UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, DC

2009 AUG 17 PM 4:15
CLERK OF COURT

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 09-09

REPORT OF THE UNITED STATES (U)

The United States of America, by and through the undersigned Department of Justice attorneys, respectfully submits this report and supporting documents in response to the Court's Primary Order dated July 9, 2009, and similar predecessor Orders. ~~(TS//SI//NF)~~

The National Security Agency (NSA) has completed an end-to-end review of its handling of call detail records produced pursuant to the Orders. The review began earlier this year after the discovery that NSA had not handled the records in the manner authorized by the Court, and it

Classified by: David S. Kris, Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: 17 August 2034

has identified several serious instances of non-compliance. Although NSA successfully implemented many of the Orders' requirements, in several instances it treated records collected pursuant to the Orders in the manner it treats information collected under other NSA collections, without the necessary regard for the unique nature and requirements of this Court-ordered collection. ~~(TS//SI//NF)~~

NSA has since remedied these instances of non-compliance, primarily through a series of technological fixes and improved training. It has implemented the new oversight procedures set forth in the Orders and self-imposed by NSA, and proposes to implement additional procedures in the event that the Court authorizes NSA to query the records using telephone identifiers that NSA has determined meet the reasonable, articulable suspicion standard. This report, the supporting declarations of the Directors of NSA (Exhibits A and B) and Federal Bureau of Investigation (FBI) (Exhibit C), and the attached NSA report (Exhibit D) (the "End-to-End Report") aim to provide the Court with assurance that NSA has addressed and corrected the instances of non-compliance and is taking the additional steps described herein to monitor and ensure compliance with the Court's Orders going forward. The documents describe the results of NSA's end-to-end review, the remedies for instances of non-compliance, the testing of technological remedies, and additional procedures employed and proposed to be employed. They also explain how valuable the collection and analysis of the records is to the national security. Based on these findings and actions, the Government anticipates that it will request in the Application seeking renewal of docket number BR 09-09 authority that NSA, including certain NSA analysts who obtain appropriate approval, be permitted to resume non-automated querying of the call detail records using selectors approved by NSA. ~~(TS//SI//NF)~~

I. BACKGROUND (U)

In docket number BR 06-05 and each subsequent authorization, including docket number BR 09-09, the Government sought, and the Court authorized NSA, pursuant to the Foreign Intelligence Surveillance Act's (FISA) tangible things provision, 50 U.S.C. § 1861 et seq., to collect in bulk and on an ongoing basis certain call detail records or "telephony metadata."[1] The Government will refer herein to call detail records collected pursuant to the Court's authorizations in this matter as "BR metadata." NSA analyzes the BR metadata, using contact chaining [redacted] to find and identify known and unknown members or agents of [redacted] ~~(TS//SI//NF)~~

The Orders direct the Government to treat the BR metadata in accordance with minimization procedures adopted by the Attorney General. Among these minimization procedures in docket number BR 06-05 was the following:

> Any 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

---

[1] "Call detail records," or "telephony metadata," include comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) numbers, International Mobile station Equipment Identity (IMEI) numbers, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. A "trunk" is a communication line between two switching systems. *Newton's Telecom Dictionary* 951 (24th ed. 2008). Metadata does 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. ~~(TS)~~

[2] The Primary Order in docket number BR 06-05 authorized NSA to query the BR metadata using telephone identifiers associated with [redacted]. Later authorizations expanded the telephone identifiers that NSA could use for queries to those associated with [redacted] see docket number BR 06-05 (motion to amend granted in August 2006), and, later, the [redacted], see docket number BR 07-10 (motion to amend granted in June 2007). The Court's authorization in docket number BR 09-09 approved querying related to [redacted]. See Primary Order, docket number BR 09-09, at 5-7. ~~(TS//SI//NF)~~

> 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.

Order, docket number BR 06-05, at 5 (emphasis added). For purposes of querying the BR metadata, all subsequent Orders in this matter required the Government to comply with the same standard of reasonable, articulable suspicion.[3] See, e.g., Primary Order, docket number BR 09-09, at 5-7. As authorized by the Orders in docket numbers BR 06-05 through BR 08-13, NSA determined which telephone identifiers met the RAS standard and, therefore, could be used to query the BR metadata. In addition, the Orders contained minimization procedures that governed other aspects of the use, retention, and dissemination of BR metadata. ~~(TS//SI//NF)~~

Beginning in mid-January 2009, the Government notified the Court of instances of non-compliance with the Court-ordered minimization procedures in this matter. The first written notice, filed on January 15, 2009, reported that, through an automated "alert list" process, NSA had conducted automated queries of the BR metadata using non-RAS-approved telephone identifiers. NSA shut down this automated alert list process entirely on January 24, 2009, and the process remains shut down. ~~(TS//SI//NF)~~

By Order dated January 28, 2009, the Court ordered the Government to file a written brief concerning the alert list process. In response to this Order, the Director of NSA ordered that NSA complete an end-to-end system engineering and process review of its handling of the BR metadata. On February 26, 2009, after it filed its brief, the Government provided written notice to the Court of additional non-compliance incidents. These incidents were identified as a

[3] In this memorandum the Government will refer to this standard as the "RAS standard" and telephone identifiers that satisfy the standard as "RAS-approved." ~~(S)~~

result of the end-to-end review and, like the alert list process, also concerned queries of the BR metadata using telephone identifiers that were not RAS-approved at the time of the queries. ~~(TS//SI//NF)~~

On March 2, 2009, the Court issued an Order that required NSA to seek Court approval to query the BR metadata on a case-by-case basis, except where necessary to protect against an imminent threat to human life. The Court further ordered that:

> Upon completion of the government's end-to-end system engineering and process reviews, the government shall file a report with the Court, that shall, at a minimum, include:
>
> a. an affidavit by the Director of the FBI, and affidavits by any other official responsible for national security that the government deems appropriate, describing the value of the BR metadata to the national security of the United States and certifying that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, and that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment;
>
> b. a description of the results of the NSA's end-to-end system engineering and process reviews, including any additional instances of non-compliance identified therefrom;
>
> c. a full discussion of the steps taken to remedy any additional non-compliance as well as the incidents described herein, and an affidavit attesting that any technological remedies have been tested and demonstrated to be successful; and
>
> d. the minimization and oversight procedures the government proposes to employ should the Court decide to authorize the government's resumption of regular access to the BR metadata.

The Court's Primary Orders in docket numbers BR 09-01, BR 09-06, and BR 09-09 contain these same reporting requirements. ~~(TS//SI//NF)~~

Subsequent Orders have required that the Government's report include additional information regarding certain instances of non-compliance and/or other matters. These further reporting requirements are summarized in the Primary Order in docket number BR 09-09:

- a full explanation of why the government has permitted dissemination outside NSA of U.S. person information in violation of the Court's Orders in this matter;
- a full explanation of the extent to which NSA has acquired call detail records of foreign-to-foreign communications from [redacted] pursuant to orders of the FISC, and whether the NSA's storage, handling, and dissemination of information in those records, or derived therefrom, complied with the Court's orders; and
- either (i) a certification that any overproduced information, as described in footnote 11 of the government's application [i.e., credit card information], has been destroyed, and that any such information acquired pursuant to this Order is being destroyed upon recognition; or (ii) a full explanation as to why it is not possible or otherwise feasible to destroy such information.

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

II. VALUE TO THE NATIONAL SECURITY (U)

Analysis of the BR metadata addresses a critical, threshold issue for the Government's efforts to detect and prevent terrorist acts affecting the national security of the United States: identifying the terrorists and their associates. Ex. B at 4-5, 15; Ex. C at 4, 19. The [redacted] analysis of the BR metadata – contact chaining [redacted] – share this purpose. Contact chaining analysis identifies which telephone identifiers have been in contact with a telephone identifier reasonably suspected to be associated with a terrorist. Ex. B at 5-7. [redacted] ~~(TS//SI//NF)~~

Because the BR metadata is a collection of historical telephony metadata, NSA analysts are able to look back in time to identify not only recent contacts and patterns, but those in the

past. Id. at 6. By the time the Government associates a telephone identifier with a terrorist, the terrorist who was using it may have moved on to a new one. The historical nature of the BR metadata, however, allows for the identification of past contacts [redacted]. It, therefore, increases the likelihood of identifying previously unknown associates and telephone identifiers. Id. at 6. ~~(TS//SI//NF)~~

The BR metadata provides information on the activities of terrorists and their associates that is not available from other sources of telephony metadata. Collections pursuant to Title I of FISA, for example, do not provide NSA with information sufficient to perform multi-tiered contact chaining [redacted]. Id. at 8. NSA's signals intelligence (SIGINT) collection, because it focuses strictly on the foreign end of communications, provides only limited information to identify possible terrorist connections emanating from within the United States. Id. For telephone calls, signaling information includes the number being called (which is necessary to complete the call) and often does not include the number from which the call is made. Id. at 8-9. Calls originating inside the United States and collected overseas, therefore, often do not identify the caller's telephone number. Id. Without this information, NSA analysts cannot identify U.S. telephone numbers or, more generally, even determine that calls originated inside the United States. Id. ~~(TS//SI//NF)~~

The BR metadata helps fill these foreign intelligence gaps. Unlike information NSA acquires during its traditional SIGINT operations outside the United States, the BR metadata identifies the telephone identifiers of the person placing a telephone call from within the United States. Id. at 9. It also identifies the U.S. telephone identifiers of persons receiving a call from a foreign terrorist. NSA thus is able to provide the FBI with information about contacts between a

U.S. telephone identifier and a foreign terrorist, thereby alerting it to possible terrorist-related activity within the United States. Id. at 9-10. ~~(TS//SI//NF)~~

According to NSA, not having this information can have grave consequences. As an illustration, prior to the September 11, 2001, attacks, NSA intercepted and transcribed seven calls made by hijacker Khalid al-Mihdhar, then living in San Diego, California, to a telephone identifier associated with an al Qaeda safe house in Yemen. Id. NSA intercepted these calls through its overseas SIGINT collection and, as noted above for telephone calls originating within the United States, the calling party identifier was not included in the signaling information. Id. Because they lacked the U.S. telephone identifier and had nothing in the content of the calls to suggest that al-Mihdhar was inside the United States, NSA analysts mistakenly concluded that al-Mihdhar remained overseas when, in fact, he was in San Diego. Id. The BR metadata, by contrast, would have included the missing information and might have permitted NSA analysts to place al-Mihdhar within the United States prior to the attacks and tip that information to the FBI.[4] Id. ~~(TS//SI//NF)~~

NSA acts on and otherwise makes use of the results of its BR metadata queries. Id. at 3. Where appropriate, it provides those results to other U.S. Government and foreign government agencies. From May 2006 (when the Court issued the first Orders in this matter) through May 2009, NSA disseminated 277 reports containing approximately 2,900 telephone identifiers that NSA had identified through its analysis of the BR metadata. Id. at 12. ~~(TS//SI//NF)~~

The tips or leads the FBI receives are among the most important because they can act as an early warning of possible domestic terrorist activity. Ex. C at 6-7. As noted above, the BR

[4] The 9/11 Commission Report alluded to the failure to share information regarding a facility associated with an al Qaeda safehouse in Yemen and contact with one of the 9/11 hijackers (al Mihdhar) in San Diego, California, as an important reason the Intelligence Community did not detect al Qaeda's planning for the 9/11 attack. See "The 9/11 Commission Report," at 269-272. (U)

metadata is unique in that it can provide more complete information about domestic telephone identifiers in contact with terrorist associates. The earlier FBI obtains information about a threat—in this case, information about a domestic contact—the more likely it will be able to protect against the threat. Id. at 6. Without BR metadata tips, the FBI might never learn about domestic contacts; with these tips, it learns about them promptly. Id. ~~(TS//SI//NF)~~

The FBI has opened predicated international terrorism investigations based, at least in part, on BR metadata tips, including twenty-seven full investigations between May 2006 and the end of 2008. Id. at 7-9. In those cases, BR metadata provided predication for opening the investigation.[5] Id. at 7. Examples are set forth in the accompanying Declaration of the FBI Director. Id. at 9-19. In other cases, BR metadata provided additional information regarding an existing investigation and advanced that investigation. Id. at 5-6. In any such case, the BR metadata was a valuable source of foreign intelligence for the FBI, assisting it in uncovering the operations of [redacted] and in thwarting terrorist activities targeting the United States, its citizens, and its interests abroad.[6] Id. at 19. ~~(TS//SI//NF)~~

III. RESULTS OF THE END-TO-END REVIEW (U)

The results of the NSA's end-to-end review are discussed in detail in the Director of NSA's Declaration (Exhibit A) and the End-to-End Report (Exhibit D). Generally, the end-to-end review focused on two major components of implementation of the BR FISA Orders—system-level technical engineering and execution within the analytical framework. The end-to-

[5] In these twenty-seven full investigations opened based on BR metadata tips, the FBI has issued forty-six intelligence information reports to U.S. government agencies and thirty-one intelligence information reports to foreign government partners. Ex. C at 9. ~~(TS//SI//NF)~~

[6] Based on the value of the BR metadata, the FBI Director has certified that the BR metadata is relevant to authorized investigations (other than threat assessments) to obtain foreign intelligence information to protect against international terrorism. See Ex. C at 19. ~~(TS//SI//NF)~~

end review revealed that there was no single cause of the identified instances of non-compliance and that there were a number of successful oversight, management, and technology processes that operated appropriately. Nonetheless, the end-to-end review uncovered additional instances of non-compliance, all of which were brought to the Court's attention shortly after their discovery during the end-to-end review.[7] The NSA concluded that these instances of non-compliance stemmed from or were exacerbated by a primary focus on analyst use of the data, the complexity of the overall BR FISA system, and a lack of shared understanding among the key stakeholders as to the full scope of the BR FISA system and the implementation of the BR FISA Orders. Each specific instance of non-compliance identified as part of the end-to-end review is briefly discussed below. The remedies for the instances of non-compliance are discussed in the following section. ~~(TS//SI//NF)~~

A. Domestic Identifiers Designated as RAS-Approved Without Review by NSA OGC ~~(TS)~~

The end-to-end review revealed that historically a significant number of domestic identifiers were added to the Station Table as RAS-approved without first undergoing the required review by NSA OGC. This happened in two distinct ways. First, identifiers reported to the Intelligence Community as having a connection with one of the Court-approved terrorist organizations before and after the BR FISA Orders were, until December 15, 2008, added to the Station Table as RAS-approved without NSA OGC review.[8] Second, NSA discovered that

---

[7] As a result of the end-to-end review, NSA also discovered several areas that presented a potential for non-compliance or a vulnerability in management and/or oversight controls. While these areas were not deemed compliance matters and therefore are not discussed in detail herein, the issues and the steps NSA has taken to address them are discussed in the End-to-End Report in sections II.B.1, II.B.4, and II.B.5. ~~(TS)~~

[8] This matter was identified as a potential instance of non-compliance on page 4 of Exhibit C to the Application in docket number BR 09-01 filed on March 4, 2009, and is discussed in section of II.A.4 of the End-to-End Report and on page 12 of Exhibit A. ~~(S)~~

historically errors were made when implementing the BR FISA Orders and consequently some domestic identifiers were initially RAS-approved without the required review by NSA OGC.[9]

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

B. Data Integrity Analysts' Identification and Use of Non-User Specific Identifiers ~~(S)~~

NSA discovered during the end-to-end review that Data Integrity Analysts were, as part of their authorized access to the BR metadata, identifying identifiers not associated with specific users [redacted] and sharing those identifiers with analysts through out the NSA not authorized to access the BR metadata.[10]

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

C. Use of Non-RAS-Approved Correlated Identifiers to Query the BR Metadata ~~(TS//SI//NF)~~

The end-to-end review revealed that management practices and NSA tools permitted analysts to query the BR metadata using a non-RAS-approved identifier if that identifier was correlated to a RAS-approved identifier.[11] [redacted] While historically NSA tools permitted queries of non-RAS-approved identifiers based on [redacted]

[9] This matter was the subject of a preliminary notice of compliance incident filed on June 29, 2009, and is discussed in section of II.B.7 of the End-to-End Report and on pages 12-13 of Exhibit A. ~~(S)~~

[10] This matter was the subject of a preliminary notice of compliance incident filed on May 8, 2009, and is discussed in section of II.B.2 of the End-to-End Report and on pages 18-20 of Exhibit A. ~~(S)~~

[11] This matter was the subject of a preliminary notice of compliance incident filed on June 15, 2009, and is discussed in section of II.B.3 of the End-to-End Report and on pages 13-15 of Exhibit A. ~~(S)~~

[redacted]

D. Improper Dissemination of the Results of BR FISA Queries ~~(TS//SI//NF)~~

As a result of the end-to-end review, it was revealed that NSA's historic, general practice as to the dissemination of U.S. person identifying information derived from BR FISA information was to apply United States Signals Intelligence Directive 18 (USSID 18) and not the more restrictive dissemination provisions of the Court's Orders.[12] In addition, NSA also uncovered two specific instances of non-compliance concerning the dissemination of BR FISA query results. First, NSA discovered that unminimized query results were available to Central Intelligence Agency (CIA), FBI, and National Counterterrorism Center (NCTC) analysts via an NSA database.[13] Second, NSA discovered that on one occasion unminimized U.S. person identifying information was improperly [redacted].[14] ~~(TS//SI//NF)~~

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

[redacted] is the software tool interface used by analysts to manually query the BR metadata chain summaries. In connection with the end-to-end review, NSA developed a new version of [redacted] - that limits the number of hops permitted

[12] This practice was the subject of a preliminary notice of potential compliance incident filed on June 26, 2009, and specifically mentioned in the Court's Primary Order in docket number BR 09-09. This practice is mentioned in section II.B.9 of the End-to-End Report and discussed more fully on pages 36-38 of Exhibit A. ~~(S)~~

[13] This matter was the subject of a preliminary notice of compliance incident filed on June 16, 2009, and is discussed in section of II.B.8 of the End-to-End Report. A fuller explanation of this practice is set forth at pages 29-36 of Exhibit A. ~~(S)~~

[14] This matter was the subject of a preliminary notice of compliance incident filed on June 29, 2009, and is discussed in section of II.B.9 of the End-to-End Report. ~~(S)~~

from a RAS-approved telephone identifier to three, in accordance with the Court's Orders. During testing of the beta version of [redacted], NSA determined that, despite the hop restriction, a feature called [redacted] could be invoked to provide an analyst with the number of unique contacts for a third-hop identifier, a type of information that would otherwise only be revealed by a fourth hop.[15] Prior versions of [redacted] also included the [redacted] feature. ~~(TS//SI//NF)~~

IV. STEPS TAKEN TO REMEDY INSTANCES OF NON-COMPLIANCE (U)

In addition to those instances of non-compliance noted above, Exhibit A and the End-to-End Report address three instances of noncompliance noted in the Court's March 2 Order—the Telephony Activity Detection Process,[16] [redacted][17] and certain inappropriate queries by NSA analysts.[18] All of these instances of non-compliance have been remedied, and the NSA Director has attested as to the testing and functionality of the technological remedies employed by NSA. Ex. A. at 28. For purposes of discussing the remedies implemented by NSA it is helpful to divide the instances of noncompliance into two broad categories: (1) unauthorized queries via automated processes and tools; and (2) operator errors within the BR FISA analytic framework.[19] ~~(TS//SI//NF)~~

---

[15] This matter was the subject of a preliminary notice of compliance incident filed on August 4, 2009, and is discussed on pages 15-17 of Exhibit A. ~~(S)~~

[16] This issue is discussed in section of II.A.1 of the End-to-End Report and on pages 5-7 of Exhibit A. ~~(S)~~

[17] This issue is discussed in section of II.A.2 of the End-to-End Report and on pages 7-9 of Exhibit A. ~~(S)~~

[18] This issue is discussed in section of II.A.3 of the End-to-End Report and on page 9 of Exhibit A. ~~(S)~~

[19] The NSA's identification and use of non-user specific identifiers is not addressed below, as that formerly non-compliant practice was specifically authorized by the Court in docket number BR 09-09. See Primary Order, docket number BR 09-09, at 12. ~~(TS)~~

A. Unauthorized Queries Via Automated Processes and Tools ~~(U//FOUO)~~

NSA has remedied the Telephony Activity Detection Process and [redacted] incidents by eliminating their ability to access the BR metadata. Ex. A. at 6-8. Specifically, NSA shut down the flow of incoming BR metadata into the Telephony Activity Detection Process on January 24, 2009. Id. at 6. Accordingly, the Telephony Activity Detection Process could no longer query the incoming BR metadata with the non-RAS-approved identifiers on the alert list. On February 20, 2009, NSA prevented the Telephony Activity Detection Process, [redacted] or any other automated processes and tools from accessing the BR metadata in its [redacted] database by removing all previously used Public Key Structure (PKI) system-level certificates that gave processes and tools access to the BR metadata.[20] Id. at 8-9. By removing these PKI system-level certificates NSA revoked all automated processes and tools' access to the BR metadata in [redacted] and, therefore, rendered the automated query processes and tools inoperable. Id. The end-to-end review concluded that apart from the Telephony Activity Detection Process's querying of incoming BR metadata, no other automated processes and tools queried BR metadata outside of [redacted] Accordingly, the removal of the PKI system-level certificates ensures that no automated processes or tools are now permitted to query the BR metadata. ~~(TS//SI//NF)~~

The Emphatic Access Restriction (EAR), discussed below, provides further protection against automated processes and tools from querying the BR metadata inappropriately. Specifically, even if [redacted] or some other tool were permitted to access the BR metadata, EAR would prevent it from doing so with anything but a RAS-approved identifier. EAR will continue to serve this function even if the Court grants NSA's request to resume querying based on its own RAS-approval authority. See id. at 28-29. ~~(TS//SI//NF)~~

[20] A PKI system-level certificate is essentially a "ticket" used by the system to recognize and authenticate that the automated capability has the authority to access the database. See Ex. A at 8. ~~(TS//SI//NF)~~

B. Operator Errors with the BR FISA Analytic Framework ~~(TS)~~

Several instances of non-compliance resulted from analysts' actions that were inconsistent with the Court's Orders rather than the functioning of a specific technological process or tool. Although some human error is inevitable in any activity, NSA has addressed each of the identified areas prone to human error with a combination of improved oversight and training, regular reports to the Court, and technological remedies. ~~(TS)~~

1. Queries with Non-RAS-Approved Identifiers ~~(S)~~

As noted in the Court's March 2 Order and uncovered during the end-to-end review, analysts used non-RAS-approved identifiers to query the BR metadata. See III.C. supra; Ex. D at II.A.3. NSA eliminated the potential for this type of analyst error from being repeated by implementation of the EAR on February 20, 2009. See Ex. A at 9, 15. ~~(TS//SI//NF)~~

The EAR is a software restrictive measure that prohibits queries to the BR metadata in [redacted] using non-RAS-approved seeds. Before a given query to the BR metadata is executed, the EAR in effect checks the RAS status of the seed for the query against the Station Table. If the seed for a given query is RAS-approved, the EAR permits the query to be run. If the seed for a given query is not RAS-approved, the EAR will not permit the query to be executed.[21] In this way, NSA has provided a technological remedy to the potential for analysts entering non-RAS-approved identifiers as query seeds, and this remedy will continue to apply should the Court permit NSA to resume non-automated querying of the BR metadata. Ex. A at 9-10. ~~(TS//SI//NF)~~

---

[21] The EAR does not offer the same protection to the BR metadata outside of [redacted] in the [redacted] NSA's audit of queries to the [redacted] revealed that no inappropriate queries were run by analysts against the BR metadata contained in it. In the future NSA intends to migrate the functionality of the [redacted] into [redacted] or its successor, to bring all BR metadata under the protection of the EAR. Ex. A at 9 n.5; Ex. D. at 9, 23. ~~(TS)~~

2. Queries More Than Three Hops From RAS-Approved Identifier ~~(S)~~

As noted above, the beta version of [redacted] and prior versions contained the [redacted] feature that gave analysts contacts information that normally is available only on an unauthorized fourth hop from a RAS-approved identifier. NSA corrected [redacted] to disable the [redacted] feature for last-hop identifiers. As of July 31, 2009, analysts can access the BR metadata contact chain summary repository only through use of [redacted]. All prior versions of [redacted] have been locked out from access to the BR metadata contact chain summary repository. Ex. A at 16-17. ~~(TS//SI//NF)~~

3. Improper Designation of Identifiers as RAS-Approved ~~(S)~~

As uncovered during the end-to-end review, historically NSA had included on the Station Table as RAS-approved identifiers reasonably believed to be used by U.S. persons without those identifiers being reviewed by NSA OGC. See III.A. supra. The first step to remedying this non-compliance was to change the identifiers that should have been reviewed by NSA OGC from "RAS-approved" to "not-RAS-approved." NSA did this for the identifiers designated as RAS-approved based on being reported to the Intelligence Community in early February 2009. Ex. A. at 12. NSA reports that the few identifiers improperly RAS-approved in 2006 were all identified and disapproved or properly approved in 2006 shortly after they were identified. Id. at 13. Continued training and oversight mechanisms employed by NSA are designed to ensure that these incidents will not be repeated. ~~(TS//SI//NF)~~

4. Improper Disseminations of U.S. Person Information ~~(S)~~

As uncovered during the end-to-end review, NSA disseminated BR metadata-derived U.S. person information in a manner not consistent with the Court's Orders. See III.D. supra. The mechanism that resulted in the inappropriate dissemination [redacted] was shut down in

advance of the end-to-end review, and, therefore, required no remediation. Moreover, NSA confirmed that [redacted] purged the inappropriately disseminated information from its systems and did not further disseminate it before doing so. Ex. D at 18. NSA disabled external access to the database that was the other mechanism for inappropriate disseminations on June 12, 2009. Ex. A at 33. NSA's review concluded that approximately one-third of the 250 analysts with permission to access the database between August 2005 and January 2009 actually accessed it. Id. at 34. NSA further determined that approximately forty-seven analysts queried the database in the course of their counterterrorism responsibilities and accessed directories containing the results of BR metadata queries, including un-minimized U.S. person-related information. Id. Finally, a review of NSA reports containing BR metadata with U.S. person identities indicated a significant number of dissemination were approved by an official permitted to approve such determinations pursuant to USSID 18, but not the Court's Orders, and without the appropriate determination required by the Court's Orders. Id. at 38-39.[22] ~~(TS//SI//NF)~~

As noted in section VI below, additional training and oversight, as well as the weekly reports to the Court on disseminations, should prevent similar instances of noncompliance.[23] Moreover, as noted in Exhibit A and the End-to-End Report, these and other non-compliant dissemination practices were the product of an incomplete understanding of the dissemination

[22] In docket number BR 09-09, the Court approved additional individuals to approve disseminations to include the Chief, Information Sharing Services, the Senior Operations Officer, the Signals Intelligence Directorate (SID) Director, the Deputy Director of NSA, and the Director of NSA. ~~(TS//SI//NF)~~

[23] In addition to the above practices, NSA's litigation support team conducts prudential searches in response to requests from Department of Justice or Department of Defense personnel in connection with criminal or detainee proceedings. The team does not perform queries of the BR metadata. See Ex. A at 36 n.19. The Government respectfully submits that NSA's sharing of U.S. person identifying information in this manner does not require a dissemination determination and need not be accounted for in NSA's weekly dissemination report. ~~(TS//SI//NF)~~

requirements set forth in the Court's Order, and as a result of the end-to-end review NSA personnel are now well aware of the Court-ordered dissemination requirements. ~~(TS//SI//NF)~~

V. OTHER MATTERS (U)

A. Storage, Handling and Dissemination of Foreign-to-Foreign Records ~~(TS)~~

NSA has acquired records of foreign-to-foreign communications from [redacted] With the possible exception of certain foreign-to-foreign records produced by [redacted] NSA has stored, handled and disseminated foreign-to-foreign records produced pursuant to the Orders in accordance with the terms of the Orders. See Ex. A at 39-44 [redacted] 44-46 [redacted], and 46-47 [redacted] ~~(TS//SI//NF)~~

[redacted]

[24] [redacted]

[redacted]

NSA advised that for the first time, in May 2009, [redacted] stated it produced foreign-to-foreign records [redacted] pursuant to the Orders. [redacted] stopped its production of this set of foreign-to-foreign records on May 29, 2009, after service of the Secondary Order in BR 09-06, which carves out foreign-to-foreign records from the description of records to be produced. Id. at 42-43. ~~(TS//SI//NF)~~

[redacted] Furthermore, because the records are records of foreign-to-foreign communications, almost all of them do not concern the communications of U.S. persons. To the extent any of the records concern the communications of U.S. persons, such communications would be afforded the same protections as any other U.S. person communication [redacted] authorities. Id. at 43. ~~(TS//SI//NF)~~

[redacted]

[redacted]

B. **Storage and Handling of Credit Card Information** ~~(TS)~~

In the months after the issuance of Orders in docket number BR 06-05, a small percentage of records produced by [redacted] and [redacted] contained credit card numbers in one of the fields when a caller used a credit card to pay for the call. See Ex. B, docket number BR 06-08, at 6-8. At NSA's request, [redacted] and [redacted] removed credit card numbers from this field in the records they provided to NSA starting on July 10, 2006, and October 11, 2006, respectively. Ex. B, docket number BR 06-12, at 5-7. Since that time, NSA spot checks have confirmed that [redacted] and [redacted] continue to remove credit card numbers from the relevant field. Ex. A, at 48. Also since that time, NSA spot checks have identified only one record containing a credit card number. Id. That record, identified in a March 2008 spot check, contained a credit card number in a field different from the field filtered by [redacted] and [redacted]. Id. ~~(TS//SI//NF)~~

According to NSA, it is not feasible for NSA to destroy the records received before October 2006 and the one identified in March 2008 that contain credit card numbers. At this time, the records are stored in one of three locations: back-up tapes, [redacted] storage of raw records, and the [redacted][25] Destroying records stored in any of these

[25] Although NSA used the records that contain credit card numbers to make chain summaries (which in turn are stored in the chain summary database), the credit card numbers did not become part of the chain summaries and, therefore, are not stored in the chain summary database. Id. at 48 n.26. ~~(TS//SI//NF)~~

three locations requires significant personnel, time, and system resources that are not justified given the operational need for certain information and the measures to secure the records. Id. at 48-50. ~~(TS//SI//NF)~~

NSA has an operational need for the non-credit card information contained in the records. To destroy records in the [redacted] that contain credit card numbers, NSA would have to destroy a swath of records in addition to those few containing credit card numbers. Id. at 49. In the event of a catastrophic failure, NSA would rebuild the contact chaining database with records now stored on tapes. If NSA were to destroy those records that contain credit card information, either in the [redacted] or on tapes, it would lack information that is necessary for operations and that otherwise it is authorized to retain under the Orders. Id. at 48-49. ~~(TS//SI//NF)~~

Balanced against this significant operational loss is the reasonable measures currently taken by NSA to secure the records. Records contained on back-up tapes and in [redacted] raw records are not available to analysts for queries. In the [redacted], NSA masks the credit card numbers when the records are retrieved in response to an analyst query. Id. at 48-50. Masking ensures that analysts do not have access to the credit card numbers, and analysts cannot unmask the information. Id. at 48 n.26. In the future, when NSA reconstitutes the [redacted] within another system, see Ex. D at 9, the fields containing credit card information will not be included in the data transfer and will be purged. Ex. A. at 49. ~~(TS//SI//NF)~~

VI. PROCEDURES DESIGNED TO MAINTAIN ONGOING COMPLIANCE WITH THE ORDERS (U)

Beginning in docket number BR 08-13, the Government has implemented and the Court has imposed several requirements that will help ensure compliance with the Orders. Each of

these requirements is set forth in the Primary Order in docket number BR 09-09. In general, they require regular communications between NSA and the Department of Justice's National Security Division (NSD) on significant legal interpretations, compliance with the Orders, and oversight responsibilities. Primary Order, docket number BR 09-09, at 13-14. Also, by requiring the sharing of NSA's procedures for controlling access and use of the BR metadata and for training with the National Security Division, the Order gives NSD greater insight into NSA's implementation of its authorities. Id. at 8, 13. ~~(TS//SI//NF)~~

Other requirements and self-imposed "fixes," including technological fixes, specifically address the problem of unauthorized queries of the BR metadata. As noted above, NSA technological fixes prevent any automated querying of the BR metadata and any querying with non-RAS-approved identifiers. NSA also has implemented a new user interface [redacted] – that will limit the number of query hops to three, as authorized by the Orders. Ex. A at 27. Apart from these technological fixes, NSA has recently created the new position of Director of Compliance, who reports directly to the Director and Deputy Director of NSA and has full-time responsibility in this area. Id. at 28. ~~(TS//SI//NF)~~

The Order's requirements serve as an important backstop for these technological fixes. In the event that NSA seeks to implement an automated query process in the future, it must obtain the approval of both NSD and the Court. Primary Order, docket number BR 09-09, at 14. The Orders also now require that all persons accessing the data, including technical personnel, be briefed on the authorizations and restrictions in Orders regarding the BR metadata. Id. at 10. This broader training requirement is designed to prevent, among other things, the creation of processes to access the BR metadata by persons lacking a necessary understanding of the restrictions. In the event that even these safeguards fail, more explicit requirements for logging

access to the BR metadata are designed to identify the source of the non-compliance. See id. at 9-10. ~~(TS//SI//NF)~~

These requirements also provide the Court with additional information regarding NSA's implementation of the Orders. Specifically, any renewal Application must include the report on the meeting between NSA and NSD regarding compliance with the Orders. Id. at 13-14. In addition, NSA must file a report every week describing any dissemination of BR metadata and certifying whether NSA followed the Order's requirements for dissemination. Id. at 10-11. The dissemination report and the training requirement for persons receiving results of BR metadata queries also address NSA's prior non-compliance with the Order's dissemination requirements. In addition, following renewal of the authorities in Docket Number BR 09-09 and any subsequent renewal, an attorney from NSD will meet with appropriate NSA personnel to brief such personnel on the requirements of the Court's authorization. ~~(TS//SI//NF)~~

Last, in the Application that the Government intends to file for the renewal of docket number BR 09-09, it will seek authority to resume querying the BR metadata using telephone identifiers that NSA has determined meet the RAS standard. Although NSA's violations of the Orders did not concern its application of the RAS standard, the standard is the cornerstone minimization procedure that ensures the overall reasonableness of the production. It is appropriate, therefore, that in connection with the request for authority to make RAS determinations the Government proposes two additional minimization and oversight procedures concerning RAS determinations and queries. First, NSA plans to review its RAS determinations at regular intervals. Specifically, NSA will review a RAS determination at certain intervals: at least once every one hundred eighty days for U.S. telephone identifiers or any identifier believed to be used by a U.S. person; and at least every year for all other telephone identifiers. Ex. A at

25. Second, where such information is available, NSA will make analysts conducting queries aware of the time period for which a telephone identifier has been associated with [redacted] organizations, in order that the analysis and minimization of the information retrieved from the queries may be informed by that fact. Id. at 26. ~~(TS//SI//NF)~~

The Application will also include two oversight requirements similar to those included in the Order in docket number BR 08-13 and prior Orders. Specifically, twice during the ninety day period of authorization, NSD will review NSA's queries of the BR metadata, including a review of a sample of the justifications for RAS approval. Moreover, NSA will report to the Court twice during the ninety day period of authorization regarding, among other things, its queries of the BR metadata. The Court will maintain the authority to approve automated query processes upon request from the Government, once DOJ and NSA are comfortable requesting such authority from the Court. ~~(TS//SI//NF)~~

CONCLUSION (U)

The Government recognizes that no oversight regime will eliminate all risk of non-compliance. The above requirements, fixes, and proposed procedures, however, address the identified and systemic instances of non-compliance with the Orders and seek to protect against vulnerabilities with the implementation of future authorities. The Government respectfully submits that together these steps provide a solid foundation to monitor and promote continued future compliance. The Government will continue to monitor, evaluate and report to the Court on the effectiveness of the oversight and compliance regime discussed herein. ~~(TS//SI//NF)~~

Respectfully submitted,

David S. Kris
Assistant Attorney General for National Security

By: [redacted]

Office of Intelligence
National Security Division
United States Department of Justice

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2009 AUG 17 PM 4:15
CLERK OF COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket number: BR 09-09

DECLARATION OF LIEUTENANT GENERAL KEITH B. ALEXANDER,
UNITED STATES ARMY,
DIRECTOR OF THE NATIONAL SECURITY AGENCY

(U) **BACKGROUND**

(U) I, Lieutenant General Keith B. Alexander, depose and state as follows:

(U) I am the Director of the National Security Agency ("NSA" or "Agency"), an intelligence agency within the Department of Defense ("DoD"), and have served in this position since 2005. I currently hold the rank of Lieutenant General in the United States

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

Army and, concurrent with my current assignment as Director of the National Security Agency, I also serve as the Chief of the Central Security Service and as the Commander of the Joint Functional Component Command for Network Warfare. Prior to my current assignment, I have held other senior supervisory positions as an officer of the United States military, to include service as the Deputy Chief of Staff (DCS, G-2), Headquarters, Department of the Army; Commander of the U.S. Army's Intelligence and Security Command; and the Director of Intelligence, United States Central Command.

(U) As the Director of the National Security Agency, I am responsible for directing and overseeing all aspects of NSA's cryptologic mission, which consists of three functions: to engage in signals intelligence ("SIGINT") activities for the U.S. government, to include support to the government's computer network attack activities; to conduct activities concerning the security of U.S. national security telecommunications and information systems; and to conduct operations security training for the U.S. government. Some of the information NSA acquires as part of its SIGINT mission is collected pursuant to Orders issued under the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA").

(U) PURPOSE AND SUMMARY

~~(TS//SI//NF)~~ This Declaration responds to the Court's Order of 2 March 2009 in docket number BR 08-13 and its subsequent orders in docket numbers BR 09-01, BR 09-06, and BR 09-09 concerning NSA's incidents of non-compliance in implementing a 24 May 2006 Order of the Court pursuant to 50 U.S.C. § 1861 (Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations), as well as subsequent renewals of the 24 May 2006 Order. NSA refers to the program in

which such records are acquired and analyzed as the "Business Records FISA Order" or as the "BR FISA."

~~(TS//SI//NF)~~ The Orders in docket numbers BR 08-13, BR 09-01, BR 09-06, and BR 09-09 direct that the government file with the Court, upon completion of NSA's end-to-end system engineering and process reviews of its handling of the BR FISA metadata, a report that includes, among other things: (1) a description of the results of NSA's end-to-end review, to include any additional instances of non-compliance identified therefrom; (2) a full discussion of the steps taken to remedy any additional non-compliance as well as those incidents described in the Court's 2 March 2009 Order in docket number BR 08-13, and an affidavit attesting that any technological remedies have been tested and demonstrated to be successful; and (3) the additional minimization and oversight procedures the government proposes to employ should the Court decide to authorize the government's resumption of regular access[1] to the BR metadata. *See, e.g.*, Primary Order, docket number BR 09-06, at 15-16. This Declaration responds to each of these requirements. Each of the matters discussed in this Declaration, with the exception of the [redacted]" matter, is discussed in greater depth in NSA's Report dated 25 June 2009 entitled "Implemention of the Foreign Intelligence

[1] ~~(TS//SI//NF)~~ The term "regular access" refers to NSA's proposed resumption of previously authorized access to the BR FISA metadata, to include automated alerting and querying of the metadata, as well as the authority to establish whether a telephony selector meets the Reasonable Articulable Suspicion ("RAS") standard for analysis. I understand that in seeking renewal of the authority granted by the Court in Docket Number BR 09-09, the government will not be seeking the resumption of "regular access" to the BR FISA metadata. Rather, the government intends to seek authority: (a) for certain designated NSA officials to approve access to the BR metadata for purposes of obtaining foreign intelligence information through contact chaining [redacted] using telephone identifiers that those officials have determined meet the RAS standard; and (b) for NSA analysts who have received appropriate training on the BR FISA metadata ("BR-cleared analysts") to be able to access the BR metadata to perform queries. Resumption of automated alerting and/or querying of the BR metadata will be sought via subsequent submissions and commence only with the approval of the Court.

Surveillance Court Authorized Business Records FISA Order – NSA Review" (hereafter "End-to-End Report"), which is attached hereto.

~~(TS//SI//NF)~~ In summary, NSA's end-to-end review compared all aspects of its handling of the BR FISA metadata with the requirements of the Orders in docket number BR 09-06 and prior docket numbers. This review identified several new issues, in addition to the issues previously reported to the Court, that are of concern to NSA. This Declaration addresses issues, including those that required some form of technical remedy or "fix," which fall into four general categories: the use of automation to assist analytic efforts in a manner not authorized; improper analyst queries of the BR metadata repository; improper access to or handling of the BR metadata; and lack of a shared understanding of the BR program. With the exception of the [redacted] issue, each of the issues addressed herein is discussed in more detail in the End-to-End Report.

~~(TS//SI//NF)~~ The Court's Primary Order in docket number BR 09-09 requires that "the government's submission regarding the results of the [BR FISA] end-to-end review" include: (1) "a full explanation of why the government has permitted dissemination outside NSA of U.S. person information in violation of the Court's Orders in this matter;" (2) "a full explanation of the extent to which NSA has acquired call detail records of foreign-to-foreign communications from [redacted] pursuant to orders of the FISC, and whether the NSA's storage, handling, and dissemination of information in those records, or derived therefrom, complied with the Court's orders;" and (3) "either (i) a certification that any overproduced information, as described in footnote 10 of the government's application, has been destroyed, and that any such information acquired pursuant to this Order is being destroyed upon recognition; or (ii) a full explanation as to

why it is not possible or otherwise feasible to destroy such information." Primary Order, docket number BR 09-09, at 16-17. This Declaration also responds to each of these requirements.

~~(TS//SI//NF)~~ The statements made in this Declaration are based upon: my personal knowledge; information provided to me by my subordinates in the course of my official duties -- in particular as a result of the end-to-end systems engineering and process reviews conducted at NSA since the filing of my declarations in this matter on 17 and 26 February 2009 in docket number BR 08-13; the advice of counsel; and conclusions reached in accordance with all of the above.

I. (U) END-TO-END REVIEW

A. (U) RESULTS, REMEDIES, AND TESTING

1. ~~(U//FOUO)~~ Use of Automation in a Manner Not Authorized

~~(TS//SI//NF)~~ The Telephony Activity Detection (Alerting) Process

~~(TS//SI//NF)~~ As previously reported in my declaration filed on 17 February 2009, until 24 January 2009, NSA employed an activity detection ("*alert*") process, which used an *"alert list"* consisting of counterterrorism telephony identifiers[2] to provide automated notification to signals intelligence analysts if one of their assigned foreign counterterrorism targets was in contact with a telephone identifier in the United States, or if one of their domestic targets associated with foreign counterterrorism was in contact with a foreign telephone identifier. NSA's process compared the telephony identifiers on

[2] ~~(TS//SI//NF)~~ In the context of this Declaration, the term "identifier" means a telephone number, as that term is commonly understood and used, as well as other unique identifiers associated with a particular user or telecommunications device for purposes of billing and/or routing communications, such as International Mobile Subscriber Identity (IMSI) numbers, International Mobile station Equipment Identity (IMEI) numbers, and calling card numbers.

the alert list against incoming BR FISA telephony metadata as well as against telephony metadata that NSA acquired pursuant to its Executive Order (EO) 12333 SIGINT authorities. Reports filed with the Court incorrectly stated that NSA had determined that all of the telephone identifiers it placed on the alert list were supported by facts giving rise to a reasonable, articulable suspicion (RAS) that the telephone identifier was associated with one of the targeted Foreign Powers as required by the Court's Orders, *i.e.*, RAS approved. In fact, the majority of telephone identifiers included on the alert list had not been RAS approved, although the identifiers were associated with the Foreign Powers covered by the Business Records FISA Order.

~~(TS//SI//NF)~~ The Telephony Activity Detection Process was turned off at 1:45 a.m. on Saturday, 24 January 2009. On Monday, 26 January 2009, the Telephony Activity Detection Process was restarted, but without the use of metadata obtained pursuant to the Business Records FISA Order. In other words, at present, NSA compares telephony metadata obtained pursuant to its EO 12333 SIGINT authorities against a list of telephone identifiers that are of interest to NSA's counterterrorism personnel. No BR FISA metadata is being used as an input in the Telephony Activity Detection Process.[3]

~~(TS//SI//NF)~~ The shutdown of the Telephony Activity Detection Process was done by technical experts assigned to NSA's Technology Directorate (TD) and witnessed by representatives from NSA's Signal's Intelligence Directorate (SID). A subsequent

demonstration to SID Oversight and Compliance on 27 January 2009, following resumption of the Telephony Activity Detection Process using telephony metadata obtained pursuant to NSA's EO 12333 SIGINT authorities, confirmed that the system was not processing any BR FISA metadata. Tests conducted at that time demonstrated that no results of "BRF" (Business Records FISA) type were contained in the system, and no internal system processes for alerting on BR FISA metadata were running on the system. A sample of alert email notifications was examined and only EO 12333 alerts were being produced. Since that time, periodic reviews conducted by NSA's Homeland Security Analysis Center (HSAC) Technical Director (at least twice per month) have confirmed that the Telephony Activity Detection Process system has continued to produce only EO 12333 alerts.

~~(U//FOUO)~~ The [redacted] Mechanism

~~(TS//SI//NF)~~ As previously reported in my declaration filed on 26 February 2009, NSA analysts working counterterrorism targets had access to a tool known as [redacted]" to assist them in determining if a telephony identifier of interest was present in NSA's EO 12333 SIGINT collection or BR FISA metadata repositories and, if so, what the level of calling activity was for that identifier. Although this tool could be used in a stand-alone manner, it was more frequently invoked by other analytic tools. On 19 February 2009, NSA confirmed that the [redacted] tool enabled analysts to query the BR FISA metadata, as well as metadata obtained from EO 12333 SIGINT collection, using telephone identifiers that had not been determined to meet the RAS standard.

~~(TS//SI//NF)~~ NSA had previously disabled certain tools designed to perform searches against BR FISA metadata in [redacted] one of the data repositories used to

store BR FISA metadata, on 6 February 2009. To prevent additional instances of non-compliance in the access to the data within the [redacted] BR FISA contact chaining repository by automated tools/processes, including [redacted] on 20 February 2009, NSA removed all existing system level Public Key Infrastructure (PKI) certificates that afforded these tools/processes access to the BR FISA metadata in [redacted].[4] A PKI system-level certificate is essentially a "ticket" used by the system to recognize and authenticate that the automated capability has the authority to access the database. As a result of the removal of system level certificates, all automated query capabilities against the [redacted] BR FISA contact chaining repository were rendered inoperable. Removal of the system level certificates was done by [redacted] technical personnel. A subsequent inspection conducted by both [redacted] technical personnel and SID's Oversight and Compliance verified that the certificates were no longer on the list of authorized BR FISA users. HSAC analysts then subsequently verified that the automated processes no longer worked following removal of the certificates.

~~(TS//SI//NF)~~ Subsequent inspection of the system logs, to include an audit of activity from 1 March – 1 June 2009, conducted by SID Oversight & Compliance, confirmed that the system level certificates were no longer able to access the BR FISA metadata in [redacted] These system logs, which document any person or process submitting queries to the [redacted] BR FISA contact chaining repository, indicated that only manual queries by individual BR-cleared analysts were performed. These logs were then used by SID Oversight & Compliance to audit each analyst's queries of the BR

[4] (S) [redacted], discussed below, exists outside of [redacted] and, therefore, was not affected by this remedy.

FISA metadata. Continued periodic review of these logs will confirm that no automated processes are gaining access to the BR FISA metadata in [redacted] until such time that a tested and Court-approved capability is brought into operation.

~~2. (TS//SI//NF)~~ Improper Queries of the BR Metadata Repository

~~(U//FOUO)~~ Improper Analyst Queries

~~(TS//SI//NF)~~ My declaration filed on 26 February 2009 identified and discussed queries using non-RAS approved identifiers of the BR FISA metadata by analysts who did not realize their queries were reaching into the BR FISA metadata. NSA implemented a software modification (the "Emphatic Access Restriction" or "EAR") that allows chaining on only those identifiers that have been determined to satsify the RAS standard. The EAR is designed to eliminate the possibility of this problem recurring.

~~(TS//SI//NF)~~ As previously reported to the Court, three NSA analysts inadvertently performed chaining within the BR FISA metadata using non-RAS approved identifiers. To ensure compliance with the Business Record FISA Order's requirement that NSA personnel use only RAS-approved identifiers to query the BR FISA metadata, NSA made system level changes to the BR FISA [redacted] repository (Action 1) that is used by analysts to perform contact chaining [redacted] This software restrictive measure, the EAR, ensures queries are employed using only RAS-approved identifiers as seeds and prohibits queries made with non-RAS-approved identifiers as seeds against the [redacted] BR FISA contact chaining repository.[5]

[5] ~~(S)~~ [redacted], discussed below, exists outside of [redacted] and, therefore, queries to it are not vetted by the EAR.

~~(TS//SI//NF)~~ [redacted] was the software tool interface used by analysts to manually query the BR FISA chain summaries in [redacted] at the time the EAR was implemented. The EAR is written into the [redacted] middleware.[6] As a BR-cleared analyst logs into [redacted], the Authentication Service determines if the user is approved for access to the BR FISA metadata. However, before the middleware will execute the query, the EAR requires that it access a [redacted] database that contains the disposition of RAS-approved identifiers. [redacted] now obtains from HSAC, on an approximately hourly basis, the most up-to-date Station Table with the current list of RAS-approved identifiers. (The Station Table serves as NSA's definitive list of identifiers that have undergone RAS determinations.) Upon obtaining the RAS-approval status of the query "seed," the EAR determines whether to allow the middleware to conduct the query or prohibit it. Additional "hop" queries will be permitted by EAR as long as the lineage of an identifier resolves back to a RAS-approved "seed." As discussed further below, NSA began to implement [redacted] in late July 2009, which, as an additional middleware software restrictive measure, will limit the number of hops permitted from a "seed" to three, in accordance with the Court's Orders. As of 31 July 2009, access to the [redacted] BR FISA contact chaining repository can only be achieved through use of [redacted] (discussed below). All prior versions of [redacted] have been locked out from access to this data.

[6] (U) Middleware is a general term for any programming that serves to "glue together" or mediate between two separate and usually already existing programs. A common application of middleware is to allow programs written for access to a particular database to access other databases.

~~(TS//SI//NF)~~ To further mitigate the possibility of additional instances of non-compliant querying of the BR FISA material, NSA created a software interface (Action 2) that requires authorized analysts affirmatively to invoke an option (or "opt in") for access. This "opt in" measure was designed prior to the end-to-end review to ensure that analysts know when they have accessed the [redacted] BR FISA metadata repository. As an additional remedy (Action 3) and to ensure queries against the BR FISA metadata are evaluated against the most current list of RAS-approved identifiers, NSA now ensures that [redacted], the system that is used for contact chaining [redacted] against the BR FISA repository, is updated on an hourly basis with the most current list of RAS-approved identifiers from the Station Table.

~~(TS//SI//NF)~~ The software measures described in Actions 1 and 2 above were tested by [redacted] technical personnel at the component level via unit tests, a methodology used to verify that individual units of source code are working properly. Each affected software component was modified as necessary, and then specific tests were conducted to ensure the proper operation of that software component. For Action 1, the test methodology for the EAR software consisted of standard component testing. The tests included attempts to query with both approved and non-approved identifiers. Queries against approved identifiers ran successfully, while queries against non-approved identifiers failed. As the deployment of the EAR was done with urgency to remedy this compliance issue, initial testing was conducted over a period of two days. For this reason, the full test suite was re-run the week following the EAR's implementation to re-verify test results. The testing was judged to be complete and no "bugs" or deficiencies were found. For Action 2, the test included attempts to use the approved user interface

(which operated correctly) and the prohibited user interfaces (which failed). Action 3 was tested by verifying receipt of the expected update file on an hourly basis, comparing the file sizes of the file-sent and file-received, and automated production of an e-mail verifying that the status changes had been applied to the operational system. Following testing, the system was demonstrated to show correct operation to TD leadership, members of the HSAC, SID Oversight & Compliance, and NSA's Office of General Counsel (OGC). Subsequent inspection of system logs, to include an audit of activity from 1 March – 1 June 2009, conducted by SID Oversight & Compliance, provided additional verification that the system was operating correctly.

~~(TS//SI//NF)~~ ~~U.S.~~ Identifiers Designated as RAS-Approved without OGC Review

~~(TS//SI//NF) Be~~tween 24 May 2006 and 2 February 2009, NSA Homeland Mission Coordinators (HMCs) or their predecessors concluded that approximately 3,000 domestic telephone identifiers reported to Intelligence Community agencies satisfied the RAS standard and could be used as seed identifiers. However, at the time these domestic telephone identifiers were designated as RAS-approved, NSA's OGC had not reviewed and approved their use as "seeds" as required by the Court's Orders. NSA remedied this compliance incident by re-designating all such telephone identifiers as non RAS-approved for use as seed identifiers in early February 2009. NSA verified that although some of the 3,000 domestic identifiers generated alerts as a result of the Telephony Activity Detection Process discussed above, none of those alerts resulted in reports to Intelligence Community agencies.[7]

[7] ~~(TS//SI//NF)~~ The alerts generated by the Telephony Activity Detection Process did not then and does not now, feed the NSA counterterrorism target knowledge database described in Part I.A.3 below.

~~(TS//SI//NF)~~ Another historic incident of non-compliance, uncovered during the end-to-end review, relates to errors made in the process of implementing the initial BR FISA Orders in 2006, when a few domestic telephone identifiers were designated as RAS-approved and chained without OGC approval due to analyst errors. For example, a process error occurred when an analyst inadvertently selected an incorrect option which put the domestic telephone identifier into a large list of foreign identifiers which did not require OGC approval as part of the RAS approval process. The HMC failed to notice the domestic identifier in the large list of foreign identifiers at the time, and once the RAS justification was approved, the domestic telephone identifier was chained without having first gone through an NSA OGC First Amendment review as required by the BR FISA Orders. NSA estimates that this type of analyst error occurred only a few times. Each time an error of this type was identified through NSA's quality control regime, senior HMCs provided additional guidance and training to analysts, as appropriate, and the incorrectly approved identifier was changed to non-RAS approved and then re-submitted for proper approval and OGC review.

~~(TS//SI//NF)~~ Use of Correlated Identifiers to Query the BR FISA Metadata

~~(TS//SI//NF)~~ The end-to-end review uncovered the fact that NSA's practice of using correlated identifiers to query the BR FISA metadata had not been fully described to, nor approved by, the Court. An identifier is considered correlated with other identifiers when each identifier is shown to identify the same communicant(s). [redacted]

[redacted]

~~(TS//SI//NF)~~ NSA analysts authorized to query the BR FISA metadata routinely [redacted] to query the BR FISA metadata without a separate RAS determination on each correlated identifier. In other words, if there was a successful RAS determination made on any one of the identifiers in th[redacted] correlation [redacted], and all of the correlated identifiers [redacted], were considered RAS-approved for purposes of the query because they were all associated with the [redacted]. NSA obtained [redacted] correlations from a variety of sources to include Intelligence Community reporting, but the tool that the analysts authorized to query the BR FISA metadata primarily used to make correlations is called [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted] - a database that holds correlations [redacted] between identifiers of interest, to include results from [redacted] - was the primary means by which [redacted] correlated identifiers were used to query the BR FISA metadata. On 6 February 2009, prior to the implementation of the EAR, [redacted] access to BR FISA metadata was disabled, preventing [redacted] from providing automated correlation results to BR FISA-authorized analysts. In addition, the implementation of the EAR on 20 February 2009 ended the practice of treating [redacted] correlations as RAS-approved in manual queries conducted within [redacted] since the EAR requires each identifier to be individually RAS-approved prior to it being used to query the BR FISA metadata. NSA ceased the practice of treating [redacted] correlations as RAS-approved within the [redacted] in conjunction with the March 2009 Court Order.

[redacted]

~~(TS//SI//NF)~~ [redacted] **Display Feature Provided Information Concerning Contacts of Third-Hop Identifiers**

~~(TS//SI//NF)~~ As discussed above [redacted] is the software tool interface used by analysts to manually query the BR FISA chain summaries in [redacted]. The latest version of [redacted] as noted above, limits the number of "hops"

permitted from a "seed" to three, in accordance with the Court's Orders. During testing of the beta version of [redacted] and its hop restriction, NSA determined that, despite the hop restriction, a feature called [redacted] could be invoked to provide an analyst with the number of unique contacts for a third-hop identifier, a type of information that would otherwise only be revealed by a fourth hop.[9] This feature did not return to the analyst any information on the contacts of the last selector in a contact chain other than their total number of unique contacts. After consultation with NSA OGC, the [redacted] feature in the beta version of [redacted] was disabled for last-hop identifiers.[10] This corrected version of [redacted] was deployed to select users beginning on 23 July 2009.

~~(TS//SI//NF)~~ The [redacted] feature was not exclusive to the beta version of [redacted] prior versions of [redacted], since its first delivery beginning in late 2001/early 2002, provided analysts the [redacted] feature. In prior versions of [redacted], Look Ahead was generally the same: if an analyst activated [redacted] in his or her preferences his or her BR FISA contact chaining query results would include the number of unique contacts for each returned identifier, including for identifiers in the third hop from the RAS-approved seed.

---

[9] ~~(S)~~ NSA discovered this issue subsequent to finalization of the end to end report. DoJ, National Security Division (NSD) personnel were notified of the [redacted] feature on 29 July 2009, and orally notified Court Advisors on 30 July 2009. The Court was formally notified of this matter with a notice filed on 4 August 2009 in accordance with Rule 10(c) of the FISC Rules of Procedure.

[10] [redacted]

~~(TS//SI//NF)~~ On 24 July 2009, HSAC instructed all persons authorized to query the BR FISA metadata not already using [redacted] to migrate to [redacted] as soon as possible and uninstall all previous versions of the [redacted] software. As of 31 July 2009, access to the [redacted] BR FISA contact chaining repository can only be achieved through use of [redacted] All prior versions of [redacted] have been locked out from access to this data. Following the lock out of all prior [redacted] versions, the system was demonstrated to show correct operation to TD leadership, the Chief HSAC, and members of SID's Oversight & Compliance. Should the Court authorize additional analysts to query the BR FISA metadata, NSA will ensure that they only do so with [redacted] or its successor that likewise does not permit [redacted] to display the number of unique contacts for a third-hop identifier in the BR FISA metadata.

~~(TS//SI//NF)~~ NSA identified two common practices used by BR metadata analysts that mitigated [redacted] potential for non-compliance. First, although NSA analysts were permitted three hops in the BR FISA metadata from a RAS-approved seed, in practice NSA analysts infrequently chained out beyond the second hop. Second, [redacted] users frequently disabled [redacted] because its use resulted in slower queries. To the extent that [redacted] was used with BR FISA metadata, NSA has concluded, based on discussions with [redacted] users, that the information returned by [redacted] would not have been disseminated. Instead, [redacted] ad information was used by NSA personnel for target development purposes. The number of unique contacts of a third-hop identifier assisted analysts in determining whether the third-hop identifier was one of genuine interest or not, such as a [redacted] identifier that might be added to a defeat list.

3. ~~(U//FOUO)~~ Improper Access to or Handling of the BR FISA Metadata

~~(TS//SI//NF)~~ **Data Integrity Analysts' Use of BR FISA Metadata**

~~(TS//SI//NF)~~ As part of their Court-authorized function of ensuring BR FISA metadata is properly formatted for analysis, Data Integrity Analysts seek to identify numbers in the BR FISA metadata that are not associated with specific users, *e.g.*, "high volume identifiers." [redacted]. NSA determined during the end-to-end review that the Data Integrity Analysts' practice of populating non-user specific numbers in NSA databases had not been described to the Court.

~~(TS//SI//NF)~~ For example, NSA maintains a database, [redacted] which is widely used by analysts and designed to hold identifiers, to include the types of non-user specific numbers referenced above, that, based on an analytic judgment, should not be tasked to the SIGINT system. In an effort to help minimize the risk of making incorrect associations between telephony identifiers and targets, the Data Integrity Analysts provided [redacted] included in the BR metadata to [redacted] A small number of [redacted] BR metadata numbers were stored in a file that was accessible by the BR FISA-enabled [redacted], a federated query tool that allowed approximately 200 analysts to obtain as much information as possible about a particular identifier of interest. Both [redacted] and the BR FISA-enabled [redacted] allowed analysts outside of those authorized by the Court to access the non-user specific number lists.

~~(TS//SI//NF)~~ In January 2004, [redacted] engineers developed a "defeat list" process to identify and remove non-user specific numbers that are deemed to be of little analytic value and that strain the system's capacity and decrease its performance. In building defeat lists, NSA identified non-user specific numbers in data acquired pursuant to the BR FISA Order as well as in data acquired pursuant to EO 12333. Since August 2008, [redacted] had also been sending all identifiers on the defeat list to the [redacted]

~~(TS//SI//NF)~~ While the positive impacts that result in making these numbers available to analysts outside of those authorized by the Court seem to be in keeping with the spirit of reducing unnecessary telephony collection and minimizing the risk of making incorrect associations between telephony identifiers and targets, upon identifying this as an area of concern NSA took several remedial actions to end these practices. As of 2 May 2009, NSA quarantined the BR-derived identifiers on [redacted] On 12 May 2009, NSA shut off access to the file containing the small number of BR-derived [redacted] identifiers by the BR FISA-enabled [redacted] tool. On 11 May 2009, [redacted] removed eight BR FISA identifiers from its SIGINT-only defeat list.

~~(TS//SI//NF)~~ To verify the technical measures taken were successful, from 1-2 May 2009, technical personnel segregated and deactivated BR FISA-derived data in [redacted] previously entered by the Data Integrity Analysts. The [redacted] database is hosted in a [redacted] database. Each record contains a STATUS field that is either set to "ACTIVE" or "DELETE." If the STATUS field is set

to "ACTIVE," then the selector is a valid phone number and is being used for a purpose of which NSA is not interested; however, the record is available for query by analysts and follow-on systems. If the STATUS field is set to "DELETE," then the record is unavailable to analysts or other systems. In order to segregate and deactivate the BR FISA-derived records, the decision was made to change the STATUS field from "ACTIVE" to "DELETE," which means that the number is unavailable to NSA analysts or other systems. Due to the volume of entries, a program was written and executed to change the status.

~~(TS//SI//NF)~~ After testing the program on a small sampling of data and the test results were found to be accurate, the program was executed. Technical personnel monitored initial execution and performed a series of tests to validate the results. At the completion of program execution, Technical Personnel again performed those tests to validate the results. The validation testing was performed three times and results were consistent.

~~(TS//SI//NF)~~ The Primary Order in docket number BR 09-09, dated 9 July 2009, now permits NSA to use certain non-user specific numbers and [redacted] identifiers for purposes of metadata reduction and management.

~~(TS//SI//NF)~~ **Handling of BR FISA Metadata**

~~(TS//SI//NF)~~ The end-to-end review uncovered that NSA's data protection measures were not constructed exactly as the Court Order sets out. Specifically, while the Order requires processing of the data to be carried out on "select" machines using "encrypted communications," the protections NSA affords the data, though different, are quite effective. NSA provides strong and robust physical and security access controls,

but there are not specifically designated machines on which the technical personnel are required to work nor are the communications encrypted. To accurately reflect NSA's data protection measures, NSA worked with the Department of Justice (DoJ) to revise the orders proposed to and ultimately adopted by the Court in docket number BR 09-06.

~~(TS//SI//NF)~~ Data Integrity Analysts sometimes pulled samples of BR metadata onto a non-audited group/shared directory to carry out authorized activities. While the Data Integrity Analysts are authorized to access the data, they are not authorized to move it from the auditable repository into a shared directory where analysts, BR-cleared and otherwise, could have viewed the data. This shared folder was in essence a work space in which the Data Integrity Analysts could perform their authorized activities. There is, however, no reason to believe that analysts, BR-cleared or otherwise, accessed the BR metadata through the shared directory: only a small group of non-cleared analysts had access to the files on this server and it would have been outside the scope of their duties to access the BR metadata samples on the group/shared directory. It is also unlikely that any of the cleared analysts would have accessed this data. As an extra safeguard, NSA has implemented additional access controls that provide appropriate storage areas for the samples of BR FISA metadata used by Data Integrity Analysts for technical purposes.

~~(TS//SI//NF)~~ System Developer Access to BR FISA Metadata while Testing New Tools

~~(TS//SI//NF)~~ During the review NSA discovered that a group of software developers designing a next generation metadata analysis graphical user interface (GUI), [redacted] ([redacted] is the replacement for [redacted] and uses the same authentication/authorization mechanism as [redacted]), had queried the BR FISA metadata 20 times while running tests between September 2008 and February 2009.

This access occurred due to the dual responsibilities of the individuals involved. The developers on [redacted] also have maintenance responsibilities of the operational system, [redacted], where their access to BR FISA is warranted on a continual basis. While the actions were in keeping with the Court Orders in place at the time of the queries, under the current Court Order the developers will require OGC approval prior to engaging in their development and testing activities.

~~(TS//SI//NF)~~ When this issue surfaced, NSA implemented a software change on 19 March 2009 to prevent the [redacted] GUI from accessing BR FISA metadata regardless of the user's access level or the RAS status of the identifier.[11] This change was tested by [redacted] developers and [redacted] technical personnel via a demonstration that the [redacted] could not be used against BR FISA metadata even when a BR FISA-cleared user attempted to do so. NSA also implemented an oversight process whereby all BR FISA-authorized technical personnel who have both maintenance and development responsibilities have their accesses to BR FISA metadata revoked when involved in new systems development, except when granted by NSA's OGC on a case-by-case basis. This process will ensure no inadvertent access to the data until such time as these technical personnel receive OGC authorization to access BR FISA metadata to test technological measures designed to enable compliance with the Court Order. SID Oversight & Compliance is notified each time anyone's permission to access the BR FISA metadata is changed and tracks these changes for compliance purposes.

---

[11] ~~(TS//SI//NF)~~ As of 20 February, EAR would have prevented any query made through the [redacted] GUI that included a non-RAS-approved identifier.

~~(TS//SI//NF)~~ **External Access to Unminimized BR FISA Metadata Query Results**

~~(TS//SI//NF)~~ During the end-to-end review, NSA's Review Team learned that analysts from the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and National Counterterrorism Center (NCTC) had access to unminimized BR FISA query results via an NSA counterterrorism target knowledge database. This matter is discussed in more detail below in Section II.

4. ~~(TS//SI//NF)~~ Lack of a Shared Understanding of the BR Program

~~(S//NF)~~ [redacted] **Not Audited Prior to January 2009**

~~(TS//SI//NF)~~ The end-to-end review surfaced an issue concerning proper auditing of the [redacted]. In addition to the [redacted] BR FISA chaining summary repository in which contact summaries are stored and where the bulk of metadata analysis takes place, a separate database, the [redacted], stores particular fields from each record (as opposed to summaries of those records). This database is used regularly by the Data Integrity Analysts but is also accessible by other analysts authorized to query the BR FISA metadata. When a report is to be issued based on analysis conducted in the repository of contact summaries, analysts often verify what they intend to report by accessing the records in this second data repository. The end-to-end review uncovered the fact that this second database had not been audited. In response, NSA modified the database to enhance its auditability and NSA has audited every query made in the database since February 2009 and found no indication of improper queries.[12]

[12] ~~(TS//SI//NF)~~ Although the [redacted] suffered a system crash in September 2008, NSA was ultimately able to recover sufficient data to permit NSA Oversight & Compliance personnel to conduct sample audits of queries since the Order's inception. These sample audits revealed no unauthorized access to nor improper queries against the BR FISA metadata.

~~(TS//SI//NF)~~ **Provider Asserts That Foreign-to-Foreign Metadata Was Provided Pursuant to Business Records Court Order**

~~(TS//SI//NF)~~ The end-to-end review team learned that [redacted] This matter is discussed in more detail below in Section III.

B. (U) MINIMIZATION AND OVERSIGHT PROCEDURES

~~(TS//SI//NF) In~~ addition to the steps taken to remedy the specific issues identified above, NSA plans to institute additional oversight and compliance processes designed to ensure that NSA will comply with any order authorizing NSA to resume regular access to the BR FISA metadata.

~~(TS//SI//NF)~~ Several additional procedures already have been incorporated into the Court's Primary Order in docket number BR 09-09. The Primary Order now imposes additional access controls for technical personnel. In the past, NSA had logged queries to the BR metadata by analysts and briefed only those analysts on the authorization granted by the Orders. Now, the Orders require NSA to log access to the BR FISA metadata by technical personnel as well as by analysts, and to brief technical personnel, as well as analysts, on the authorization granted by the Orders. *See* Primary Order, docket number BR 09-09, at 9-10. These tightened controls should provide greater accountability for any decision to access the BR FISA metadata and will educate all personnel, particularly those who set up the tools and processes for accessing the BR FISA metadata, about the rules governing access and use. Additionally, the Primary Order now incorporates mechanisms to better ensure that the results of queries to the BR FISA metadata are

treated in accordance with the Court's Orders. Specifically, NSA is now providing weekly dissemination reports to the Court and analysts not cleared to query the metadata are not permitted access to query results before they receive appropriate training. *See id.* at 10-12.

~~(TS//SI//NF)~~ The current Primary Order also incorporates the additional oversight procedures first proposed by the government in its application in docket number BR 09-01. *See id.* at 8, 13-14. In general, those additional oversight procedures require greater coordination between various NSA components and DoJ's National Security Division concerning implementation and interpretation of the Orders. They also require that the Court approve the implementation of any automated process involved in the querying of the BR FISA metadata. These additional procedures are designed to eliminate the risk of incorrect legal interpretations, to ensure timely notice to DoJ and the Court of material issues, and to ensure that any automated query process has been tested and demonstrated to be compliant with the Orders, and approved by the Court, before implementation.

~~(TS//SI//NF)~~ NSA will also propose several new minimization and oversight procedures in the application seeking the renewal of docket number BR 09-09. The application will request authority for NSA to resume approving telephone identifiers for contact chaining [redacted] First, the application will propose that NSA re-visit its RAS determinations at certain intervals: at least once every one hundred and eighty days for U.S. telephone identifiers or any identifier believed to be used by a U.S. person; and at least every year for all other telephone identifiers. This new re-validation procedure is designed to ensure that for as long as NSA queries the BR FISA metadata

with RAS-approved telephone identifiers, those identifiers will continue to meet the RAS standard. Second, the application will propose an express requirement that, where NSA has affirmative information that a RAS-approved telephone identifier was, but may not presently be, or is, but was not formerly, associated with a Foreign Power, analysis and minimization of results of queries using that identifier be informed by that fact. This requirement is designed to focus NSA's analysis on the period for which the RAS-approved telephone identifier is associated with a Foreign Power.

~~(TS//SI//NF)~~ NSA has recently reviewed and revalidated the oversight documentation governing the BR FISA. This documentation consists of a set of Standard Operating Procedures (SOPs). These SOPs address: access to BR FISA metadata; BR FISA audit procedures; compliance notifications; DoJ and NSA OGC spot checks; and the respective roles of various NSA personnel involved in oversight and compliance activities.

~~(TS//SI//NF)~~ More recently, NSA's Associate Directorate of Education and Training (ADET) has redesigned the BR FISA training package to ensure common and expert level proficiency in the rules and procedures governing appropriate handling of the BR FISA metadata. ADET, together with NSA OGC and the SID Oversight & Compliance organization, has developed and is in the process of implementing a series of on-line training modules, complete with competency testing, specifically addressing activities conducted with respect to the BR FISA Order. Moreover, an oral competency test is currently being administered to each Homeland Mission Coordinator at the completion of the training they are currently receiving to ensure they understand the restrictions governing access to the BR FISA metadata.

~~(TS//SI//NF)~~ Should the Court approve the application seeking the renewal of docket number BR 09-09 and grant NSA authority to resume approving telephone identifiers for contact chaining [redacted] NSA will update its SOPs and training package for the BR FISA to account for the change in authority and the new procedures associated with that change.

~~(TS//SI//NF)~~ NSA has implemented and intends to implement additional software restrictions and changes to the BR metadata system architecture. As discussed above, NSA implemented a software change, [redacted] n July 2009 to restrict analyst queries to the number of hops authorized by the Orders.[13] Furthermore, NSA is revamping its baseline system architecture, to include formal system engineering of all aspects governing the interaction of analysts and processes. Using principles of system engineering, configuration management, and access control, NSA has explored a future implementation of the BR FISA program to be used should the Court authorize NSA to resume regular access to the BR FISA metadata. This architecture has the potential to offer more effective management of the system as a whole, and a team of employees will collaborate to manage the entire system. The single approach, providing visibility into the overall structure of the system to the entire team, together with the technology solutions discussed above, will help prevent an isolated decision to connect a tool or process to the BR FISA database.

~~(TS//SI//NF) In~~ addition, requirements from the Court Order will be formally translated by NSA into system requirements prior to any changes to the system

[13] ~~(S)~~ NSA OGC granted approval for developers to access BR FISA metadata for the specific purpose of testing and demonstrating [redacted]

architecture, which should prevent problems such as the misunderstanding among different personnel as to how the Telephony Activity Detection Process functioned. Finally, NSA has recently created the new position of Director of Compliance, reporting directly to me and the Deputy Director of NSA. The Director of Compliance has full-time responsibility in this area. The Director of Compliance will be responsible for continuous modernization and enforcement of our mission compliance strategies and activities to ensure their relevance and effectiveness. At the same time, this new position will serve as an ongoing reminder of the importance of compliance work, and provide greater visibility and transparency in this essential area.

~~(TS//SI//NF)~~ The Court entrusted NSA with extraordinary authority, and with it came the highest responsibility for compliance and protection of privacy rights. In several instances, NSA implemented its authority in a manner inconsistent with the Orders, and some of these inconsistencies were not recognized for more than two and a half years. These are matters I take very seriously, and the changes NSA has made and will make as a result of the end-to-end review, with regard to both analyst access and the handling of data, are intended to address them directly and to provide an environment for successful implementation and management of the program should the Court decide to authorize NSA's resumption of regular access to the BR metadata. The technological remedies discussed herein have remedied the identified instances of noncompliance and should significantly improve future compliance with the Court's Orders. I attest that each of these remedies has been tested and demonstrated to be successful insofar as each functions as intended. Although no corrective measures are infallible, I believe that this more robust regime and the technological remedies NSA has instituted, particularly the

implementation of the EAR, represent significant steps to reduce the possibility of any future compliance issues and to ensure that mechanisms are in place to detect and respond quickly if a compliance incident were to occur.

II. ~~(TS//SI//NF)~~ PRE-JUNE 2009 BR FISA DISSEMINATION PRACTICES

~~(TS//SI//NF)~~ In a 16 June 2009 notice to the Court, the government reported that NSA had provided personnel from CIA, FBI, and NCTC access to a database that contained, among other things, some unminimized results of BR FISA metadata queries. NSA did not make all, or even most, BR FISA query results available via this database. Instead, NSA placed only certain BR FISA query results in the database, generally in response to specific requests for information received from specially-cleared personnel from NSA, CIA, FBI, or NCTC.

~~(TS//SI//NF)~~ In response to this compliance incident, the Court issued an order on 22 June 2009 which directed NSA to provide the Court with "a full explanation of why the government has permitted the dissemination outside NSA of U.S. person information without regard to whether such dissemination complied with the clear and acknowledged requirements for sharing U.S. person information ... pursuant to the Court's orders" in the BR docket. This section responds to the Court's Order for a full explanation of how this compliance incident occurred. It also describes actions NSA has taken to investigate and remediate the problem.

~~(S//NF)~~ [redacted]

[redacted]

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

[redacted]

[14] ~~(TS)~~ The BR FISA end to end report stated that approximately 200 external analysts were permitted access to the database; further investigation revealed that the number is actually closer to approximately 250.

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

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

~~(S//NF)~~

~~(TS//SI//NF)~~ The Court's 2006 BR FISA Order authorized NSA to acquire the [redacted]

[redacted]

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

[redacted]

[15] ~~(U//FOUO)~~ In contrast, USSID 18 permits NSA to disseminate outside of NSA information identifying U.S. persons if the U.S. person information is necessary to understand *foreign intelligence* or assess its importance. USSID 18 also permits the Deputy Chief of Information Sharing Services, among others, to approve disseminations of U.S. person identifying information.

[redacted]

(U) **Discovery and Response to the Problem**

~~(TS//SI//NF)~~ In June 2009, during the course of NSA's end-to-end review of the Agency's implementation of the BR Order, NSA identified as a compliance matter the use of the database to make unminimized BR and [redacted] query results available to FBI, CIA, and NCTC. NSA personnel also determined that, despite the disabling of the hyperlink button in July 2008, external analysts could have continued accessing the database if they retained the Uniform Resource Locator (URL) address for the database. After this problem was identified on 11 June 2009, NSA immediately began terminating individual external customer account access to the target knowledge database. NSA completed this action by 12 June 2009.

~~(TS//SI//NF)~~ To determine why this compliance issue occurred, NSA spoke with the senior analysts and oversight personnel who were aware of the Court-ordered minimization requirements and of how the database was used. These conversations revealed NSA personnel generally followed the minimization requirements when the Agency issued formal reports based on queries of the metadata acquired pursuant to the Court's BR FISA Orders. However, even though the applicability of the minimization requirements to the shared database is clear in hindsight, until the issue was discovered during NSA's end-to-end review [redacted] the new dissemination procedures required by the Court's Orders.

~~(TS//SI//NF)~~ Since identification of this matter, NSA has attempted to determine the actual extent of access to the database and/or use of the BR[redacted]metadata. As part of that effort, the Agency has conducted a detailed audit of log-in activity of external analysts from each of the participating organizations.[16] The audit revealed that no external analysts accessed the database after January 2009. Prior to that, [redacted] approximately 250 analysts had permission to access the database but only about one-third actually did so. Of that number, only approximately 47 external analysts did more than log in and change their passwords. These approximately 47 external analysts appear to have queried the database in the course of their counterterrorism responsibilities and they accessed directories that contained the results of [redacted] BR queries, including unminimized U.S. person-related information. The BR [redacted] derived U.S. person information consisted of unmasked telephone numbers or email addresses that were returned in response to RAS-approved queries made of the underlying metadata.

~~(TS//SI//NF)~~ In addition to the audits, NSA also asked CIA, FBI, and NCTC to describe how their personnel made use of their access to the database.[17] The NCTC employees with access to the database reported that they did not make use of any unminimized BR[redacted]query results in any NCTC analytic products. Only two FBI analysts accessed this database while researching counterterrorism leads. Several other

[redacted]

[17] ~~(S)~~ The response from each agency covered the entire period of time that their respective personnel had access to the database.

FBI analysts believe they may have accessed the database while working closely with a team of FBI analysts [FBI Team 10] who were detailed to NSA and working under NSA's control.[18] The FBI reported that none of the external FBI analysts published or disseminated anything as a result of their access to the database and FBI believes that it is "highly unlikely that any FBI-published analytical products or investigative reports ever contained this data" from the database. CIA reported that some of its personnel who were approved for access to the compartmented counterterrorism program used information in the database for lead purposes, to include as a basis for initiating counterterrorism discussions between CIA and FBI personnel. However, CIA's review indicated that any information contained in the database, to include [redacted] BR metadata chaining results, "was used very rarely in finished intelligence products produced by CIA analysts for senior policymakers." Instead, information obtained from CIA's access to the database was usually used "in conjunction with reporting from other intelligence sources."

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

[redacted]

~~(S//SI//NF)~~ NSA has corrected the problem in this specific instance by terminating all external access to the database in question. Beyond that, the Agency recognizes that the underlying issue is the need to identify all areas of activity that are subject to these Court Orders and/or other legal restrictions and conditions, in order to ensure compliance. This requires several elements, including an accurate end-to-end picture of how data is handled -- by technical (*e.g.*, systems administrators) and operational personnel alike -- from collection through dissemination; ongoing oversight, training, and compliance efforts; and system testing procedures that give assurance that data is actually being handled as required. NSA has instituted measures in all these areas, as described in detail in the report on the Agency's end-to-end review. In addition, as discussed above, NSA has created the new position of Director of Compliance to ensure that NSA has a comprehensive and effective compliance program and maintain heightened attention in this particular area. NSA continues to work to discover and correct any outstanding issues and avoid any recurrence.

(U) **Dissemination of U.S. Person Identifying Information**

~~(TS//SI//NF)~~ When an NSA analyst determines that information identifying a U.S. person needs to be included in a report, a designated NSA approving official must authorize the release.[19] The Information Sharing Services office is generally the

[19] ~~(TS//SI//NF)~~ The designated approving official does not make a determination to release U.S. person information requested by DoJ or DoD personnel in connection with prudential searches, such as those

responsible entity for approving such releases. Within the context of EO 12333 collected information, the release authority includes the Chief and Deputy Chief, Information Sharing Services, SID Director and Deputy Director, Senior Operations Officer (SOO),[20] DIRNSA, and Deputy DIRNSA. In the EO 12333 context, the approving authority must determine that the information is related to a foreign intelligence purpose, and that the U.S. person information is necessary to understand or assess the value of the information.

[redacted]

NSA followed USSID 18 procedures for the dissemination of U.S. person identities and did not appropriately implement the additional requirements identified in the Court orders for a determination that the information is related to counterterrorism information. Furthermore, NSA did not implement appropriate procedures reflecting the fact that individuals other than the Chief, Information Sharing Services were not specifically authorized to grant the release of U.S. person information. Although NSA now understands the fact that only a limited set of individuals are authorized to approve these releases under the Court's authorization, it seemed only appropriate at the time to allow her Deputy or those acting in her capacity to be delegated with this authority as well.

~~(TS//SI//NF)~~ On 18 June 2009, NSA advised the Office of Information Sharing Services that the chief of that office was the only NSA official authorized to approve the

---

conducted for criminal or detainee proceedings. In the case of such requests, NSA's Litigation Support Team conducts specific prudential searches of NSA holdings but these prudential searches do not include or result in queries of the BR FISA metadata.

[20] ~~(S)~~ The SOO is the Senior Operations Officer, in charge of the National Security Operations Center, NSA's 24/7 operations center. The SOO acts in place of the DIRNSA, when the DIRNSA is unavailable. The Court's Order dated 29 May 2009 recognized that the SOO may approve disseminations for after-hours requests.

dissemination of any U.S. person identity derived from BR FISA metadata and that the chief must make the required findings and document those findings prior to any such dissemination. Moreover, on 9 July 2009, in docket number BR 09-09, the Court increased the numbers of individuals permitted to approve disseminations to include the Chief, Information Sharing Services, the SOO, the SID Director, the Deputy Director of NSA, and the Director of NSA.

(U) **Review of Prior Disseminations**

~~(TS//SI//NF)~~ On 29 July 2009, members of DoJ/NSD's Office of Intelligence Oversight Section completed a review of all BR FISA disseminations containing U.S. person identities in order to determine who approved the disseminations and what determinations were made, if any, by the approving official.

~~(TS//SI//NF)~~ The NSD review identified 280 disseminations of reports containing BR FISA-derived U.S. person identities. Of the 280 disseminations, 92 were approved by the Chief of Information Sharing Services, 170 were approved by the Deputy Chief of Information Sharing Services, 15 were approved by a SOO, one was approved by an acting Chief of Information Services, and two were approved by an acting Deputy Chief of Information Sharing Services. The disseminations authorized by persons other than the Chief of Information Sharing Services did not occur during any particular time frame. Rather, they were distributed throughout the lifespan of the collection.

~~(TS//SI//NF)~~ Of the 280 disseminations of reports containing BR FISA-derived U.S. person identities, 74 were made in 2006, 101 were made in 2007, 95 were made in 2008, and ten were made in 2009. The waiver forms authorizing each of the disseminations in 2006 and 2007, 175 in total, contained no particularized finding relating to the purpose of the dissemination. Beginning in July 2008, however, the

authorizing waivers contained a general finding that the U.S. person identity was foreign intelligence or necessary to understand foreign intelligence. Of the 95 disseminations approved in 2008, 82 contained no finding and 13 contained the foreign intelligence finding. Beginning in January 2009, the authorizing waiver contained specific counterterrorism findings as required by the Court's orders. Eight of the ten waivers issued in 2009 contained this finding. The last two disseminations in 2009, one in May and one in June, however, had only the more general foreign intelligence finding in the waivers.

~~(TS//SI//NF)~~ NSA also reviewed its records of all reports issued that may have included BR FISA-derived information, including the records of reports written by analysts not specifically authorized to query the BR FISA metadata.[21] NSA did not discover any additional reports that were issued by non-BR cleared analysts.

III. ~~(TS//SI//NF)~~ NSA'S COLLECTION OF FOREIGN-TO-FOREIGN CALL DETAIL RECORDS PURSUANT TO THE BR FISA ORDERS

~~(S)~~ [redacted]

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

[21] ~~(TS//SI//NF)~~ To identify the total number of reports produced and disseminated that contained BR-derived information, the NSA reviewed all analyst reporting records, including the records of reports written by non-BR-cleared analysts. When drafting reports, all NSA analysts, including both BR-cleared analysts and non-BR-cleared analysts, are trained to include in any reporting record the sources of the information contained in a report. The NSA's review included an examination of these records, including the fields of each record that might include references to BR-derived source information. The NSA then audited the reports that referenced BR-derived information as a source, and excluded those that referenced BR sources but in fact that did not contain BR-derived information. Through this methodology the NSA was able to determine that 280 were reports were produced and disseminated. Admittedly, this methodology would not account for reports issued with BR-derived data that mistakenly failed to reference BR sources.

[redacted]

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

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

[redacted]

[redacted]

[redacted]

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

[redacted]

[redacted]

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

~~(TS//SI//NF)~~ In May 2009, during a discussion between NSA and [redacted] regarding the production of metadata, a [redacted] representative stated that [redacted] produced the records [redacted] pursuant to the BR FISA Orders. This was the first indication that NSA had ever received from [redacted] of its contrary understanding. At the May 28, 2009, hearing in docket number BR 09-06, the government informed the Court of [redacted] To address the issue, based on the government's proposal, the Court issued a Secondary Order to [redacted] in docket number BR 09-06 that expressly excluded foreign-to-foreign call detail records from the scope of

records to be produced. On May 29, 2009, upon service of the Secondary Order in docket number BR 09-06, [redacted] ceased providing foreign-to-foreign records [redacted]

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

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

almost all of them concern the communications of non-U.S. persons located outside the United States. If NSA were to find that any of the records concerned U.S. persons, their dissemination would be governed by the terms of USSID 18 which are the procedures established pursuant to EO 12333, as amended.

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

[redacted]

[redacted]

[redacted]

[redacted]

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

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

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

[redacted]

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

~~(S)~~ [redacted]

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

[redacted]

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

[redacted]

[redacted]

IV. ~~(TS)~~ NSA'S TREATMENT OF CREDIT CARD DATA CONTAINED IN BR FISA METADATA

~~(TS//SI//NF)~~ As first noted in a report to the Court in docket number BR 06-08, and noted in footnote 10 in the Application in docket number BR 09-09, a small percentage of records received from [redacted] contained credit card numbers in one of the fields when a caller used a credit card to pay for the call. Exhibit B, docket number BR 06-08, at 6-8. At NSA's request, [redacted] removed credit card numbers from this field in the records it provided NSA starting on 10 July 2006, and 11 October 2006, respectively. Exhibit B, docket number BR 06-12, at 5-7. Since that time, NSA spot checks have confirmed that [redacted] continue to remove

credit card numbers from the relevant field. Also since that time, NSA spot checks have identified only one record containing a credit card number. That record contained a credit card number in a field different from the field filtered by [redacted] NSA identified this record during a spot check in approximately March 2008.

~~(TS//SI//NF)~~ The records containing credit card numbers received before [redacted] began filtering (*i.e.*, records received in October 2006 and before) are stored on back-up tapes.[26] Records contained on back-up tapes are not available to analysts for queries and are not readily available to technical personnel. To destroy the individual records that are on back-up tapes would be an extreme resource and system intensive endeavor and therefore not feasible. It would require reloading the records from the tapes onto servers authorized to process BR metadata, uncompressing the records, converting them to a readable format, identifying those with a field containing a credit card number, and then deleting the records. Then NSA would have to test to confirm that only the records with credit card numbers were deleted, back-up the records again to tape storage and delete them from BR metadata servers. As the back-up tapes are necessary to rebuild the contact chaining database in the event of a catastrophic failure, to destroy the tapes prematurely would put at risk NSA's ability to recover information important for operations and still allowed under the Court Order. In the event of the need to restore the [redacted] BR FISA contact chaining repository, as the credit card numbers contained in those records do not become part of the chain summaries, analysts would still not have

[26] ~~(TS//SI//NF)~~ These records also are stored in the [redacted] discussed further below, where they were masked to analysts, and in the raw call detail record repositories, where they were accessible only to technical personnel. *See* Exhibit B, docket number BR 06-12, at 5-7, and Exhibit B, docket number BR 09-09, at 9-10. Analysts are not allowed to have the credit card number unmasked. Although these records were used to make chain summaries and stored in the chain summary database, the credit card numbers contained in the records did not become part of the chain summaries.

access to this information. Based on the above information and that the back-up tapes will be destroyed upon reaching the end of their authorized retention period, NSA considers this information on the back-up tapes secured from user access until their required date of destruction.

~~(TS//SI//NF)~~ The above records containing credit card information are also stored in the [redacted] It is not feasible to delete individual records based on the technical architecture of the [redacted] without deleting all data from the beginning of the BR FISA orders up to October 2006. The loss of such data would be so operationally detrimental that deletion is not feasible. As described in Exhibit B to the Application in BR 09-09, NSA's current solution to ensure NSA analysts do not have access to this credit card information is masking the data upon retrieval. As NSA reconstitutes the [redacted] to systems under a supported architecture, the fields containing credit card information will not be included in the data transfer and will be purged.

~~(TS//SI//NF)~~ The one record with a credit card number identified by NSA since October 2006 exists only in [redacted] storage of raw call detail records, known as the [redacted] and on back-up tapes. As noted above, back-up tapes are not available to analysts. Likewise, the [redacted] is not accessible to analysts for queries. This record is not stored in the [redacted] database and was not used to build a chain summary because it was an incomplete record. In order to delete this single record from the [redacted] upon first isolating the appropriate file, NSA would have to uncompress the data from the provider's proprietary format, convert the data into a readable format, and move the data to a server that hosts the Data Integrity Analysts'

tools to isolate and delete the one record. Removing data on back-up tapes is a difficult process as described above. Based on the above information and that the back-up tapes will be destroyed upon reaching the end of their authorized retention period, NSA considers this information on the [redacted] and the back-up tapes secured from user access until their required date of destruction.

~~(TS//SI//NF)~~ In summary, I certify that the overproduced credit card information has been destroyed or secured as noted above, and that the records containing overproduced credit card information still retained by NSA cannot be accessed by an analyst, but as noted above will be destroyed no later than when the records reach the end of their authorized retention period.

V. (U) Conclusion:

~~(TS//SI//NF)~~ The instances of non-compliance that have been identified in NSA's implementation of the Court's orders in the BR docket stemmed from a basic lack of shared understanding among the key NSA mission, technical, legal and oversight stakeholders concerning the full scope of the BR FISA program. With the remedial steps described above, NSA has taken significant steps to reduce the possibility of future compliance issues. Further, in moving forward, lessons learned as a result of NSA's review of BR FISA practices will be institutionalized, and we will remain constantly vigilant in ensuring that we are in strict compliance with the Court's orders. Although no corrective measures are infallible, NSA has taken significant steps to reduce the possibility of any future compliance issues and to ensure that the mechanisms are in place to detect and respond quickly if a compliance incident were to occur. Therefore, I am

hopeful the Court will again grant NSA regular access to the BR FISA metadata, which I believe is invaluable in helping the Nation detect and thwart potential terrorist threats.

(U) I declare under penalty of perjury that the facts set forth above are true and correct.

KEITH B. ALEXANDER
Lieutenant General, U.S. Army
Director, National Security Agency

Executed this 17TH day of August, 2009

2009 AUG 17 PM 4:16
CLERK OF COURT

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 09-09

DECLARATION OF LIEUTENANT GENERAL KEITH B. ALEXANDER, UNITED STATES ARMY, DIRECTOR OF THE NATIONAL SECURITY AGENCY

(U) I, Lieutenant General Keith B. Alexander, depose and state as follows:

(U) I am the Director of the National Security Agency ("NSA" or "Agency"), an intelligence agency within the Department of Defense ("DoD"), and have served in this position since 2005. I currently hold the rank of Lieutenant General in the United States Army and, concurrent with my current assignment as Director of the National Security

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: Source Marked MR

Agency, I also serve as the Chief of the Central Security Service and as the Commander of the Joint Functional Component Command for Network Warfare. Prior to my current assignment, I have held other senior supervisory positions as an officer of the United States military, to include service as the Deputy Chief of Staff (DCS, G-2), Headquarters, Department of the Army; Commander of the U.S. Army's Intelligence and Security Command; and the Director of Intelligence, United States Central Command.

(U) As the Director of the National Security Agency, I am responsible for directing and overseeing all aspects of NSA's cryptologic mission, which consists of three functions: to engage in signals intelligence ("SIGINT") activities for the U.S. Government, to include support to the Government's computer network attack activities; to conduct activities concerning the security of U.S. national security telecommunications and information systems; and to conduct operations security training for the U.S. Government. Some of the information NSA acquires as part of its SIGINT mission is collected pursuant to Orders issued under the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA").

(U) The statements herein are based upon my personal knowledge, information provided to me by my subordinates in the course of my official duties, advice of counsel, and conclusions reached in accordance therewith.

(U) I. Introduction

~~(TS//SI//NF)~~ Pursuant to a series of Orders issued by the Foreign Intelligence Surveillance Court ("FISC" or "Court") beginning in May 2006, NSA has been receiving

and analyzing certain call detail records or telephony metadata[1] from [redacted] telecommunications providers. NSA refers to the Orders collectively as the "Business Records Order" or "BR FISA." The telephony metadata NSA receives via the BR FISA has enabled it in the past to discover [redacted] and unknown persons in the United States and abroad affiliated with [redacted] and unknown persons in the United States and abroad affiliated with [redacted] and their communications, and act upon and disseminate such information to support the efforts of the United States Government, including the Federal Bureau of Investigation (FBI), to detect and prevent terrorist acts against the United States and U.S. interests. Continued receipt of the telephony metadata is advantageous to NSA's ability to continue its efforts to discover such terrorist organizations and their communications, in order to assist the FBI in detecting, investigating and preventing terrorist acts against the United States. Accordingly, this declaration is intended to provide the Court with my assessment of the value that the BR FISA metadata provides to the NSA and the FBI with respect to the Government's national security responsibilities for the detection, investigation, and prevention of terrorist activities by [redacted]

[1] ~~(S)~~ "Call detail records," or "telephony metadata," include comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) numbers, International Mobile station Equipment Identity (IMEI) numbers, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. A "trunk" is a communication line between two switching systems. *Newton's Telecom Dictionary* 951 (24th ed. 2008). Telephony metadata does not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer.

[redacted] (collectively, the "Foreign Powers").

~~(TS)~~ II. Value of BR FISA Metadata

~~(TS//SI//NF)~~ The BR FISA provides access to bulk call detail records which primarily include records of telephone calls that either have one end in the United States or are purely domestic. This collection of information is not available to NSA through its other authorized foreign intelligence information collections.[2] This data has value to NSA analysts tasked with identifying potential threats to the U.S. homeland and U.S. interests abroad by enhancing their ability to identify, prioritize, and track terrorist operatives and their support networks both in the U.S. and abroad. By applying the Court-ordered "reasonable, articulable suspicion" or "RAS" standard to telephone identifiers[3] used to query the BR FISA metadata, NSA analysts are able to: (i) detect domestic identifiers calling foreign identifiers associated with one of the Foreign Powers and discover who the foreign identifiers are in contact with; (ii) detect foreign identifiers associated with a Foreign Power calling into the United States and discover which

[2] ~~(TS//SI//NF)~~ For example, NSA obtains foreign intelligence information from its collection of overseas communications (SIGINT collection) authorized by Executive Order (EO) 12333, traditional Court-authorized electronic surveillance pursuant to Titles I and III of FISA, Pen Register and Trap and Trace surveillance authorized pursuant to Title IV of FISA, and, more recently, the targeting of non-United States persons reasonably believed to be located overseas pursuant to Section 702 of the FISA Amendments Act of 2008 (FAA). None of these authorities would allow NSA to replicate, or appropriately analyze, the call detail records it receives pursuant to the BR FISA.

[3] ~~(TS//SI//NF)~~ In the context of this Declaration, the term "identifier" means a telephone number, as that term is commonly understood and used, as well as other unique identifiers associated with a particular user or telecommunications device for purposes of billing and/or routing communications, such as International Mobile Subscriber Identity (IMSI) numbers, International Mobile station Equipment Identity (IMEI) numbers, and calling card numbers.

domestic identifiers are in contact with the foreign identifiers; and (iii) detect possible terrorist-related communications occurring between communicants located inside the United States.

~~(TS//SI//NF)~~ Although NSA possesses a number of sources of information that can each be used to provide separate and independent indications of potential terrorist activity against the United States and its interests abroad, the best analysis occurs when NSA analysts can consider the information obtained from each of those sources together to compile and disseminate to the FBI as complete a picture as possible of a potential terrorist threat. Although BR FISA metadata is not the sole source available to NSA counterterrorism personnel, it provides a key component of the information NSA analysts rely upon to execute this threat identification and characterization role.

~~(S)~~ **A. The Value of BR FISA Metadata: Contact-Chaining** [redacted]

~~(TS//SI//NF)~~ The primary advantage of metadata analysis as applied to telephony metadata is that it enables the Government to analyze past connections and patterns of communication. The ability to accumulate metadata substantially increases NSA's ability to detect and identify persons affiliated with the Foreign Powers. Specifically, the NSA performs [redacted] queries on the metadata: contact-chaining [redacted]

~~(TS//SI//NF)~~ When the NSA performs a contact-chaining query on a terrorist-associated telephone identifier, [redacted] identify the further contacts made by that first tier of contacts. In addition, the same process can be used to identify additional tiers of

contacts, out to a maximum of three "hops" from the original identifier, as authorized by the Business Records Order. The collected metadata thus holds contact information that can be immediately accessed as new terrorist-associated telephone identifiers are identified. Multi-tiered contact chaining identifies not only the terrorist's direct associates but also indirect associates, and, therefore provides a more complete picture of those who associate with terrorists and/or are engaged in terrorist activities.

~~(TS//SI//NF)~~ One advantage of the metadata collected in this matter is that it is historical in nature, reflecting contact activity from the past that cannot be captured in the present or prospectively. To the extent that historical connections are important to understanding a newly-identified target, metadata may contain links that are unique, pointing to potential targets that may otherwise be missed. [redacted]

[redacted]

~~(TS//SINF)~~ In sum, the BR FISA metadata analysis enriches the NSA analysts' understanding of the communications tradecraft of terrorist operatives who may be preparing to conduct attacks against the U.S. Terrorist operatives often take affirmative and intentional steps to disguise and obscure their communications. They do this by using a variety of tactics,

~~(TS)~~ B. Filling the Gaps: BR FISA Metadata in the Context of Other Collections

~~(TS//SI//NF)~~ The BR FISA metadata complements information NSA collects via other means and is a valuable, if not the only, means available to NSA for linking possible terrorist-related telephone communications that occur between communicants based solely inside the U.S. NSA analysts use the combination of telephony metadata and communications content collected pursuant to EO 12333 and/or Court-authorized electronic surveillance in concert with BR FISA metadata to develop an accurate characterization of individual/network activity; potentially derive the intent of the individual(s) or network; and learn of new terrorist networks or cells working inside the U.S. NSA's access to the BR FISA metadata improves the likelihood of the Government being able to detect terrorist cell contacts within the U.S.

~~(TS//SI//NF)~~ NSA's traditional SIGINT collection, which focuses strictly on the foreign end of communications, provides limited signals-related information available to aid analysts in identifying possible terrorist connections emanating from or within the U.S. Collection authorized by Section 702 of the FAA is limited to the targeting of non-United States persons located overseas and does not provide NSA with information sufficient to support contact chaining [redacted] Traditional Court-authorized electronic surveillance does not make available the full extent of metadata resident with the service providers and provided through the BR FISA. With the metadata provided by BR FISA, NSA has the information necessary to perform call chaining [redacted] This analysis enables NSA to obtain a fuller understanding of the target and provide FBI with a more complete picture of possible terrorist-related activity occurring inside the U.S.

~~(TS//SI//NF)~~ The value of the BR FISA is not hypothetical. Additional detail available in call data records (CDRs) allows NSA to recognize that a communicant is based in the U.S., a detail often absent in traditional SIGINT collection. Unlike traditional SIGINT collection, BR FISA CDRs include the calling party number in a call that originates from the United States. From telecommunications provider's perspective, only the called number is necessary to complete a call. The originating, or calling, number is not required and, as unnecessary data, is often removed or manipulated by the U.S. telecommunications provider before leaving the U.S en route to an overseas provider. If the calling party information is present, it can be used by other telecommunication providers to understand macro traffic statistics and identify important business opportunities. For this reason, U.S.-origin calls collected overseas often lack a valid U.S. calling party number, making it difficult or impossible to identify that a particular call originated in the U.S.

~~(TS//SI//NF)~~ In illustration, prior to the attacks of 9/11, NSA intercepted via its overseas SIGINT collection and transcribed seven (7) calls made by hijacker Khalid al-Mihdhar, then living in San Diego, California, to a telephone identifier associated with an al Qaeda safe house in Yemen. However, the NSA SIGINT intercept was collected through an access point overseas and the calling party identifier was not available because it had not been transmitted with the call. Lacking this U.S. phone identifier and having nothing in the content of the calls to suggest that al-Mihdhar was actually inside the United States, NSA analysts concluded that al-Mihdhar remained overseas when, in fact, he was in San Diego. The BR FISA metadata addresses the information gap that existed at the time of the al-Mihdhar case. It potentially allows NSA to note these types

of suspicious contacts and, when appropriate, to tip them to the FBI for follow-on analysis or action.

~~(TS//SI//NF)~~ Once an identifier has been detected, NSA can use BR FISA metadata along with other data sources to quickly identify the larger network and possible co-conspirators both inside and outside the U.S. for further investigation by the FBI with the goal of preventing future attacks. One recent example of BR FISA's contribution to characterizing a network of interest was the investigation referred to within NSA and FBI as [redacted]

~~(TS//SI//NF)~~ NSA's involvement with [redacted] began in January 2009. NSA analysts were following a foreign-based e-mail identifier associated with an al Qaeda facilitation cell in Yemen, an activity of significance due to U.S. Government concern with Yemen's potential to serve as an al Qaeda safe haven. This particular e-mail identifier was tasked under FAA authorities while numerous other network identifiers were monitored through EO 12333 authorities. [redacted] Upon verification, NSA [redacted] as permitted by the Court-approved minimization procedures for NSA's FAA collection, informed the FBI of the U.S. location of the identifiers. Upon receipt of

[redacted]

the NSA information, the FBI initiated a full field investigation and sought its own FISA coverage on the newly-discovered domestic links.

~~(TS//SI//NF)~~ NSA used the BR FISA metadata to aid the FBI investigation by adding critical insight into the network's functions and intent. Analysis of the BR FISA metadata demonstrated foreign contacts within the suspected network stretching from Kansas City to New York, the United Arab Emirates, Yemen and Denmark. While BR FISA did not discover the person of interest in Kansas City, the telephony metadata was able to confirm suspicions that the FBI already had about him. It confirmed the target's outbound contacts with other members of the network and provided a better understanding of the network. This characterization would not have happened without leveraging both the BR FISA metadata and the FAA access in conjunction with FBI's investigation.

~~(TS//SI//NF)~~ As the [redacted] example illustrates, BR FISA metadata is an important resource for investigating threat leads obtained from other SIGINT collection or partner agencies. This is especially true for the NSA-FBI partnership. The BR FISA metadata enables NSA analysts to evaluate potential threats that it receives from or reports to the FBI in a more complete manner than if this data source was unavailable. Even the absence of terrorist-related contacts in the BR FISA metadata can be valuable, because such "negative reporting" helps to assess the credibility of a prospective threat.

~~(TS//SI//NF)~~ A final benefit of the way in which BR FISA metadata complements other counterterrorist-related collection sources is by serving as a significant enabler for NSA intelligence analysis. It assists NSA in applying limited linguistic resources

available to the counterterrorism problem against links that have the highest probability of connection to terrorist targets. Put another way, analysis of the BR FISA metadata can help NSA prioritize for content analysis communications which it acquires under other authorities. While [redacted] assists in identifying terrorist communications of interest, content exploitation is required to achieve a full understanding and characterization of the associations between the telephony identifiers and users. Additionally, content is critical to deriving intent of the individuals and associated networks. BR FISA metadata is an important piece for steering and applying content analysis so the U.S. Government can gain the best possible understanding of terrorist target actions and intentions.

(U) C. Statistics/Additional Examples

~~(TS//SI//NF)~~ The foregoing discussion is not hypothetical. As noted on page seven of NSA's end-to-end report on the Agency's implementation of the Business Records Order, between inception of the first Business Records Order in May 2006, and May 2009, NSA issued 277[5] BR FISA-based reports to FBI and, if appropriate, to other NSA customers. These reports tipped to the FBI roughly 2,900 identifiers that were noted to be in contact with identifiers associated with [redacted]

[5] ~~(TS//SI//NF)~~ The number of reports included in my Declaration of 13 February 2009 was 275. This was based upon information gathered on 6 February 2009. Further review has taken into account the fact that an additional report was issued after 6 February, but before 13 February. Some of these reports had been cancelled for various reasons and some of the cancelled reports were reissued with corrections. Therefore, the correct number of unique reports as of the 13 February 2009 declaration should have been 274. My Declaration also stated that there were 2,549 selectors tipped in these reports. The actual number of selectors tipped in the 274 reports is 2,888.

~~(TS//SI//NF)~~ A recent illustration of the use of the BR FISA metadata can be found in the evaluation of telephony contacts associated with [redacted] an [redacted] associate and primary suspect [redacted]

[redacted]

[redacted]

[redacted]

~~(TS//SI//NF)~~ In an even more recent example, on 2 June 2009 NSA received a request for information from the FBI pertaining to leads associated with [redacted] NSA conducted initial research on the identifiers provided by the FBI in EO 12333 metadata and subsequently sought approval from the FISC to query the identifiers against the BR FISA metadata. [redacted] Without the BR FISA metadata, a significant number of those leads would have remained undiscovered and NSA's ability to evaluate [redacted] U.S. contacts would have been degraded.

(U) IV. Conclusion

~~(TS//SI//NF)~~ In conclusion, while all metadata analysis is essential in the fight against terrorism, the BR FISA metadata provides NSA with additional information readily available through the providers, but which would be otherwise unavailable to NSA. The BR FISA metadata complements and enriches NSA analysts' understanding of the target and provides the capability to detect domestic identifiers calling foreign terrorist identifiers abroad; foreign terrorist-associated targets calling into the United States; and possible terrorist-related communications occurring between communicants solely in the U.S. That the BR FISA metadata is generating what may be perceived as little foreign intelligence in comparison with the volume of the data collected does not discount its value to NSA's analysis of potential terrorist threats to the U.S. and to NSA's ability to provide security for the nation. NSA's access to the BR FISA metadata addresses a key gap in the Intelligence Community's ability to connect foreign and domestic threat-related information and tip this information for appropriate follow-up investigation.

(U) I declare under penalty of perjury that the facts set forth above are true and correct.

VR

KEITH B. ALEXANDER
Lieutenant General, U.S. Army
Director, National Security Agency

Executed this 3rd day of August, 2009

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2009 AUG 17 PM 4:16
CLERK OF COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket No.: BR 09-09

AFFIDAVIT OF ROBERT S. MUELLER, III

I, Robert S. Mueller, III, hereby affirm the following:

(U) I am the Director of the Federal Bureau of Investigation (FBI), United States Department of Justice (DOJ), a component of an Executive Department of the United

~~Derived From: Multiple Sources~~
~~Declassify On: 20340810~~

States Government (USG). I am responsible for, among other things, the national security operations of the FBI, including the FBI's Counterterrorism Division (CTD).

(U) The matters stated herein are based upon my personal knowledge, my review and consideration of documents and information available to me in my official capacity, information furnished by the National Security Agency (NSA) and information furnished by Special Agents and other employees of the FBI.

(U) Purpose of the Affidavit

~~(S//NF)~~ This affidavit is submitted in response to the Court's Orders dated March 2, March 5, May 29, and July 9, 2009 (Orders). It describes the FBI's assessment of the value of the Business Records FISA (BR FISA) metadata to FBI national security investigations and, more broadly, to the national security of the United States.

(U) Relevance to Authorized Investigations

~~(S//NF)~~ [redacted] and unknown persons in the United States and abroad affiliated with [redacted] [redacted] are the subject of numerous FBI predicated investigations being conducted under guidelines approved by the Attorney General pursuant to Executive Order 12333, as amended. As of August 10, 2009, the FBI had approximately [redacted] open predicated investigations[1] targeting [redacted]

[1] (U) Predicated investigations are either full investigations or preliminary investigations. A full investigation may be initiated if there is an articulable factual basis for the investigation that reasonably indicates, *inter alia*, that a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity. A preliminary investigation may be initiated on the basis of information or an allegation

[redacted]. As of August 10, 2009, the FBI was conducting approximately [redacted] predicated investigations of individuals believed to be associated with [redacted] under guidelines the Attorney General has approved pursuant to Executive Order 12333, as amended.

~~(TS/SI//NF)~~ The National Security Agency (NSA) has issued and is expected to continue to issue to the FBI BR FISA metadata "tippers" regarding telephone numbers that are associated with [redacted] that are targets of FBI investigations. The tippers provide information regarding contacts between these foreign telephone numbers and domestic telephone numbers. NSA identifies the assessed users of the foreign telephone numbers, the dates of contact between the foreign telephone numbers and the domestic telephone numbers, and any additional information, e.g., foreign telephone number's country of origin, domestic telephone number's city and state, etc., that NSA may have regarding the telephone numbers.

~~(S//SI)~~ FBI Processing of BR FISA Metadata Reports

~~(S//NF)~~ FBI employees from the Counterterrorism Division's (CTD) Communications Analysis Unit (CAU) are detailed full-time to the NSA's Homeland

---

indicating, *inter alia*, that a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.

Security Analysis Center (HSAC). These detailees, known as "Team 10," consist of a Supervisory Special Agent and several Intelligence Analysts. Team 10's chief responsibility is to identify and initially process domestic information contained in reports disseminated to the FBI from HSAC.[2] Upon receiving an HSAC report, Team 10 queries FBI databases to determine whether the FBI already has information about any of the domestic facilities contained in the report. Team 10 then transmits the NSA information together with additional analysis based on any information already known to the FBI to the appropriate FBI field offices. Team 10 also recommends subsequent investigation to the field office.

~~(S//SI)~~ Value of BR FISA Metadata to FBI Investigations

~~(TS//SI//NF)~~ The FBI derives value from the BR FISA metadata primarily in two ways. First, BR FISA metadata provides information that assists the FBI in detecting, preventing, and protecting against terrorist threats to the national security of the United States by providing the predication to open investigations, advance pending investigations, and revitalize stalled investigations. Second, metadata obtained via the BR FISA can provide warning signals that alert the FBI to individuals who are inside the United States and are linked to persons who pose a threat to the national security.

~~(S//SI)~~ I. BR FISA Metadata as Additional Information

~~(S//SI)~~ The FBI is authorized, *inter alia*, to collect intelligence and to conduct investigations to detect, obtain information about, and prevent and protect against

[2] ~~(S//NF)~~ HSAC reports include BR FISA metadata "tippers."

terrorist threats to national security. The more information the FBI has regarding such threats to the national security, the more likely it will be able to prevent and protect against those threats. The BR FISA metadata program is a source of information that the FBI uses in its mission to detect, prevent, and protect against terrorist threats to national security. The oft-used metaphor is that the FBI is responsible for "connecting the dots" to form a picture of the threats to national security. BR FISA metadata provides additional "dots" that the FBI uses to ascertain the nature and extent of domestic threats to the national security.

~~(S//SI)~~ In certain circumstances, the FBI may already have an investigative interest in a particular domestic telephone number prior to receipt of a BR FISA metadata tipper containing that domestic telephone number. Nevertheless, the tipper may be valuable if it provides new information regarding the domestic telephone number that revitalizes the investigation or otherwise allows the FBI to focus its resources more efficiently and effectively.

~~(S//SI)~~ The FBI has received BR FISA metadata tippers containing information not previously known to the FBI about domestic telephone numbers utilized by targets of pending preliminary investigations. The information from the BR FISA metadata tippers has provided articulable factual bases to believe that the subjects posed a threat to the national security such that the preliminary investigations could be converted to full investigations, which, in turn, led the FBI to focus resources on those targets.[3] The FBI has also re-opened previously closed investigations based on information contained in

[3] (U) Because there is greater predication for a full investigation (an articulable factual basis to believe the subject poses a threat to the national security) than for a preliminary investigation (information or allegation that the subject is or may be a threat to the national security), the FBI tends to focus more resources on full investigations than preliminary investigations.

BR FISA metadata tippers. In those instances, the FBI had previously exhausted all leads and concluded that no further investigation was warranted. The new information from the BR FISA metadata tippers was significant enough to warrant the re-opening of the investigations.

~~(S//NF)~~ Provided below are two examples of investigations [redacted] that were re-opened because of new information provided by a BR FISA metadata tipper.

~~(S//SI)~~ II. BR FISA Metadata Analysis as an "Early Warning System"

~~(S//SI)~~ The earlier the FBI obtains information about a threat to national security, the more likely it will be able to prevent and protect against those threats. The BR FISA metadata program sometimes provides information earlier than the FBI's other investigative methods and techniques. To use the oft-used metaphor, BR FISA metadata sometimes provides "dots" that the FBI may not otherwise have uncovered until much later in its investigation. In those instances, the BR FISA metadata program acts as an "early warning system" of potential threats against national security.

~~(S//SI)~~ In certain circumstances, the FBI may receive a BR FISA metadata tipper containing information regarding a domestic telephone number that the FBI inevitably would have discovered via other investigative techniques. Nevertheless, that tipper is valuable because it provides information earlier than the FBI would otherwise have obtained it. Earlier receipt of the information may advance the investigation and could contribute to the FBI preventing or protecting against a threat to national security that, absent the BR FISA metadata tipper, the FBI could not.

~~(S//SI)~~ The FBI has also received BR FISA metadata tippers regarding domestic telephone numbers in which the FBI had little or no prior investigative interest at the time the tipper was received. In those instances, the FBI opened either a preliminary or a full investigation of the user of the domestic telephone number. Here again, although the FBI may have inevitably developed an investigative interest in these domestic telephone numbers, it is impossible to say when that would have occurred or whether it would have occurred too late to prevent or protect against a terrorist attack.

~~(S//SI)~~ Provided below are two examples of preliminary investigations [redacted] that were commenced based upon BR FISA metadata tippers. In both cases, the investigations were eventually converted to full investigations based on information developed by the FBI, thus demonstrating the value of the BR FISA metadata information.

(U) III. Statistical Information Pertaining to Full Investigations

~~(TS//SI//NF)~~ One method of quantifying the value of the BR FISA metadata to the FBI's efforts to protect the nation's security is the number of predicated full investigations that the FBI has opened or supported using BR FISA metadata provided by the NSA.[4] Full investigations opened based on BR FISA metadata tippers illustrate the value of the BR FISA metadata in assisting the FBI to identify previously unknown connections between persons in the United States and [redacted]. Similarly,

[4] ~~(S//NF)~~ Full investigations are typically more significant and fruitful than preliminary investigations. I will, therefore, limit the information discussed in this affidavit to full investigations that were predicated, in whole or part, or assisted by BR FISA metadata.

the number of preliminary investigations converted to full investigations illustrates the importance of the BR FISA metadata in assisting the FBI to develop suspected connections between persons in the United States and [redacted].

~~(S//NF)~~ Below is a chart containing statistical information pertaining to investigations that were opened as full investigations or converted from preliminary investigations to full investigations based, at least in part, on information from BR FISA metadata since the Court first authorized the BR FISA order in 2006 through 2008. These statistics show that the BR FISA metadata's contribution to FBI investigations is not insignificant. This chart includes (1) the total number of full investigations that are predicated, at least in part, on BR FISA metadata;[5] (2) the number of Intelligence Information Reports (IIRs) issued to foreign partners from these full investigations; and (3) the number of IIRs issued to other U.S. government agencies from these full investigations.

[5] ~~(S//NF)~~ The FBI's statistics include investigations that were (1) opened as full investigations based, at least in part, on BR FISA metadata, and (2) preliminary investigations that were converted to full investigations based, at least in part, on BR FISA metadata. These statistics are limited to investigations that are connected directly to BR FISA metadata tippers. BR FISA metadata tippers have also indirectly contributed to the predication for other investigations. For example, information obtained during the full investigation of [redacted] discussed below, led the FBI to open preliminary investigations of others suspected of engaging in similar activities. This affidavit is limited to investigations based directly, at least in part, on BR FISA metadata.

Year	Full Investigations Opened/Preliminary Investigations Converted to Full Investigations	Intelligence Information Reports (IIRs) Issued to Foreign Partners	IIRs issued to Other U.S. Government Agencies
2006	3	1	3
2007	9	6	8
2008	15	24[6]	35
Total	27	31	46

~~(S//SI)~~ During the 27 full investigations that were based, at least in part, on BR FISA metadata tippers, the FBI has found and identified known and unknown members or agents of [redacted], and those in communication with them. The information NSA has tipped to the FBI has also permitted FBI to acquire additional information about such individuals and their activities, including criminal activities in support of international terrorism.

(U) IV. Specific Examples of Noteworthy Full Investigations

~~(S//SI)~~ To illustrate the value of the BR FISA metadata program to the FBI, four (4) full investigations that were predicated, at least in part, on BR FISA metadata tippers are summarized below.

[6] ~~(S//NF)~~ Because certain IIRs were issued to multiple countries, the FBI issued a total of 51 IIRs to foreign partners.

~~(S)~~ A. [redacted]

~~(S)~~ On or about [redacted] the FBI opened a preliminary investigation of [redacted] a U.S. person, based on an anonymous letter alleging that he and eight others had ties to the Muslim extremist organization [redacted] After pursuing all available leads, the FBI closed the preliminary investigation on [redacted], because it had not developed any evidence tending to show that [redacted] was, in fact, affiliated with [redacted]

~~(TS//SI//OC//NF)~~ On or about [redacted], the FBI received an intelligence report from the NSA that included information and contact chaining analysis conducted on data obtained through the BR FISA order ("metadata report"). The metadata report established a [redacted] connection between a [redacted] telephone known to be used by [redacted] a [redacted]-based extremist with ties to [redacted] and [redacted] an unlisted [redacted] telephone number.[7] The FBI's [redacted] Division opened a preliminary investigation of the unknown user of the [redacted] telephone number based upon the information contained in the metadata report and information contained in FBI's databases that telephone number [redacted] was linked to [redacted] other pending FBI investigations.[8]

---

[7] ~~(S//NF)~~ The metadata tipper established that [redacted] telephone was in contact with another [redacted] telephone. That second [redacted] cellular telephone was in contact with [redacted].

[8] ~~(S)~~ Most notably, prior to [redacted] opening of the preliminary investigation, in an investigation conducted by the [redacted] Division, the FBI had obtained via a national security letter (NSL) telephone records for [redacted], the target of the investigation, who was suspected of [redacted]. According to the telephone records, [redacted] telephone number had contact with [redacted]

~~(TS//SI/REL TO USA, AUS, CAN, GBR, NZL)~~ On or about [redacted], during [redacted] preliminary investigation, the FBI received information from the NSA indicating that someone named [redacted] using the [redacted] telephone number [redacted] had stated that [redacted]. At the time, [redacted] was linked to the [redacted]

~~(S)~~ On or about [redacted] [redacted] was identified by the FBI as a user of telephone number [redacted][10] Based on that identification, the fact that [redacted] was formerly the subject of a [redacted] preliminary investigation, and the phonetic similarity between [redacted] first name [redacted] and the name [redacted] the [redacted] Division converted the preliminary investigation of the unknown user of [redacted] into a full investigation of [redacted]

~~(TS//SI)~~ During the full investigation, the FBI obtained authorization from this Court to conduct electronic surveillance of [redacted] [redacted] Court-authorized electronic surveillance of [redacted] revealed that [redacted] and [redacted] routinely discussed [redacted] Also through this investigation, the FBI has identified other individuals in the United States who are believed to be involved in [redacted]

[redacted]

[10] ~~(S)~~ [redacted] provided [redacted] as his telephone number in a [redacted] he filed with the [redacted]. In addition [redacted]

for [redacted] full investigations have been opened as a result of information obtained through the [redacted] investigation. The FBI has also identified certain methods and means that these individuals use to [redacted], including the suspected use of [redacted]

~~(S//OC/NF)~~ The FBI is working with the Department of Justice, National Security Division, and the United States Attorney's Office, [redacted] to indict [redacted] on criminal charges that include, but are not limited to, [redacted]

~~(S)~~ B. [redacted]

~~(S)~~ On or about [redacted], the FBI opened a full investigation of [redacted] based on information indicating that [redacted] made terrorist threats and were connected to [redacted] On or about [redacted] the FBI closed this investigation (the [redacted] investigation) after pursuing all available leads because the U.S. Attorney's Office, [redacted], was reluctant to proceed unless additional evidence could be obtained.

~~(TS//OC/NF)~~ On or about [redacted] the FBI received a BR FISA metadata report from the NSA that included information and contact chaining analysis

indicating that [redacted] and [redacted] had each been in contact with several cellular telephone numbers in [redacted] that were believed to be used by [redacted][11] The [redacted] cellular telephone numbers were, in turn, in contact with [redacted] telephone numbers believed to be associated with [redacted] which are owned by [redacted][12] In addition, the BR FISA metadata report stated that a [redacted] telephone number, reportedly registered to [redacted] had also been in contact with two of the aforementioned [redacted] telephone numbers.

~~(S//NF)~~ Based upon the information obtained in the [redacted] investigation, information obtained from another investigation that had been conducted from [redacted],[14] and on the information provided by the BR FISA metadata report, the FBI re-opened the full terrorism investigation of [redacted] on [redacted]

~~(S//OC//NF)~~ Since re-opening the investigation in [redacted], the FBI has received reports from various sources, [redacted] are connected to and [redacted] to [redacted]

---

[11] ~~(S//NF)~~ According to NSA reporting, [redacted] was believed to be [redacted] and [redacted] was believed to be a [redacted] and [redacted]

[12] ~~(S)~~ The FBI subsequently confirmed via an NSL that [redacted] and [redacted] were the subscribers of two of the [redacted] telephone numbers.

[13] ~~(S)~~ According to U.S. Intelligence Community reporting, [redacted] that is responsible for directing and supporting [redacted].

[14] ~~(S)~~ In [redacted], the FBI re-opened the full investigation of [redacted] based on an anonymous letter alleging that they supported [redacted]. The FBI uncovered no new additional evidence, and closed the investigation again in [redacted]

~~(S)~~ The FBI continues to investigate [redacted] suspected [redacted] for [redacted] The FBI recently obtained renewed FISC authority to conduct electronic surveillance and physical searches of [redacted] telephone and e-mail accounts, as well as [redacted] telephone and e-mail accounts, as agents of [redacted] The FBI's investigation of [redacted] is ongoing.

~~(S)~~ C. [redacted]

~~(TS//SI//OC/NF)~~ On or about [redacted], the FBI received a BR FISA metadata report from the NSA that included information and contact chaining analysis indicating that associates of [redacted][15] [redacted] living in the [redacted], had been in contact with several U.S. [redacted] telephone numbers.[16] According to the NSA's BR FISA metadata report, two of the foreign telephone numbers that were in contact with [redacted] one [redacted] cellular number and one [redacted] cellular number, were also in contact with U.S. telephone number [redacted] An Internet search of [redacted] by the FBI revealed [redacted] as the apparent subscriber of the telephone number. Furthermore, toll billing records obtained via NSL's in [redacted] by the FBI in connection with other FBI investigations revealed that [redacted] had been in contact with telephone numbers associated with four other pending counterterrorism investigations. That information, in conjunction with the information obtained from the

[15] ~~(TS//SI//OC/NF)~~ According to the NSA, [redacted] is the leader of a mainly [redacted] Islamic extremists called [redacted] and maintains ties to more radical members of [redacted] an organization designated by the Interagency Intelligence Committee on Terrorism (IICT) as a tier 1 support entity to [redacted]

[16] ~~(S//NF)~~ The FBI had received previous reports regarding [redacted] and his activities from both the [redacted].

BR FISA metadata program, formed the basis for the FBI's decision to open a preliminary investigation of [redacted] The preliminary investigation was opened on [redacted]

~~(S//OC//NF)~~ During the preliminary investigation, the FBI learned that [redacted] is a [redacted] board member of [redacted] According to [redacted] [redacted] On or about [redacted] reported to the FBI that [redacted] had been designated by [redacted] as a point-of-contact for [redacted] a senior member of [redacted] and that [redacted] has donated funds to [redacted] Based on this additional information, on [redacted], the FBI converted the preliminary investigation of [redacted] to a full investigation.

~~(S//NF)~~ The FBI has obtained information about several financial transactions that suggests [redacted] is providing material support to a foreign terrorist organization. On [redacted] [redacted] sent [redacted] to [redacted] in [redacted] According to the CIA, [redacted] was a member of [redacted] [redacted] as well as the [redacted]. In addition, [redacted] sent [redacted] to [redacted] in [redacted] on [redacted]. The CIA has reported that [redacted] is believed to be a member of [redacted] Finally, [redacted] sent [redacted] to [redacted]

[redacted], in [redacted] on [redacted]. According to the CIA, [redacted] is a former senior member of [redacted]

~~(S//NF)~~ Although these known money transfers to [redacted] and [redacted] are not particularly large, they do show connections between [redacted] and members and former members of [redacted]. These connections are troubling in light of significant account activity that occurred on [redacted]. On that date, [redacted] made deposits to his checking account of [redacted] and [redacted] including [redacted] in foreign currency. [redacted] also transferred [redacted] to a [redacted] bank named [redacted] This transfer is suspicious because it is larger than [redacted] typical transactions.[18]

~~(S//NF)~~ The FBI continues to investigate [redacted] and has begun to receive and analyze responses to eleven national security letters that were served during [redacted] The FBI is also investigating the [redacted] bank account that received [redacted] from [redacted]

~~(S)~~ D. [redacted]

~~(TS//SI//OC//NF)~~ On or about [redacted], the FBI received a BR FISA metadata report from the NSA that included information and contact chaining analysis

---

[17] ~~(S//NF)~~ The CIA reported in March 2009 that [redacted]

[redacted]

indicating that a [redacted] cellular telephone number used by several extremists associated with the [redacted] had been in contact with several U.S. telephone numbers, including [redacted] cellular number [redacted] The FBI's database contained information from another investigation indicating that the subscriber of the [redacted] telephone number was [redacted] Based on the information contained in the BR FISA metadata report, the [redacted] Division was instructed by FBI HQ to conduct a threat assessment of the user of the [redacted] ostensibly [redacted]

~~(S//NF//OC)~~ The [redacted] Division subsequently received information from a [redacted] that [redacted] had been killed on or about [redacted] Based on the BR FISA metadata, the information identifying the subscriber of the [redacted] telephone number, and [redacted] the FBI's [redacted] Division opened a full investigation of [redacted] to investigate [redacted] alleged association with [redacted] Although [redacted] had been reported killed, the FBI elected to investigate, *inter alia*, whether the report of [redacted] death was accurate and whether others traveled overseas and took part in terrorist training with him in [redacted]

(U) Conclusion

~~(TS//SI)~~ The facts set forth above demonstrate that the BR FISA metadata has historically proved to be a valuable source of intelligence to the FBI. Its historic value leads me to conclude that the BR FISA metadata will continue to be a valuable source of

intelligence that is relevant to numerous FBI-authorized international terrorism investigations. Accordingly, I hereby certify that the BR FISA metadata is relevant to an authorized investigation (other than a threat assessment) to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, and that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment.

(U) Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on August 13, 2009.

ROBERT S. MUELLER, III
Director
Federal Bureau of Investigation