

~~TOP SECRET~~

(Security Classification)

ROUTING			
TO:	NAME AND ADDRESS	DATE	INITIALS
1			
2			
3			
4			
ACTION	DIRECT REPLY	PREPARE REPLY	
APPROVAL	DISPATCH	RECOMMENDATION	
COMMENT	FILE	RETURN	
CONCURRENCE	INFORMATION	SIGNATURE	
REMARKS:			
FROM: NAME, ADDRESS, AND PHONE NO.			DATE

CONTROL NO. _____

COPY _____ OF _____

Handle Via

~~COMINT~~ ~~CODEWORD~~

~~CODEWORD~~

Channels

Access to this document will be restricted to those approved for the following specific activities:

~~CODEWORD~~



NATIONAL SECURITY INFORMATION

Unauthorized Disclosure Subject to Criminal Sanctions



~~TOP SECRET~~

(Security Classification)

NSA REPORT TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT
(BR 06-05) (TS//SI//NF)

(TS//SI//NF) The National Security Agency (NSA) submits this report as required by the May 24, 2006 Order of the Foreign Intelligence Surveillance Court (FISC), Docket Number BR 06-05, which authorized NSA to acquire certain tangible things in connection with investigations to protect against international terrorism concerning [REDACTED] pursuant to the Foreign Intelligence Surveillance Act, as amended (the "Act"), 50 U.S.C. § 1861.

BACKGROUND (U)

(TS//SI//NF) On May 24, 2006, the FISC issued an Order authorizing NSA to acquire certain tangible things - "call detail records" maintained by [REDACTED] - in connection with investigations to protect against international terrorism concerning [REDACTED] pursuant to the Act.¹ The Court's Order requires that any application to renew or reinstate the authority shall include a report describing (i) the queries that have been made since this Order was granted; (ii) the manner in which NSA applied the procedures set forth in subparagraph A (which describes the access control and the

¹ (TS//SI//NF) "Call detail records," or "telephony metadata," were defined in NSA's declaration, and similarly in the Court's Order, to include 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, but not to include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

standard for querying the data); and (iii) any proposed changes in the way in which call-detail records would be received [REDACTED]. See Docket Number BR 06-05 at 9(para. 4.I). This report addresses the period between May 24, 2006 and August 2, 2006, a cut-off date that was selected in order to allow for the gathering of data and composition of the report; the next report will address a period beginning with August 3, 2006. Because the cut-off date is prior to the date of the Court's August 8, 2006 Amended Order in this matter, this report does not discuss NSA's activities under that Amended Order. (~~TS//SI//NF~~)

ROLE OF DATA INTEGRITY ANALYSTS (e)

(~~TS//SI//NF~~) As an initial matter, NSA wants to clarify the fact that a small team of analysts who have access to the data acquired pursuant to the Order do not engage in call-chaining analysis for the purpose of discovering terrorist suspects and disseminating information to other appropriate elements of the Government; rather, their function is to support such efforts by continually assuring the quality, accuracy and utility of the information received. Because these analysts access the acquired data before it is archived into the analytic database, and do not conduct the operational analysis that has been detailed for the Court in accordance with the standard provided by the Court, NSA believes it important to highlight with particularity their role in the analytic process.

(~~TS//SI//NF~~) The successful use of the call-detail records acquired under the Order is made possible in part through the efforts of a small team of "data integrity" analysts. This team - currently consisting of four

individuals - has access to -- and does access -- the data acquired under the Order before it is archived into the database used by intelligence analysts to carry out their counter terrorism mission. The data integrity analysts work with the [REDACTED] providing the data to NSA and with the data itself to ensure NSA understands what data it is receiving, how the fields of data are arranged, what is contained in them, how they are used by the [REDACTED], and similar issues concerning the delivery of the data to NSA. These analysts also write software that facilitates the normalization and archiving of the incoming data into the NSA analytic database, review the incoming records for problems and irregularities, and generally ensure the quality of the data archived for operational purposes. These individuals are expert in the data itself, rather than in drawing conclusions about individuals based on the data.

(TS//SI//NF) The data integrity analysts do not query the archived data to perform intelligence analysis, but their role in supporting that analysis is a crucial one.² These data integrity analysts have been trained by NSA management and by the NSA Office of General Counsel in the appropriate handling of the data, the purpose for and conditions under which NSA receives it, and the limitations and conditions on its storage and use. The Government's filings seeking renewal of the Order make specific reference to the unique role of the data integrity analysis team.

² (TS//SI//NF) Indeed, it was through the efforts and attention of the data integrity analysts that the presence of credit card information in a small percentage of the records, discussed below, became known to NSA management.

CALL DETAIL RECORDS ACQUIRED PURSUANT TO THE COURT'S ORDER, AND REPORTABLE ISSUES CONCERNING THEM (S)

a. The Records (U)

~~(TS//SI//NF)~~ Pursuant to the Court's Order, NSA was authorized to acquire call detail records from [REDACTED] companies, and during this reporting period acquired such records from [REDACTED] companies, [REDACTED].³ The call detail records of [REDACTED] companies [REDACTED]

[REDACTED]

~~(TS//SI//NF)~~ In all cases, the records consist of numerous data fields that provide information about telephone calls, but do not contain the content of any calls as defined in 18 U.S.C. 2510(8). The fields of data in the records contain information such as the telephone number of the device initiating the call, the telephone number of the device that was called, the date and duration of the call, the identifiers assigned to the communications trunks that carried the call, whether a call originated or terminated overseas, [REDACTED]

[REDACTED]

³ ~~(TS//SI//NF)~~ [REDACTED] It is referred to throughout this report as [REDACTED]. The [REDACTED] subject to the Court's Order in BK 06-05, [REDACTED] continues to [REDACTED] to effect delivery of its call detail records.

[REDACTED]

(TS//SI//NF) Often, numerous fields within a call detail record contain no information. Some fields contained in a call detail record, such as the field indicating the called number, almost always contain data. Other fields, such as the field indicating [REDACTED] only contain data when the field is relevant to the particular call in question - in this case when the call [REDACTED]

[REDACTED] The number of fields in a record varies depending on which company provided it and which set of the company's records it belongs to; accordingly, the number of fields in a record varies from [REDACTED]

(TS//SI//NF) One field NSA has found particularly useful in making associations among users of telephone numbers is a field that [REDACTED] field and that [REDACTED] field. This field is sometimes blank, but sometimes contains a [REDACTED] indicating that the telephone call was made using [REDACTED]

[REDACTED]

[REDACTED] al

[REDACTED] by

[REDACTED]

NSA submits that [REDACTED]

[REDACTED] do not constitute [REDACTED]

Nevertheless, out of an abundance of caution, the current application specifically seeks authority to obtain and use [REDACTED]

[REDACTED]

b. Reportable Issues During This Period(U)

(e) Before elaborating on its application of the standard used to conduct searches of the archived call detail records, NSA wishes to bring to the Court's attention two issues that arose during the initial period the Order was in effect.

(TS//SI//NF) NSA averred in its Declaration in support of the Government's application for tangible things that the term "call detail records" would not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. The Court's Order adopted similar language to describe the limits of its authorization. Docket Number BR 06-05 at 2 (para. 2).

(TS//SI//NF) A very small percentage of the call detail records did, however, contain a 16-digit credit card number in those cases when the caller selected a credit card as the payment method for the call. In addition, some records contained proper names - in some cases just a first name, and in some a first and a last name - when the calling party sought to place a collect call.

(TS//SI//NF) While NSA OGC advised that it believes that the restrictions contained in the Court's Order were not designed to prevent NSA from receiving the particular information discussed below in the context it was received, the credit card numbers are at least arguably financial information,⁴ and the names are clearly names. NSA

⁴ (TS//SI//NF) Upon notification of the facts surrounding the inclusion of the credit cards numbers as described, the NSA OGC advised that it was not persuaded that the inclusion of the 16-digit string of numbers in these records was unauthorized under the Order's terms. NSA OGC opined that a credit card number, standing alone, does not indicate

describes below the conditions surrounding its receipt of this information, the steps taken to eradicate it, and the current status of the records with respect to such information.

1. Credit card numbers in certain records

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

~~(TS//SI//NF)~~ A very small percentage of the records NSA acquired between May 24 and August 2 - approximately 0.001% - contained credit card numbers in one of the fields. NSA did not make use of this information in any way. Upon recognizing that this information could be considered financial information, NSA management directed that software be written immediately to suppress - or mask - the digits in the archived data whenever a 16-digit string of numbers appeared in the relevant field. This was accomplished on June 19, ensuring that NSA analysts querying the archived data could neither see the credit card information nor make use of it in their analysis.

~~(TS//SI//NF)~~ At the same time, NSA representatives initiated contact with [REDACTED] to request that the [REDACTED] stop sending information in the relevant data field whenever the contents of the field consisted of a 16-

anything about the financial situation, purchasing habits, payment record, or any other such private information concerning a customer or subscriber. NSA OGC believes it is this type of private information about the finances of U.S. persons that the Court sought to protect in its Order, rather than the mechanism used to pay for a particular telephone call. Nonetheless, NSA OGC recognizes there exists a respectable argument that a credit card number is financial information, and also recognizes that such information could be used to derive more private information about an individual; therefore, NSA OGC believes it imperative to bring the issue to the Court's attention. As is set out above, NSA never did any analysis or took any other action with respect to the credit card numbers, and rendered the credit card numbers inaccessible to operational analysts 26 days after the Order was signed.

digit number. On July 10, [REDACTED] stopped providing the 16-digit string [REDACTED]. NSA and [REDACTED] continue to take steps aimed at terminating the delivery to NSA of similar information [REDACTED].⁵ Again, however, the NSA analysts conducting searches of the archived data have not had credit card numbers available to them since June 19, 2006. Moreover, no record exists of any analyst having made any use of the credit card numbers, and no NSA methods would have called upon them to do so.

2. Proper Names in some records (S)

(TS//SI//NF) In addition, a field [REDACTED] [REDACTED] which is normally blank, in a small number of instances contained a proper name. This occurred even less frequently than the 0.001% frequency with which credit card numbers appeared, evidently when the calling party sought to place a collect call. When the field contained a proper name, it was sometimes a first name only, and sometimes both a first and last name.

⁵ (TS//SI//NF) Achieving this without endangering the operation is somewhat complicated. NSA data integrity analysts (discussed above) have written software that helps load the call detail records into the NSA database used to search the archived data. Part of that software's function is to "recognize" a field for what it is, and treat it accordingly in organizing the data for use. NSA cannot simply ask the company to summarily eliminate the field without a likely disruption of its operations, for two reasons: first, as discussed above, with respect to the vast majority of call detail records, the field does not contain credit card information, and does contain useful information that permits the association of previously unassociated individuals; second, because NSA data integrity analysts have written software that moves the information acquired pursuant to the Order into the database in which the archived data is searched, and because that software "recognizes" a particular number of fields and the contents of each with respect to the different types of records, the precipitous elimination of a field would likely disrupt the functioning of the system, treating data from one field as though it were data from another field. As was stated above, however, NSA analysts conducting searches of the archived data do not have access to the credit card information, and have never made use of it.

~~(TS//SI//NF)~~ As was the case with respect to credit card information, when NSA recognized that it was receiving proper names in a small number of records and that this fact was significant under the Order, it took immediate steps along two paths: at the direction of management, software was implemented on June 19 to suppress from view the proper names that appeared in the archived data queried by the analysts, and NSA officials worked with [REDACTED] officials to curtail delivery of such information. On July 9, procedures were implemented that precluded completely the delivery of proper names in the records [REDACTED] provided to NSA. NSA no longer receives proper names from [REDACTED] and the proper names it did receive have been masked from the view of analysts. NSA never received similar information from [REDACTED]

THE STANDARD SET OUT IN THE COURT'S ORDER (U)

~~(S//SI//NF)~~ The standard set out by the Court for the purpose of querying data acquired pursuant to the authorization and referred to for purposes of the required report is as follows:

"[a]ny search or analysis of the data archive shall occur only after a particular known telephone number has been associated with [REDACTED]. More specifically, access to the archived data shall occur only when NSA has identified a known telephone number for which, 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] provided, however, that 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." See Docket Number BR 06-05 at 5 (para 4.A).

NSA ACTIVITIES UNDER THE AUTHORITY GRANTED BY THE COURT'S MAY 24, 2006 ORDER (~~TS//SI//NF~~)

~~(TS//SI//NF)~~ The Court's Order instructed the NSA Office of General Counsel to brief analysts with respect to the authorization granted by the Order, and the limited circumstances in which queries of the archive are permitted, as well as other procedures and restrictions regarding the retrieval, storage and dissemination of the archived data. See BR 06-05 at 6 (para 4.C).

a. OGC Briefings

~~(TS//SI//NF)~~ During this period, NSA's OGC conducted formal briefings at three different sessions, at least one of which was attended by every analyst authorized to query the archived data, as well as each the seven individuals authorized to approve queries of the archived data. These briefings consisted of descriptions of the retrieval, storage and dissemination procedures and restrictions included in the Court's Order, as well as a description of the standard applicable to the processing of information in the archive and legal advice concerning its application. In addition to the scheduled formal briefings, NSA's OGC also provided frequent advice and counsel on these and similar topics throughout the period to analysts applying the standard and to members of management responsible for approving requests to query the archived data.

~~(TS//SI//NF)~~ In addition, as NSA makes clear above and in its application for renewal and accompanying

declaration, a small team of "data integrity" analysts ensure the quality of the call detail records prior to their inclusion in the NSA analytic database. Because they have access to the data, NSA required them to attend one of the above briefings, and each of them has done so.

b. Procedures for Applying the Court Ordered Standard (e)

(TS//SI//NF) When a number is considered as a candidate to be a seed with which to query the archive, one of the designated approval authorities examines whatever supporting documentation is included with the request with an eye towards deciding whether, 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 a particular known telephone number is associated with [REDACTED]

(TS//SI//NF) The application of this "reasonable person" standard is applied using a test similar to the "totality of the circumstances" test used by the courts. The decision as to whether a particular telephone number qualifies as a seed in connection with the Order is informed by a variety of factors that could give rise to a reasonable articulable suspicion. Some of the factors militating in favor of using a particular telephone number as a seed include (but are not limited to):

- telephonic contact between the phone number in question and that of a person reasonably believed

to be a member or agent of [REDACTED]
[REDACTED]

- other direct contact, as revealed through other SIGINT, HUMINT, or other intelligence information, in which a telephone number is conveyed when that contact involves a person reasonably believed to be a member or agent of [REDACTED]
[REDACTED]

- open source information that indicates a telephone number is used by a person who is reasonably believed to be a member or agent of [REDACTED]
[REDACTED]

c. Application of the Standard to Determine Whether a Telephone Number Qualifies as a Seed Number Under the Court's Order ~~(TS//SI//NF)~~

1. Queries Made as a Result of Automated Alerts ~~(e)~~

~~(TS//SI//NF)~~ NSA has compiled through its continuous counter-terrorism analysis, a list of telephone numbers that constitute an "alert list" of telephone numbers used by members of [REDACTED]
[REDACTED].

This alert list serves as a body of telephone numbers employed to query the data, as is described more fully below.

~~(TS//SI//NF)~~ Domestic numbers and foreign numbers are treated differently with respect to the criteria for including them on the alert list. With respect to foreign telephone numbers, NSA receives information indicating a tie to [REDACTED]
[REDACTED].

[REDACTED] from a variety of sources. Principal among these are: reporting by the FBI, CIA or NSA; open source information tying a telephone number to a member of [REDACTED] [REDACTED] known to the Intelligence Community; information from a foreign intelligence service known by the U.S. Intelligence Community to be reliable; and telephony contact between the telephone of a known [REDACTED] and another telephone. Each of the foreign telephone numbers that comes to the attention of NSA as possibly related to [REDACTED] [REDACTED] is evaluated to determine whether the information about it provided to NSA satisfies the reasonable articulable suspicion standard. If so, the foreign telephone number is placed on the alert list; if not, it is not placed on the alert list.

(TS//SI//NF) The process set out above applies also to newly discovered domestic telephone numbers considered for addition to the alert list, with the additional requirement that NSA's Office of General Counsel reviews these numbers and affirms that the telephone number is not the focus of the analysis based solely on activities that are protected by the First Amendment. There are, however, two categories of domestic telephone numbers that were added to the NSA alert list prior to the date the Order took effect, and the basis for their addition is slightly different.

(TS//SI//NF) The first category consists of 177 domestic numbers that are currently the subject of FISC authorized electronic surveillance based on the FISC's finding of probable cause to believe that they are used by [REDACTED]

[REDACTED] Since these numbers were already reviewed and authorized by the Court for electronic surveillance

purposes, they were deemed approved for meta data querying without the approval of an NSA official.

(TS//SI//NF) The second category consists of 199 domestic numbers each of which was added to the NSA alert list after coming to NSA's attention because of its direct contact with a known foreign [REDACTED] seed number, and subsequent NSA analysis produced a sufficient level of suspicion that NSA generated an intelligence report about the telephone number to the FBI and the CIA. NSA's OGC has not reviewed the domestic numbers on the alert list that predate the effective date of the Order, as there was no requirement to do so with respect to NSA's activities prior to the effective date of the Order. However, it is important to note that these numbers are not used as seeds. Rather, with respect to this category of telephone numbers, in the event of a new contact, the foreign [REDACTED] telephone number that originally sparked NSA's interest in the domestic number would be the seed. Accordingly when conducting contact chaining as a result of an alert list "hit", NSA limits the number of hops it undertakes from the domestic number to two.⁶

⁶ (TS//SI//NF) Note that NSA could - if it chose to - conduct queries against the original foreign seed number every day or even multiple times a day, so long as it continued to have a reasonable articulable suspicion that the foreign number was associated with [REDACTED]. If NSA did so, every day NSA would see the contact between the foreign seed and the domestic number that is on the alert list, as well as all new foreign and domestic contacts. The inclusion of these domestic numbers on the alert list is merely a quicker and more efficient way of achieving the same result without looking at all the domestic to domestic contacts that would be revealed if this were done. Stated another way, the system is designed to bring to the attention of NSA the fact that a telephone number about which NSA has suspicion has had a new contact with a number overseas, but all of this is premised on the existence of a foreign seed number that originally surfaced the domestic number in question. Each seed number NSA uses, whether derived from information that was on the alert list prior to the effective date of the Order or after, meets the standard set out in the Order.

(TS//SI//NF) However, in order to avoid any appearance of circumventing the procedures, NSA will change its software to build the chains from the original foreign number and remove the 199 domestic numbers described above from the alert list. While the software is being developed, which will take approximately 45 days, NSA will continue to run the domestic numbers on the alert list as described.

(TS//SI//NF) As of the last day of the reporting period addressed herein, NSA had included a total of 3980 telephone numbers on the alert list, which includes foreign numbers and domestic numbers, after concluding that each of the foreign telephone numbers satisfied the standard set forth in the Court's May 24, 2006, and each of the domestic telephone numbers was either a FISC approved number or in direct contact with a foreign seed that met those criteria.

(TS//SI//NF) To summarize the alert system: every day new contacts are automatically revealed with the 3980 telephone numbers contained on the alert list described above, which themselves are present on the alert list either because they satisfied the reasonable articulable suspicion standard, or because they are domestic numbers that were either a FISC approved number or in direct contact with a number that did so. These automated queries identify any new telephone contacts between the numbers on the alert list and any other number, except that domestic numbers do not alert on domestic-to-domestic contacts.

(TS//SI//NF) During this reporting period, a combination of the alert system and queries resulting from leads described below in paragraph two led to analysis that resulted in the discovery of 138 new numbers that were

tipped as leads to the FBI and the CIA as suspicious telephone numbers.

2. Queries Resulting From Leads Other Than the Automated Alert System (e)

~~(TS//SI//NF)~~ The other type of query that NSA analysts run are those based upon seed telephone numbers of which NSA became aware through means other than the automated alerting system. These are telephone numbers that NSA has learned about through other sources, such as communications it intercepted through other authorized surveillance activities or information provided to NSA by other elements of the U.S. Intelligence Community. A Shift Coordinator approves all proposed queries of the archived data prior to their taking place, applying the standard set out in the Court's Order. If the Shift Coordinator determines an address is known or believed to be used by a U.S. person, the query is sent to the NSA OGC. Otherwise, the Shift Coordinator authorized (or disallowed) the use of the address as a seed address based on the criteria contained in the Court's Order.⁷

~~(TS//SI//NF)~~ During this reporting period, in response to lead information primarily from CIA, FBI and internal to NSA, NSA determined that 153 new telephone numbers satisfied the reasonable articulable suspicion and designated them as seeds; NSA then conducted analyses of

⁷ ~~(TS//SI//NF)~~ Analysts are well-versed in the rules governing queries of the data obtained as a result of the Court's Order. Informal discussion among the counter-terrorism analysts frequently precedes the submission of a formal request for authorization to conduct contact chaining [REDACTED]. Accordingly, a subset of the potential seed numbers is discussed among the analysts and rejected as candidates at the analyst level. In these cases, no formal request to use the number as a seed number is ever made.

the acquired data as described in the Court's Order. Also during this reporting period, NSA declined to process 46 telephone numbers it had received primarily from CIA, FBI and internal to NSA, concluding the standard had not been satisfied. Of the 199 numbers proposed, 108 numbers were submitted to the NSA OGC because they were believed to be used by U.S. persons. NSA's OGC approved 99 as seeds, and declined to approve 9.

c. Example of Application of the Standard and Resulting Report (e)

(~~TS//SI//NF~~) Analysis of information obtained pursuant to the Court's authorization in the above-captioned matter resulted in querying the archived data using a known telephone number that satisfied the standard set out in the Court's Order, and a subsequent report identifying multiple foreign and two US-based possible terrorist-related leads. This new information was a direct result of meta data analysis of telephone numbers used by [REDACTED]

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

[REDACTED] from intelligence information gathered in the area, immediately after the raid. An NSA Shift Coordinator determined that, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there existed facts giving rise to a reasonable articulable suspicion

that this phone number was associated with [REDACTED]. The Shift Coordinator approved querying the archived data using this number as a seed, and NSA learned from several SIGINT sources that prior to [REDACTED], his [REDACTED] number had been in contact with multiple numbers in [REDACTED] which were subsequently in contact, [REDACTED] with numbers in the United States, Australia, Canada and the United Kingdom. NSA reported these foreign and domestic [REDACTED] contacts obtained through analysis of data authorized by this Court through BR-06-05 to FBI, CIA, and the NCTC.

PROPOSED CHANGES IN THE WAY CALL DETAIL RECORDS WILL BE RECEIVED BY NSA ~~(TS//SI//NF)~~

(TS//SI//NF) NSA anticipates that, if the Order is renewed, it will [REDACTED]

TOP SECRET//COMINT//NOFORN//MR

█ Aside from this, NSA anticipates no changes and proposes no changes to the way it receives the call detail records.

17 August 2006
Date

█
█
SID Program Manager for █
Projects █
National Security Agency