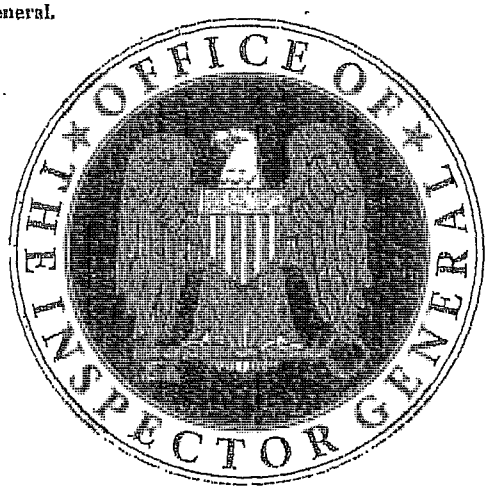
National Security Agency/Central Security Service

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.

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 R. 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)

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

~~(TS//SI//[redacted]//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 from* [Telecommunications Providers] *Relating to* [redacted] *in the United States and Abroad*, 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//[redacted]//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/[redacted]~~/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 regarding [redacted] in the United States. 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.

(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//[redacted]/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//[redacted]/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: Chief,** [redacted] **)**

(U) Management Response

CONCUR. ~~(TS//SI//~~ [redacted] ~~//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 8 September 2006. Testing is currently ongoing.

Status: **OPEN**
Target Completion Date: **8 September 2006**

(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/~~ [redacted] ~~//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:

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]

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//[redacted]/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 two 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: **28 February 2007**

(U) OIG Comment

~~(TS//SI//[redacted]/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//[redacted]//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 two 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: **28 February 2007**

(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/[redacted]/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 [redacted] 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.

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).	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).
	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).	PM, Chief or D/Chief of AAD, Shift Coordinators	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).
	▪ 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);	PM; Chief & D/Chief of AAD, & Shift Coordinators	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).
		AAD Analysts	*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).
	▪ 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).	[redacted] and Technical Support	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).
		OGC	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).
	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	

~~(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
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

PROGRAM MEMORANDUM

PM-031-06 Reissued
29 Aug 2006

To: Office of the Inspector General [redacted]

Cc: Office of [redacted]
Counterterrorism Production Center [redacted]
Chief, SID Oversight and Compliance [redacted]
SSG1 [redacted]

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//[redacted]/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 [redacted] 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.

a. ~~(TS//SI//[redacted]/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 by 8 September 2006. Testing continues at this time.

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~~

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 two 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. (TS//SI//NF) Corrective Action: Acceptable tools and procedures can be developed within six months if the required manpower is allocated. Assuming the Program team's request is granted, this initiative can be completed by 28 February 2007. The corrective action will include:

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.

[redacted]

29 Aug 06

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]
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