run by visually inspecting a recent log for each feed in [redacted] 2. Witness the execution of the daily monitoring process [redacted] 3. Review the weekly summary log [redacted] personnel should be prepared to address all data anomalies reported. 4. Review the latest weekly report provided to ODOC.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) POC: [redacted] 963-0245s

Recommendation 5

(U//~~FOUO~~) Implement a process to conduct periodic reviews of the structure code.

(ACTION: [redacted]

(U) Agree

(U) Estimated Completion Date: Requesting closure.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) SID Comment: [redacted] verified with the Advanced Intelligence Research Services (AIRS) that the versions of the standards that [redacted] are valid and remain the most recent versions. [redacted] has implemented a process (see chart below) to review [redacted] the structure code to verify that [redacted] software remains up-to-date. SID respectfully requests that this item be considered satisfied and closed.

Review [redacted] to determine if changes are needed.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] has an information need for the most recent versions of the documents listed below in order to maintain software which can detect the presence of credit card numbers in data. [redacted] has a requirement to check [redacted] for updates for these three standard documents.

(b)(3)-P.L. 86-36

- [redacted]

(U//~~FOUO~~) [redacted] submits a query to AIRS via their web page asking if the three documents have been updated:

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

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

1. Type 'go AIRS' in your browser.
2. Click on "Request Information" located on the lower right side of the page (as of June 2012).
3. Click on "All Source Research"
4. Fill out the request form.
   - In the Classification box select TS//SI//REL TO USA, AUS, CAN, GBR, NZL
   - In the Date/Time Needed pull down box, select "3-5 working days."
   - In the Request box put the following text:
   - (U//~~FOUO~~) Please let me know if the following standards have been updated:
   - [redacted]
   - In the Justification for Research Request box put the following text:
   - ~~(TS//SI//REL TO USA, FVEY)~~ [redacted] has an information need for the most recent versions of the documents listed below in order to maintain software which can detect the presence of credit card numbers in data. PE has a requirement to check [redacted] for updates for these three standard documents.
5. Submit the form and someone from AIRS will contact you. If there is an update to any of these documents, they will get it for you.
6. Update the documents in CVS if necessary.
7. If there is an update to any of these standards, [redacted] must evaluate the document and determine if the change impacts credit card detection [redacted]

(b)(3)-P.L.

(U//~~FOUO~~) POC: [redacted] 963-0245s (b)(3)-P.L. 86-36

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

(b)(3)-P.L. 86-36

From: [redacted] NSA-S022 USA CIV
To: [redacted] NSA-D11 USA CIV
Cc: DL SIDIGLIAISON (ALIAS) S022
Subject: ~~(TS//SI//NF)~~ Questions answered - Signals Intelligence Directorate (SID) Response to the Draft Report on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Collection (ST-12-0003) - Recommendation 2
Date: Friday, July 27, 2012 2:03:25 PM

Classification: ~~TOP SECRET//COMINT//NOFORN~~

[redacted]

(U//~~FOUO~~) Apologies for the delay in getting this to you –

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] reviewed the entire document and provides specific comments in response to the item titled *Reconciling Data from Providers* and *Recommendation 2*. [redacted] supports the OIG's findings in this section and provides the following technical feedback as consideration for the action cited in Recommendation 2. Comments are specific to the individual telecommunications providers.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted]

~~(TS//SI//NF)~~ For each provider, [redacted] will establish a reasonable periodicity for reconciliation that is technically feasible yet meets OIG's recommendation. Additional technical discussions with the providers and developers of follow-on in-house activities will be required for full consideration and implementation [redacted]

(U//~~FOUO~~) POC: [redacted] 769-4058s

(U//~~FOUO~~) [redacted]
SID IG LIAISON
OPS1 2N006 Suite 6245
dl sidigliaison 963-2014
(U//~~FOUO~~)

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.