Business Records FISA
NSA Review

25 June 2009

Prepared by: Business Records FISA Team
Lead, [redacted]

~~(TS//SI//NF)~~ Implementation of the Foreign Intelligence Surveillance Court Authorized Business Records FISA – NSA Review
25 June 2009

I. (U) Executive Summary

~~(TS//SI//NF)~~ The Business Records FISA Compliance Review Team of the National Security Agency (NSA), in response to instructions from the Director of NSA (DIRNSA) and as set out in DIRNSA's Declaration of 13 February 2009 to the Foreign Intelligence Surveillance Court (FISC), conducted a comprehensive systems engineering and process review of the instrumentation and implementation of the Business Records (BR) FISA authorization. This review was focused along the two major components where compliance issues had been reported – system-level technical engineering and execution within the analytic workforce.

~~(TS//SI//NF)~~ The review entailed 8 major system or process components of the BR FISA metadata workflow, 248 sub-components, and 93 requirements and resulted in 9 new areas of concern based on past practices as described herein. NSA has taken steps, described herein, to remedy the problems identified, and to ensure to the extent possible they will not recur. NSA has also developed plans for both the current and future architecture to provide more rigorous and efficient protection, control and monitoring of the BR FISA metadata. Implementation of the envisioned changes in architectural design and oversight procedures briefly described in this report will help mitigate vulnerabilities and correct the problems identified through the course of the end-to-end review.

~~(C//REL TO USA, FVEY)~~ The end-to-end review revealed that there was no single cause of the problems that occurred and, in fact, there were a number of successful oversight, management and technology processes in place that operated as designed. The problems NSA experienced stemmed from a basic lack of shared understanding among the key mission, technology, legal and oversight stakeholders of the full scope of the program to include its implementation and end-to-end design. The complexity of the overall configuration, due in part to the intricacy of the system and the differing rules associated with NSA's various authorizations, was also a contributing factor as was the fact that NSA oversight was primarily focused on analyst access to and use of the metadata.

~~(TS//SI//NF)~~ This report, which assumes a basic knowledge of NSA's structure and some familiarity with the FISC documents and DIRNSA declarations associated with the BR FISA program, addresses previously identified and newly uncovered areas of concern, as well as the corrective actions already taken, and those on-going or planned, to address these issues. It details the scope of the end-to-end review, the methodology employed and the results. It also describes the minimization and oversight procedures NSA proposes to employ should the FISC decide to approve NSA's 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.e., regular authorized access). Additionally, the report outlines the checks, balances and safeguards

engineered into the system; points to the need to clarify existing language in some cases; and describes enhanced training for the workforce that is designed to prevent future instances of non-compliance. Finally, the report includes a summary of a proposed technical architecture which will further protect BR FISA metadata.

~~(TS//SI//NF)~~ In conducting the end-to-end review, NSA established a diverse team of technical, legal and mission experts to examine jointly the key functional areas of system engineering, mission operations and oversight. The NSA team created an architectural diagram of the end-to-end data and workflow and examined each major system component and sub-component to ensure a complete understanding of how the data was handled. In addition, NSA compiled all BR FISA-related requirements and evaluated each system and process component against those requirements to identify areas of concern or vulnerability.

~~(U//FOUO)~~ In moving forward, NSA will not only address the specific technical and process issues identified in this report, but will also implement changes in its program management construct to increase transparency and awareness among accountable parties and establish an enduring view of the full scope of the program.

~~(U//FOUO)~~ NSA may produce additional supplements to this report to the extent necessary to respond to additional items that may be of interest to the court.

II. ~~(U//FOUO)~~ Results of Detailed Analysis on Identified Areas of Concern

A. ~~(U//FOUO)~~ Previously Reported Compliance Issues

1. ~~(U//FOUO)~~ Telephony Activity Detection (Alerting) Process

(U) Description

~~(TS//SI//NF)~~ As previously described to the Court,[1] NSA implemented an activity detection (alerting) process[2] in a manner that was not authorized by the Court's Order, and then inaccurately described that process in its initial and each subsequent report to the Court. NSA stated that only RAS-approved selectors were included on the Activity Detection List when, in fact, the list included those RAS-approved and non-RAS-approved selectors[3] which were also tasked for content collection by counterterrorism analysts tracking [redacted] and associated terrorist organizations or, subsequent to

[1] ~~(U//FOUO)~~ See DIRNSA Declaration dated 13 February 2009, at Sections III.A. and III.B.

[2] ~~(U//FOUO)~~ NSA now refers to the Alert Process and the Alert List as the Activity Detection Process and the Activity Detection List to more accurately describe their functions.

[3] ~~(TS//SI//NF)~~ In mid-January 2009, there were 1,935 RAS-approved and 15,900 non-RAS-approved selectors on the Activity Detection List. At that time, the Station Table (the reference database of all RAS evaluations) had approximately 27,000 selectors identified as RAS-approved and 63,000 selectors identified as non-RAS-approved.

the modifications of the BR FISA Court Order on 8 August 2006 and again on 14 June 2007, [redacted][4]

~~(TS//SI//NF)~~ The Activity Detection List that was used prior to 24 January 2009 to alert analysts to a selector of potential interest was a list independent of the Station Table, the historic reference database of all RAS evaluations. The Activity Detection List was compared against the incoming BR FISA data to assist analysts in prioritizing their work. Some of the selectors on the Activity Detection List had been RAS evaluated, and their status would have been reflected on the Station Table. Others had never been evaluated for RAS and would not have appeared in the Station Table. In this latter case, they were treated as non-RAS-approved on the alert list which meant that contact chaining did not take place in the complete body of archived data until and unless the particular selector had satisfied the RAS standard.

~~(TS//SI//NF)~~ NSA's description of this process to the Court reflected a similar process already in place for the [redacted] program, but NSA's implementation of the two processes was actually different. Further, as described to the Court, the NSA personnel who designed the BR FISA Activity Detection List process believed that the requirement to satisfy the RAS standard was only triggered when access was sought to NSA's stored (i.e., "archived" in NSA parlance) repository of BR FISA metadata. The inaccurate characterization was identified in the course of a meeting between NSA and representatives from the National Security Division (NSD) of the Department of Justice (DoJ) on 9 January 2009. During discussions, DoJ identified what was ultimately determined to be an incident of non-compliance with the Order. After additional inquiry, NSD/DoJ officially reported the incident to the FISC on 15 January 2009.

~~(TS//SI//NF)~~ Between 20 and 24 January 2009, the RAS-approved portion of the Station Table was mistakenly implemented as the Activity Detection List in an attempt to address the original problems identified with the alerting process. At that time there were approximately 27,000 selectors on this list, approximately 600 of which were designated as RAS-approved without having undergone NSA Office of General Counsel (OGC) review as described in Section II.A.4.

(U) Remedial Steps

~~(TS//SI//NF)~~ NSA completely shut down the Activity Detection Process against the BR FISA metadata on 24 January 2009 as a corrective measure.

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

[4] ~~(TS//SI//NF)~~ As of 8 August 2006, queries of the BR metadata for telephone identifiers reasonably believed to be associated [redacted] were permitted by the Court. As of 14 June 2007, the authorization expanded again to include queries of the BR metadata for telephone identifiers reasonably believed to be associated with [redacted] associated terrorist organizations to include [redacted]

(U) Description

~~(TS//SI//NF)~~ As previously reported to the Court,[5] from May 2006 to 18 February 2009, NSA intelligence analysts who were working counterterrorism targets had access to a tool known as [redacted] which was used to assist them in determining whether or not a telephone identifier of interest was present in NSA's metadata repositories and, if so, what the level of calling activity was for that selector. Between these dates, [redacted] in turn, accessed the data present in the BR FISA metadata repository to assist in responding to these questions. [redacted] is not a tool used for contact chaining or [redacted]. Rather, for each query of a specific telephony selector, the [redacted] tool returns the number of unique contacts, the number of calls made, the dates of the first and last call events recorded in NSA's data repositories and the amount of time it took to process the query. It does not return the actual telephone identifiers in contact with the selector that serves as the basis for the analyst's query. Though [redacted] can be used as a stand-alone tool, it is more commonly invoked by other tools such as [redacted]

~~(TS//SI//NF)~~ On 19 February 2009, NSA confirmed that [redacted] performed queries against the BR FISA metadata repository using non-RAS-approved selectors. It was also confirmed that analysts who were not BR FISA-authorized inadvertently accessed BR FISA metadata without realizing it as a result of accessing [redacted]. The results returned from this tool did not identify to the user whether their results came from BR FISA or from metadata collected pursuant to NSA's authority to collect signals intelligence information under Executive Order (EO) 12333, but rather combined them into a consolidated summary.

(U) Remedial Steps:

~~(TS//SI//NF)~~ On 20 February 2009, NSA removed the specific system-level certificate (cryptologic authentication for software akin to a ticket used to confirm the bearer is entitled to enter) that had allowed the BR FISA-enabled [redacted] to access the BR FISA metadata chain repository.[6] Out of an abundance of caution, NSA also made software changes on 6 March 2009 which removed analysts' ability to manually invoke [redacted] against BR FISA metadata. While [redacted] could still automatically be

[5] ~~(U//FOUO)~~ See DIRNSA Supplemental Declaration dated 25 February 2009 at Section II.A. & B.

[6] ~~(TS//SI//NF)~~ The removal of the system-level certificate cut off all access to the BR FISA metadata chain repository by any automated process or subroutine. [redacted]

invoked via the Automated Chaining Analysis Tool (ACAT),[7] as stated, the revocation of the system level certificate prevented [redacted] from accessing the BR FISA metadata chain repository.

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

(U) Description

~~(TS//SI//NF)~~ Among the compliance issues previously reported to the Court[8] was NSA's discovery that between 1 November 2008 and 23 January 2009, three analysts inadvertently performed chaining within the [redacted] BR FISA metadata repository using 14 different telephone identifiers that did not meet RAS approval prior to the query. The analysts did not realize they were querying the BR FISA metadata and none of the identifiers was associated with a U.S. telephone number or person. Based on an audit of other queries the analysts were conducting at the same time, it appears each analyst thought he or she was conducting queries of other repositories of telephony metadata that are not subject to the requirements of the Business Records Order.

(U) Remedial Steps

~~(TS//SI//NF)~~ NSA implemented the Emphatic Access Restriction (EAR) to ensure that contact chaining [redacted] in the [redacted] BR FISA repository is restricted to only those seeds that have been RAS-approved [redacted] support personnel have conducted tests to ensure the EAR is functioning properly by monitoring manual query input and output, evaluating individual and connected functions, as well as examining log files to ensure the results of manual queries, now with the EAR in place, produce the desired results. Earlier NSA had also introduced a safeguard requiring the analysts to acknowledge that they were about to access the BR FISA metadata [redacted] to further reduce the potential for additional instances of non-compliance. More formal and rigorous training also emphasizes the need for caution when invoking their BR FISA authority. NSA is in the process of finalizing the testing of a software modification which will restrict the analysts to chaining no more than three hops from a RAS-approved selector within [redacted] BR FISA metadata repository.

~~(TS//SI//NF)~~ Internal audits of the activities of NSA personnel authorized to query the data under the 5 March 2009 order since 17 March 2009, when the Court approved the first batch of BR FISA metadata selectors as meeting the RAS standard, have shown no further compliance issues.

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

---

[7] ~~(U//FOUO)~~ The relationship between the tools [redacted] ACAT can be found in the Appendix, Glossary of Terms.

[8] ~~(U//FOUO)~~ See DIRNSA Supplemental Declaration dated 25 February 2009 at Section II.B.

(U) Description

~~(TS//SI//NF)~~ Between 24 May 2006 and 2 February 2009, NSA designated approximately 3,000 U.S. selectors as RAS-approved on the Station Table without undergoing the required OGC approval. This set of numbers was derived from two time periods: 1 January 2005 to 23 May 2006 and 24 May 2006 to mid-December 2008.

~~(TS//SI//NF)~~ Approximately 600 U.S. selectors that had been tipped to FBI and CIA between 1 January 2005 and 23 May 2006 as having ties to known, or probable, terrorist entities were added to the Station Table after the BR FISA Order was issued in an effort to "jumpstart" the BR FISA operations. These 600 U.S. selectors did not undergo OGC review.

~~(TS//SI//NF)~~ Between 24 May 2006 and 6 May 2009, NSA issued 277[9] BR FISA-based reports, all of which were based on contact chaining of RAS-approved selectors. Included in these reports were tips to customers (FBI, CIA, NCTC, and/or ODNI) of U.S. telephone numbers which had been in contact with a RAS-approved selector associated with [redacted] or were within three hops of a RAS-approved selector. For those reports issued between 24 May 2006 and mid-December 2008, NSA took the additional step of designating as RAS-approved in the Station Table the subset of these domestic selectors that were tipped as having ties to known, or probable, terrorist entities. However, these selectors did not undergo the required OGC review. For this entire period (24 May 2006 to 15 December 2008), the total number of U.S. selectors added to the station table as RAS-approved, but without the OGC review, was approximately 2,400.[10]

~~(TS//SI//NF)~~ At the time the RAS-approved portion of the Station Table was mistakenly implemented as the Activity Detection List in mid-January 2009, as described in Section

---

[9] ~~(TS//SI//NF)~~ The number of reports included in the DIRNSA Declaration of 13 February 2009 was 275. This was based upon information gathered on 6 February. 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. Since then, additional reports have been issued for a current total of 277 (as of 6 May 2009). The 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.

[10] ~~(TS//SI//NF)~~ Approximately 1000 of these selectors from the post-23 May 2006 era were reported to customers as having only an indirect connection to known or probable terrorist selectors. It was not NSA policy to include this category of numbers in the Station Table as "RAS-approved." However, an error was made during a bulk upload to the Station Table of tipped numbers on 9 December 2008 and these numbers were inadvertently included. They were present on the Station Table as RAS-approved until the entire set of 2,400 U.S. selectors were changed to "not RAS-approved" on 15 December 2008 (six days later). An audit of the Alert system, the [redacted] system and the Transaction Database showed that no chaining in the BR FISA metadata was performed on these numbers during this period.

II.A.1., approximately 600[11] of the U.S. selectors from the Table had not undergone the required OGC review. Forty-six of these approximately 600 selectors generated alerts as a result of the actions described in Section II.A.1; however, none of the resulting analysis based on these alerts yielded information that was subsequently tipped to customers.

~~(TS//SI//NF)~~ Designating these U.S. identifiers as RAS-approved without the required OGC review grew out of a related practice that NSA applied briefly to its development of the Telephony Activity Detection List in 2006. Specifically, in its first periodic report to the Court as directed in the initial May 2006 Order, NSA stated that U.S. identifiers that had been reported to FBI and CIA prior to 24 May 2006 because of their direct contact with international terrorism selectors had also been added to the alert list, even though they had not been qualified as seed identifiers and had not been reviewed by OGC. While the initial report explained to the Court the NSA rationale for the belief that these identifiers did not need to go through the full approval process to be included on the alert list, the November 2006 90-day report also stated that the practice had ceased as of 18 August 2006. Although the use of this process to add identifiers to the Alert List did cease on that date, NSA failed to discontinue the process of adding selectors to the Station Table.

(U) Remedial Steps

~~(TS//SI//NF)~~ In early February 2009, all selectors that the OGC had not reviewed were changed to *non*-RAS-approved on the Station Table.

B. (U) Newly Identified Areas of Concern

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

(U) Description

~~(TS//SI//NF)~~ January 2009 discussions between Oversight and Compliance (O&C) and the BR FISA-authorized analysts revealed that the [redacted], NSA's repository for individual BR FISA metadata one-hop chains, had not been audited, prompting further investigation as part of the end-to-end review. Prior to that time, NSA O&C was not aware of its existence in the technical architecture and therefore did not audit the database.

(U) Remedial Steps

~~(TS//SI//NF)~~ Between May 2006 and January 2009 [redacted] logging capability recorded all queries via the analyst graphical user interface

[11] ~~(TS//SI//NF)~~ These were the approximately 600 from the pre-FISA era; the others had been changed to "not RAS-approved" in mid-December 2008. The failure to remove these approximately 600 numbers was an oversight. The 600 selectors were changed to "non-RAS-approved" on the Station Table in early February 2009.

to the data within the [redacted] to include the user's login, Internet Protocol (IP) address, date and time, and retrieval request -- all fields required by the Order. Analysts use the [redacted] to verify the specific call event details between two individuals -- details such as which selector initiated each call, when the call was initiated and how long the call lasted. However, sometimes to verify the call details of a communication event the analyst uses the selector that was the first or second hop result as the retrieval request. Because of this, the selector that was the RAS-approved seed is not always evident in the [redacted]. In January 2009, NSA took steps to augment the information recorded in the [redacted] system log to include the RAS-approved seed that the user was asserting to be within two hops of the selector being queried. O&C began auditing queries to the database in February 2009. Since this enhanced auditing capability was added, O&C has audited the BR FISA-authorized intelligence analysts' queries and found no evidence of improper queries. Although the [redacted] suffered a system crash in September 2008, NSA was ultimately able to recover sufficient data to permit O&C to conduct sample audits of queries since the Order's inception. These sample audits revealed no unauthorized analysts conducted queries against the BR FISA metadata and no authorized analysts conducted improper queries of the metadata.

~~(TS//SI//NF)~~ As the [redacted] is outside the [redacted] architecture, it is currently not protected by the EAR. NSA will migrate [redacted] system functionality into the corporate architecture to provide greater accountability and to help ensure compliance with the Court Order and any future requirements. Reconstituting this database within the corporate architecture will ensure that it is established and supported on systems that use corporate authentication/authorization services, use system security and configuration management practices, are certified and accredited with approval to operate on an active System Security Plan (SSP),[12] and above all employ software measures that minimize compliance risks.

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

(U) Description

~~(TS//SI//NF)~~ As part of their Court-authorized function of ensuring BR metadata is properly formatted for analysis, data integrity analysts seek to identify numbers in the BR metadata that are [redacted] Once the data integrity analysts had identified such [redacted] selectors in the BR FISA data, they

[12] ~~(U//FOUO)~~ An SSP is a formal document describing the implemented protection measures for the secure operation of a computer system.

would not only take steps to prevent the selectors becoming part of the analysis in the BR FISA context, but would also note them as [redacted] selectors in other NSA systems in order to similarly prevent them from being included in analysis conducted outside the BR FISA context. NSA determined that the data integrity analysts' practice of populating [redacted] numbers in NSA databases outside the BR FISA 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 [redacted] 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 the BR metadata [redacted] A small number of [redacted] BR metadata business 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 selector of interest. Both [redacted] and the BR FISA-enabled [redacted] allowed analysts outside of those authorized by the Court to access the [redacted] number lists. The end-to-end review has not identified any other systems that have been fed using [redacted] numbers uncovered by the data integrity analysts from the BR FISA metadata.

~~(TS//SI//NF)~~ Similarly, in January 2004 [redacted] developed a 'defeat list' process to identify and remove [redacted] selectors deemed to be of little analytic value and that [redacted] In building defeat lists, NSA identified [redacted] selectors in data acquired pursuant to the BR FISA Order as well as in data acquired pursuant to EO 12333. When candidate [redacted] selectors contained in the BR FISA metadata were found to have a [redacted] obtained approval from the data integrity analysts to allow those selectors, which come from BR FISA metadata, to be added to the defeat list. This resulted in all references to those selectors being removed from all of [redacted] chain databases, to include the database containing and processing data acquired pursuant to EO 12333. Since August 2008, [redacted] had also been sending all selectors on the defeat list to the [redacted] A notice was filed with the FISC on these issues on 8 May 2009.

(U) Remedial Steps

~~(TS//SI//NF)~~ On 1 May 2009, NSA determined that the data integrity analysts' practice of populating [redacted] numbers in [redacted] and using BR FISA-enabled [redacted] to access this database was an area of concern. NSA immediately began quarantining the BR-derived identifiers in [redacted], completing the action by 2 May 2009. Access to the file containing the small number of BR-derived [redacted]

identifiers by the BR FISA-enabled [redacted] was shut off on 12 May 2009, when files created by the data integrity analysts were moved to a protected work file system.

~~(TS//SI//NF)~~ NSA determined that only eight selectors from the BR FISA metadata have ever been added to the [redacted] list. Starting in November 2008, [redacted] began to maintain separate defeat lists for BR FISA [redacted], and on 11 May 2009, [redacted] removed the eight BR FISA selectors from its [redacted] defeat list. The BR FISA defeat list will no longer be shared with [redacted] until this issue is resolved.

~~(TS//SI//NF)~~ As 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, NSA will work with DoJ to seek Court approval to continue such practices.[13]

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

(U) Description

~~(TS//SI//NF)~~ The end-to-end review revealed the fact that NSA's practice of using correlated selectors to query the BR FISA metadata had not been fully described to the Court. A communications address, or selector, is considered correlated with other communications addresses when each additional address is shown to identify the same communicant(s) as the original address [redacted]

~~(TS//SI//NF)~~ NSA analysts authorized to query the BR FISA metadata routinely used [redacted] to query the BR FISA metadata without a separate RAS determination on each correlated selector. In other words, if there was a successful RAS determination made on any one of the selectors in

---

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

[14] ~~(U//FOUO)~~ See Appendix 1, Glossary of Terms, for expansion and definition of [redacted]

the correlation, all were considered RAS-approved for purposes of the query because they were all associated with the same [redacted] account [redacted]

~~(TS//SI//NF)~~ Although NSA obtained [redacted] correlations from a variety of sources to include Intelligence Community reporting, the tool that the analysts authorized to query the BR FISA metadata primarily used to obtain the correlations is called [redacted]. A description of how [redacted] is used to correlate [redacted] was included in the government's 18 August 2008 filing to the FISA Court. While NSA previously described to the FISC the practice of using correlated selectors as seeds, the FISC never addressed whether [redacted] correlated selectors met the RAS standard when any one of the correlated selectors met the RAS standard. A notice was filed with the FISC on this issue on 15 June 2009.

(U) Remedial Steps

~~(TS//SI//NF)~~ The [redacted] - a database that holds correlations between selectors of interest, to include results from [redacted] was the primary means by which correlated selectors 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 ended the practice of treating [redacted] correlations as RAS-approved in manual queries conducted within [redacted], since the EAR requires each selector to be individually RAS-approved prior to it being used to query the BR FISA data. NSA ceased the practice of treating [redacted] correlations as RAS-approved within the [redacted] in conjunction with the March 2009 Court Order.

4. ~~(TS//SI//NF)~~ Handling BR FISA Metadata

(U) Description

~~(TS//SI//NF)~~ The results of the Homeland Security Analysis Center (HSAC) analysts' BR FISA metadata contact chaining queries have been routinely made available to the broader population of NSA analysts working [redacted] This sharing helps ensure that analysts with specific foreign target expertise can apply the full scope of their knowledge to the BR FISA-generated information to identify all possible terrorist connections quickly and characterize them within the context of the target's known activities. With only 20 HSAC analysts approved to query the bulk BR FISA metadata and more than one thousand analysts working various aspects of the counterterrorism mission enterprise-wide, fewer than two percent of counterterrorism

analysts currently have the authority to access the BR FISA metadata. Thus, the collective experience of the BR FISA-authorized analysts represents a small fraction of NSA's overall expertise on counterterrorism targets. CT target analysts beyond the small number currently authorized to query the BR FISA metadata are responsible for analyzing the data in the context of SIGINT information and writing reports; this practice continued under the structure imposed by the March Court Orders. NSA believed such internal sharing of the results of its analysis (as distinct from the bulk metadata itself) was consistent with the Court's Orders, but had not included a description of it to the Court in its periodic reports prior to May 2009 [redacted]

~~(TS//SI//NF)~~ In addition, the Court Orders prior to 2 March 2009 state that "any processing by technical personnel of the BR metadata acquired pursuant to this Order shall be conducted through the NSA's private network, which shall be accessible only via select machines and only to cleared technical personnel, using secured encrypted communications." The end-to-end review revealed that the way in which NSA protects the data is not precisely as stated in the Court Order; however we believe NSA's implementation *is* consistent with the intent of preventing unauthorized users from accessing the data. For example, there are not specifically designated or "select" machines from which technical personnel access and process the data on NSA's private, secure network. The internal NSA communications paths on its classified networks are not encrypted, but are subject to strong physical and security access controls[15] which provide the necessary protections.

~~(TS//SI//NF)~~ The end-to-end review also revealed that data integrity analysts, in order to conduct their authorized duties, pull samples of raw BR metadata into their private directories on the NSA network, which they access via username and password, to analyze the metadata in order to develop new parsing rules or prepare samples for spot checks. The private directories offered them a workspace to analyze the metadata using tools and applications that they could not invoke in the [redacted] While these private directories could be interpreted to be an additional data repository to the two [redacted] already described to the Court, the BR FISA data is not accumulated as in a true database repository. The data integrity analysts are authorized to access the data, and any importation to their own systems was deleted when no longer needed.

~~(TS//SI//NF)~~ Additionally, the review uncovered that data integrity analysts, in conducting their authorized duties, copied data into two shared directories created for

[15] ~~(TS//SI//NF)~~ The NSA complex is a Sensitive Compartmented Information Facility (SCIF) that is an accredited installation, incorporating strong physical and security access control measures (barriers, locks, alarm systems, armed guards), to which only authorized personnel are granted access. Within NSA, only approved users of NSANET can gain access to the network through login and password. Once on the network, the user can only access the BR FISA metadata if additional access controls specifically allow such access. Access to particular data sets is granted based on need-to-know and is verified via Public Key Infrastructure (PKI).

restricted information with a controlled user set. These shared directories also offered access to similar tools and applications as mentioned above. NSA learned that roughly 170 personnel who at one time had been cleared for sensitive metadata programs had access to files on this server. Approximately 15% of these personnel were system administrators or data integrity analysts; the remainder included intelligence analysts, managers and engineers. While it was possible for the files to be accessed by any of these personnel, it is unlikely that anyone other than data integrity analysts would have done so since it would have been outside the scope of their duties.

(U) Remedial Steps

~~(TS//SI//NF)~~ A notice was filed with the FISC on the matter of sharing results of queries within NSA as it relates to the BR FISA Order on 12 June 2009. While NSA believes the ability of BR FISA-authorized analysts to share unminimized query results with the broader population of NSA analysts working [redacted] is critical to the success of its counterterrorism efforts, effective 18 June 2009 NSA began the process of limiting access to unminimized BR FISA metadata query results to only authorized analysts. [redacted] the Court explicitly authorized the continuation of internal sharing of the results of authorized queries with NSA analysts other than the limited number authorized to access the bulk metadata, provided all analysts receiving such results receive appropriate and adequate training. The government anticipates seeking [redacted] in the BR FISA context.

~~(TS//SI//NF)~~ Regarding the handling of metadata by technical personnel, NSA implemented additional access controls using UNIX group access control which assured that only the data integrity analysts were in the "group" which could access this data, and is providing appropriate protected storage areas for the data integrity analysts' work files. With regard to the manner in which NSA secures the BR FISA metadata, NSA will work with DoJ to more accurately reflect in any future application to the Court the current method of providing protection. Instead of accessing the data via select machines using secured encrypted communications, NSA provides protection through the use of the secure network; use of NSA's identity and authorization access control service; and other NSA corporate standard data protection services.

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

(U) Description

~~(TS//SI//NF)~~ In its review of all tools and interfaces that allowed access to BR FISA metadata, NSA determined that developers assigned to work [redacted] a next generation metadata analysis graphical user interface (GUI) which is the replacement for [redacted] had queried BR FISA metadata chaining summaries 20 times during the course of their testing between 26 September 2008 and 11 February 2009. This access occurred due to the dual responsibilities of the

individuals involved. The developers of [redacted] also have maintenance responsibilities for 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 that were in place at the time of the queries, access to the BR metadata was unintentional and unknown to the developers at the time.

(U) Remedial Steps

~~(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 selector. 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. 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. The NSA O&C is notified each time anyone's permission to access the BR FISA metadata is changed and tracks these changes for compliance purposes.

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

(U) Description

~~(TS//SI//NF)~~ [redacted] NSA's mission element which obtains the BR FISA metadata from the providers, reported during the end-to-end review that [redacted] raised a question concerning whether certain foreign-to-foreign metadata it provides to NSA is subject to the terms of the BR FISA Order [redacted] This foreign-to-foreign metadata started coming into NSA in January 2007.

(U) Remedial Steps

~~(TS//SI//NF)~~ When the provider began providing NSA with foreign-to-foreign metadata in January 2007 [redacted] The Court is now aware of this issue, and the Court's 29 May Order specifically excludes from its scope the aforementioned foreign-to-foreign metadata. The provider ceased providing this metadata on the same day as the Order was signed. NSA is coordinating with the provider and the NSD/DoJ to resolve this matter.

7. ~~(TS//SI//NF)~~ Unintentional Omission of OGC Review of U.S. Identifiers

(U) Description

~~(TS//SI//NF)~~ It was recently discovered that during the June through October 2006 timeframe, in the process of implementing the initial BR FISA Orders, a few domestic numbers were designated as RAS approved and chained without OGC approval due to compound analyst errors. These errors occurred when analysts inadvertently selected the incorrect option in a GUI. The correct option would have designated the domestic identifier as needing OGC approval. The incorrect option put the domestic selector into a large list of foreign selectors which did not need OGC approval as part of the RAS approval process. In those cases where the Homeland Mission Coordinator (HMC) failed to notice the domestic number in the large list of foreign selectors and the RAS justification was approved, the number was chained. NSA continues to investigate this matter, but, based on available records, NSA's initial estimate is this occurred fewer than ten times. NSA will provide additional information as appropriate. A notice was filed with the FISC on this issue on 29 June 2009.

(U) Remedial Steps

~~(TS//SI//NF)~~ Each time an error was identified through quality control, senior HMCs provided additional guidance and training, as appropriate. Continued training and management oversight, in particular when new analysts arrived, helped ensure such errors were not repeated.

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

(U) Description

~~(TS//SI//NF)~~ In examining NSA's practice of sharing BR FISA metadata query results internally with other NSA analysts working authorized [redacted], NSA learned of CIA, FBI, and NCTC analyst access to unminimized BR FISA metadata-derived query results and target knowledge information via an NSA counterterrorism database. This matter, just recently identified, was a collaboration practice that was in place prior to the inception of the BR FISA Court Order. Over time, approximately 200 analysts at CIA, FBI, and NCTC had been granted access to this target knowledge base. When the BR program was brought under the jurisdiction of the FISA Court, this practice was not modified to conform with the Order's requirements for the dissemination of BR FISA metadata-derived query results outside of NSA. A notice was filed with the FISC on this matter on 16 June 2009.

(U) Remedial Steps

~~(TS//SI//NF)~~ While NSA disabled the hyperlink button used by the external analysts to access this target knowledge database in the Summer 2008 timeframe, NSA learned that the external analysts could have still accessed the data if they retained the URL address.

Upon identifying this as an area of concern on 11 June 2009, NSA began terminating external customer account access to the target knowledge database, completing the action by 12 June 2009. NSA is continuing to investigate this matter; audits are now underway to determine the extent to which the query results may have been accessed. Once completed, NSA will provide a full explanation of this practice.

9. ~~(TS//SI//NF)~~ Dissemination of BR FISA Information

(U) Description

~~(TS//SI//NF)~~ When an NSA analyst determines that information identifying a U.S. person is critical to include in a metadata report, he or she is required to obtain dissemination authorization from the designated NSA approving office in accordance with the Court's Order. Specifically, the order requires that prior to disseminating any U.S. person information outside of the NSA, the Chief of Information Sharing Services must determine that the information is related to counterterrorism information and is necessary to understand the information or to assess its importance. In fact, the Chief of Information Sharing Services, when unavailable, has in the past delegated this authority, typically to the Deputy Chief. Additionally, after hours or in an emergency situation, this authority has also been delegated to NSA's Senior Operations Officer (SOO) in its National Security Operations Center (NSOC).

~~(TS//SI//NF)~~ The practice of sharing BR FISA metadata analytic results also applied to [redacted] process which was established to facilitate sharing of sensitive metadata among NSA's [redacted] Queries, called Requests for Information (RFIs), submitted to the [redacted] were disseminated to all the partners for response. Only those RFIs that the [redacted] determined were answerable by NSA were forwarded to the HSAC. HSAC queries in response to the RFIs were only performed against valid RAS-approved selectors. The [redacted] standard operating procedure was to minimize HSAC's results and then merge them with the results of [redacted] with any sourcing information sanitized. Of the 12 RFIs sent to HSAC from the [redacted] etween 2007 and 2008, HSAC affirmatively responded to only four. The [redacted] in turn, provided the results of one[16] of these RFIs, in a sanitized format, back to the [redacted] requestor. While the query results were sanitized to remove information regarding the collection source, it was recently discovered that two U.S. telephony identifiers derived from BR FISA metadata analysis results were inadvertently shared, without being minimized by NSA, with the [redacted][17] As it was not [redacted] practice to disseminate unminimized U.S. person information, obtaining dissemination authorization from the designated NSA approving office was not part of their process.

(U) Remedial Steps

[16] ~~(U//FOUO)~~ The RFI response *is not* a subset of the 277 reports discussed earlier in Section II.A.4.

[redacted]

~~(TS//SI//NF)~~ NSA is currently conducting a review of any BR FISA metadata-derived reports that contained U.S. person identifying information to determine consistency with the Court's Order. Once this is completed, the results will be provided.

[redacted]

III. ~~(U//FOUO)~~ NSA's End-to-end BR FISA Review

A. (U) Scope

~~(TS//SI//NF)~~ NSA established a team of experts to conduct a thorough end-to-end systems engineering and process review of the BR FISA metadata workflow. The team reviewed 93 requirements extracted from the March 2009 BR FISA Court Order, Application and Declaration; dataflow diagrams; and system documentation (to include systems engineering and security plans) to ensure a complete understanding of how the requirements were being met prior to 2 March 2009, how well they are currently being met, and what changes may be needed to ensure compliance. The team then used these requirements as a basis to examine six key aspects (systems architecture, analyst workflow, management control, compliance auditing, oversight, and training) of NSA's handling of BR FISA metadata, and to establish a comprehensive plan to ensure that all requirements are addressed and properly implemented.

~~(TS//SI//NF)~~ Another critical step in preparing to conduct the end-to-end review was to identify and map how all the system components fit together. Lack of such end-to-end awareness contributed to the problems initially reported to the FISC.[18] The systems/processes reviewed were:

1. [redacted]
2. [redacted], NSA's corporate file transfer/distribution system
3. [redacted], NSA's corporate contact chaining system
4. [redacted], NSA's repository for individual BR FISA metadata one-hop chains
5. the Telephony Activity Detection (Alerting) Process
6. the Reasonable Articulable Suspicion (RAS) Approval Process
7. the BR FISA Analytic Tools and Processes
8. the BR FISA Analyst Decision and Reporting Process.

---

[18] ~~(U//FOUO)~~ See Declaration of the Director of the National Security Agency (DIRNSA) dated 13 February 2009.

~~(TS//SI//NF)~~ The interaction of these systems and processes can be summarized as follows (see Figures 1 and 2): [redacted] Both of these databases are accessible to BR FISA-authorized intelligence analysts. These analysts also use the following processes: the *Activity Detection (Alerting) Process*, the *RAS Approval Process*, the *BR FISA Analytic Tools/Processes*, and the *BR FISA Analyst Decision/Reporting Process* to identify, query, analyze and ultimately disseminate information derived from the metadata. These eight components, part of a large and complex system, are further described in Section III.C. and pictured in Figures 1-10. Figure 1 provides a top-level view of the overall architectural system, Figure 2 highlights the eight components, while Figures 3-10 highlight each of the individual components in greater detail. Each component is reflected with corresponding colors in the diagrams.

~~(TS//SI//NF)~~ In concert with this systems engineering end-to-end review, NSA conducted a thorough review of its analytic processes, management controls, auditing mechanisms, oversight and training for the BR FISA metadata handling. This included a thorough examination of each activity, tool and analytic process to assure that it operated in compliance with the Court Order. The review led to several additional audits to ensure that no compliance incidents had occurred and to examine whether or not the individuals who worked with the BR FISA metadata fully understood the applicable authority and limitations. Documentation and training were also updated. Each part of the review compared the component or process being reviewed with the relevant requirement from the list extracted from the Court documents.

~~(TS//SI//NF)~~ NSA's systems engineering and workflow reviews surveyed the processes and tools as they existed before any remedies were implemented. This retrospective evaluation enabled NSA to develop the near-term corrective measures necessary for current Court-approved operations and potential resumption of regular access to the BR FISA metadata should it be authorized by the Court. It also informed plans for incorporating the BR FISA flow into the NSA future architecture more effectively.

B. (U) Methodology:

~~(TS//SI//NF)~~ NSA employed a repeatable and well-documented process in conducting its end-to-end review. NSA derived technical requirements from the legal requirements governing BR FISA metadata handling. As noted, NSA simultaneously began to develop an end-to-end systems engineering diagram of the systems and databases that support BR processing and storage. NSA also developed and conducted Initial Privacy Assessments (IPAs) which include a standard set of questions used to determine, among other things, whether the system or process under review interacts with data that could contain information about U.S. persons. The outcome of the IPA determines whether a more in-

depth Privacy Impact Assessment (PIA)[19] is required to fully explore the extent of interaction and whether any privacy compliance concerns exist. An IPA was conducted for any system or process identified as potentially part of the BR FISA metadata end-to-end data flow. For those systems confirmed to be in contact with BR FISA metadata via the IPA, a PIA was performed. The results of the IPAs and PIAs were then compared against the Court-derived requirements to determine the level to which each requirement was satisfied. For any system or process for which there was concern, NSA is developing well-documented, fully-tested corrective solutions should the Court decide to allow NSA to resume its regular access.

C. (U) Results:

1. ~~(U//FOUO)~~ [redacted]

~~(TS//SI//NF)~~ [redacted] receives BR FISA metadata from [redacted] in bulk. Upon receipt, [redacted] sorts and labels the data according to data source and type, and determines the necessary routing path that is to be used for the different data types. [redacted] does not derive, process or create new data from this data set.

~~(TS//SI//NF)~~ Except for the provider issue identified in Section II.B.6, NSA identified no other significant issues in [redacted] receipt or handling of the BR FISA metadata [redacted]

2. ~~(U//FOUO)~~ [redacted]

~~(TS//SI//NF)~~ [redacted] NSA's corporate file forwarding service, provides for distribution of the BR FISA metadata from the collection source to the analytic repositories. It accepts files from sources and transports those files to the end destinations identified in the filename given to the file by the source system.

[19] ~~(C//REL TO USA, FVEY)~~ The IPA/PIA framework provided a way for the Agency to assess compliance risk. This framework was not used to supersede any Court-derived requirements. Both the IPA and PIA templates were based on Department of Defense (DoD), DoJ or Homeland Security Privacy Assessment frameworks and then adjusted for the SIGINT environment. While IPAs and PIAs are not required for the Intelligence Community, they provided a sound methodology for the systems engineering end-to-end review.

~~(TS//SI//NF)~~ [redacted] is configured to allow dataflows and system accesses by technical personnel to be monitored and logged. The [redacted] system has security controls that are documented across multiple SSPs. [redacted] employs security access controls, such as PKI, to verify users and their system level access and likewise employs file transfer controls[20] to verify file transfer access, file source and file destination. The [redacted] system also employs a stringent configuration management methodology such that software changes cannot be implemented without the required testing and approval.

3. ~~(U//FOUO)~~ [redacted]

~~(TS//SI//NF)~~ [redacted] NSA's corporate contact chaining system, accepts metadata from multiple sources. It accepts the BR FISA metadata files from [redacted] stores the raw metadata in a separate realm, performs data quality, preparation and sorting functions; and then summarizes contacts represented in the processed data. [redacted] stores the resulting contact chains and provides analysts with access to these contact chains.

~~(TS//SI//NF)~~ The [redacted] portion of the end-to-end review demonstrated that the system is now providing the necessary protection of the BR FISA metadata while it is in the [redacted] domain given the added protection provided by the implementation of the EAR and the removal of the system level certificates. [redacted] has always employed other access controls, system security and configuration management practices for ensuring appropriate protection of the BR FISA metadata residing in its database and accessed by authorized analysts. They include, but are not limited to, a fully certified and accredited system under a System Security Plan and effective use of corporate authentication and authorization service.

~~(TS//SI//NF)~~ As stated earlier, NSA installed the EAR on 20 February 2009 in response to a compliance issue previously reported to the Court.[21] Prior to the EAR, NSA was relying on analytic due diligence to query [redacted] with only RAS-approved selectors. The EAR, via internal software system controls, now ensures that manual contact chaining is restricted to only those seeds that have been RAS-approved by the Court by preventing a non-RAS-approved selector from being used as a seed for conducting call chaining [redacted] of the BR FISA metadata in the [redacted] repository. In addition, NSA removed the system level certificate that had been used by automated tools to access the BR FISA metadata. In so doing, NSA disabled all automated querying of the BR FISA metadata. Access to the BR FISA metadata chaining information in [redacted] is strictly controlled via individual user access authentication/permission and this access is logged in accordance with the current BR FISA Court Order.

[redacted]

[21] ~~(U//FOUO)~~ See DIRNSA Supplemental Declaration dated 25 February 2009.

(TS//SI//NF) The implementation of the EAR had an unintentional adverse impact on the technical support mission of NSA's BR FISA-authorized data integrity analysts. Prior to the addition of the EAR, these analysts frequently queried [redacted] Contact Chaining Database for the limited purpose of verifying their parsing rules (a method for separating data into standardized data fields). Analysts composed these rules for [redacted] BR FISA metadata to determine whether the system output represented accurate connections between communicants. In so doing, the data integrity analysts queried [redacted] using both RAS and non-RAS-approved selectors, as they were authorized to do. This type of querying is especially important when a new data format is received from one of the providers. Once the EAR was put in place, these analysts could only query the database using a RAS-approved selector. This diminishes their ability to test and evaluate their parsing rules. NSA is finalizing testing of a technical solution to create an EAR-bypass capability solely for the data integrity team. The existing impaired ability of the data integrity analysts is assessed as a system performance vulnerability, as it could result in improperly formatted data.

(TS//SI//NF) While the EAR restricts the ability to query the [redacted] Contact Chaining Database to only RAS-approved seeds, there is no similar technical restriction to prevent a BR FISA-authorized analyst from chaining beyond the Court-mandated three hops from a RAS-approved selector. NSA is finalizing testing of a software modification to provide this contact-chaining hop restriction. In the meantime, training and management oversight ensure that contact chaining is executed in accordance with the Court Order.

(TS//SI//NF) The end-to-end review also identified the fact that [redacted] incorporated a defeat list including BR FISA-derived selectors to manage data ingest volumes more effectively. The inclusion of BR FISA-derived selectors on this list is described more fully in Section II.B.2.

4. (U//FOUO) [redacted]

(TS//SI//NF) [redacted] is used by authorized BR FISA analysts to view detailed data about specific calling events. As the [redacted] Contact Chaining Database only contains summaries of one-hop chains (i.e., selector 1 was in contact with selector 2 - N times within a specific timeframe), [redacted]

(TS//SI//NF) The end-to-end review revealed an area of concern resulting from the fact that queries within the [redacted] had not been audited, as described in Section II.B.1. As previously noted, subsequent audits showed no indication of unauthorized access to the [redacted] metadata or of any improper querying of the [redacted]

~~(TS//SI//NF)~~ The review also identified other system weaknesses. First, insufficient documentation and configuration management (the ability to track versions) exist to ensure that no unauthorized or unintended changes can be made that would make the system non-compliant. Second, although it is attached to the [redacted] network, the [redacted] is not afforded the additional protection of [redacted] although access to the database is strictly controlled. Third, the [redacted] is not protected by the EAR, thus there are no technical measures in place to prevent a BR FISA-approved analyst from querying the metadata using a non-RAS-approved selector or one that is not within two hops of a RAS-approved selector. To prevent improper manual queries of metadata [redacted] using non-Court-approved selectors, NSA has provided enhanced training to authorized analysts and is conducting regular audits of queries. Additionally, analysts using [redacted] see a pop-up window reminding them to use only RAS-approved selectors for queries and limit their chaining to the Court-approved number of hops.

~~(TS//SI//NF)~~ NSA is preparing to incorporate the [redacted] into the NSA corporate architecture. This transition to the corporate engineering framework will maximize use of the latest technologies and proven configuration management to minimize any security and compliance risks. In the interim, NSA is addressing these vulnerabilities through improved training, competency testing and increased management oversight.

5. ~~(U//FOUO)~~ Telephony Activity Detection (Alerting) Process

~~(TS//SI//NF)~~ The Activity Detection (Alerting) Process identified when a selector on the Activity Detection List was in contact with an incoming number in a given day's BR metadata when that contact originated or terminated in the U.S. This notification, in turn, allowed analysts to prioritize their follow-on analysis. If the RAS standard was met on the selector, the system performed automated contact chaining in the BR FISA metadata archive to identify and track terrorist operatives and their support networks both in the U.S. and abroad. If not, a notification was made to NSA personnel so that they could determine whether to attempt to satisfy the RAS standard, which would then allow such contact chaining to take place manually.

~~(TS//SI//NF)~~ As noted in Section II.A.1., the Activity Detection List consisted of telephony selectors [redacted] that had been RAS evaluated as well as selectors that had never been RAS evaluated. The original Activity Detection List was built from two sources; one was called the "Address Database," which was a master target database of foreign and domestic telephone identifiers that were of current foreign intelligence interest to counterterrorism personnel. The second source was [redacted] which was and continues to be a database NSA uses as a selection management system to manage and task identifiers for SIGINT collection. One of the features of [redacted] is that it is enriched with correlations of telephony identifiers associated with numbers tasked to the SIGINT system. This enrichment is enabled by [redacted], which is a

database used to store correlations between selectors [redacted]

~~(TS//SI//NF)~~ The Telephony Activity Detection Process is not currently operational as the result of the compliance issue previously reported to the FISC[22] and as described in Section II.A.1 of this report. NSA shut down the Activity Detection Process entirely on 24 January 2009 as a corrective measure. (Of note, under the prior implementation before contact chaining could take place in the complete body of archived metadata and before any results of such analysis were disseminated, the alerting selector had to satisfy the RAS standard and be approved explicitly as having done so.) This process was thoroughly examined in the course of the end-to-end review and consequently a revised implementation, as described in Section V.A., has been proposed should the Court approve resumption of regular access.

6. ~~(TS//SI//NF)~~ RAS Approval Process

~~(TS//SI//NF)~~ The RAS Approval Process is the mechanism by which an analyst must be able to articulate some fact or set of facts that causes him or her to suspect in light of the totality of the circumstances that a particular number is associated with [redacted] before he or she may use a telephone number or electronic identifier as a seed to query the BR FISA metadata.

~~(TS//SI//NF)~~ The RAS Approval Process in place until 2 March 2009 (the date of the FISC Order) incorporated a combination of documented guidance and well-understood procedures as outlined in the OGC RAS Memo and the analytic office's RAS Working Aid. During the three years that DoJ has reviewed NSA RAS approvals, no spot check has revealed a faulty RAS approval decision.

7. ~~(TS//SI//NF)~~ BR FISA Analytic Tools and Processes

~~(TS//SI//NF)~~ The BR FISA Tools were designed to analyze the raw BR FISA metadata as well as the output of analytics such as [redacted] contact chaining. Analysts used these tools against the BR FISA metadata and chaining results to identify possible terrorist communications into, from and within the US.

~~(TS//SI//NF)~~ Two instances of concern related to the analytic tools and processes used by the BR FISA-authorized intelligence analysts were identified through the end-to-end review and are described in Sections II.A.2. and II.B.3. These tools and processes, which were designed to function against both the BR FISA metadata and other categories of telephony metadata that NSA acquires through SIGINT operations authorized under the general provisions of EO 12333, were used primarily by analysts within NSA's Office of Counterterrorism to identify possible terrorist connections into, from, and within the U.S., as well as foreign-to-foreign communications. Twelve of the 19 analytic tools examined

---

[22] ~~(U//FOUO)~~ See DIRNSA Declaration dated 13 February 2009

were developed under [redacted] systems architecture and are well-documented, configuration-controlled and audited. The other seven BR FISA analytic tools examined were developed in whole or in part by engineers working in the Counterterrorism Organization to meet constantly changing mission requirements, resulting in limited configuration and change management control. All seven of these tools were either monitored through existing O&C audits or were subjected to new audits and/or reviews as part of the end-to-end review. With the exception of [redacted] and GUI, none of these tools are currently able to access the BR FISA metadata.

~~(TS//SI//NF)~~ To mitigate risk in the future, NSA will transition the BR FISA analytic tools and processes to the corporate NSA enterprise architecture and will no longer develop tools within the Office of Counterterrorism. Complete end-to-end testing will be conducted for all tools against a standard set of BR FISA requirements to ensure they are fully compliant prior to resumption of automated operations if authorized by the Court.

8. ~~(U//FOUO)~~ Analyst Decision and Reporting Process

~~(TS//SI//NF)~~ The Analyst Decision and Reporting Process encompasses the target knowledge, guidelines and procedures that enable intelligence analysts to determine what information meets customer requirements. It also involves the evaluation and minimization procedures intelligence analysts employ when analyzing data and drafting and disseminating reports.

~~(TS//SI//NF)~~ Prior to the alert list shutdown on 24 January 2009, the BR FISA analyst decision and reporting work flow began when an HSAC analyst was notified of a match between a known selector of counterterrorism interest and an identifier in the ingested BR FISA metadata, when an analyst received an RFI from a customer, or when an analyst was continuing analysis on an existing target set. Aside from the activity detection list, the process remains the same today on selectors that are specifically approved in accordance with the Court's Orders. If NSA has reason to believe the information constitutes valid threat-related activity, NSA applies USSID 18 to minimize information concerning U.S. persons and then reports the information to the FBI, CIA, NCTC and ODNI, and other customers, as appropriate.

~~(TS//SI//NF)~~ NSA reviewed its analytic workflow to ensure the BR FISA metadata was appropriately handled, analyzed and disseminated. Three new areas of concern, discussed in Section II.B, were identified with the BR FISA Analysis Decision and Reporting Process in addition to that which was previously described to the Court[23] and discussed in Section II.A.

[23] ~~(U//FOUO)~~ See Supplemental DIRNSA Declaration dated 25 February 2009, at 8, Section 2 (Inappropriate analyst querying).

~~(TS//SI//NF)~~ As a by-product of the end-to-end review, NSA has updated the interim analytic BR FISA Standard Operating Procedures (SOP) to ensure compliance with the current Court Orders and is coordinating this document with DoJ as required by the Court. This SOP outlines step-by-step instructions for the authorized intelligence analysts in handling the BR FISA metadata; describes the procedures used to control access to the BR FISA metadata; provides the steps used to conduct weekly audits of the analysts' queries and tools; and details the methodology used to query the BR FISA metadata under newly established Imminent Threat Concept of Operations guidelines. NSA will continue to maintain the SOP and CONOP as "living documents" and update them as needed.

~~(TS//SI//NF)~~ NSA also continues to maintain and regularly update an 11-step comprehensive checklist that outlines both the Homeland Mission Coordinator and analyst responsibilities in the BR FISA metadata analysis and reporting process. The checklist is comprised of over 30 components that require analysts to answer a variety of questions, including whether the proposed report falls within the scope of BR FISA authorities and express OGC guidelines; whether NSA attempted to get additional information about the selector from the FBI and CIA integrees at NSA; and whether cellular identifiers were checked to determine if the user had roamed into another country. The checklist also reminds analysts to detail the information/intelligence source(s) that prompted the report's production.

~~(TS//SI//NF) In~~ addition, NSA has in place a combination of web pages and on-line aids dedicated to end-product reporting and dissemination guidance. These detailed working aids, together with required USSID 18 training for all BR FISA-approved intelligence analysts, require that any NSA BR FISA-based reporting that contains U.S. person information follow NSA's standard minimization procedures found in USSID 18 and the Court Order.

IV. ~~(U//FOUO)~~ NSA's Minimization and Oversight Procedures

~~(TS//SI//NF)~~ NSA has well-documented and long-standing minimization procedures for ensuring protection of U.S. persons' information in SIGINT analysis and reporting under all SIGINT authorities, to include the FISA Order. NSA's normal regime of compliance oversight for handling the BR FISA is a comprehensive, multi-pronged approach involving DoJ and NSA's OGC, O&C, Office of the Inspector General and SID. Currently, NSA is required to consult with DoJ on all significant legal opinions involving BR FISA metadata handling. DoJ meets with the appropriate NSA representatives at least once every renewal period to review the program. Prior to the 2 March Court Order that the FISC make all RAS determinations, DoJ also conducted "spot checks" to review a sampling of justifications (RAS determinations) for querying the metadata. NSA, in turn, provides internal oversight to the BR FISA program by a variety of oversight controls and compliance mechanisms to prevent, detect, correct and report incidents and violations of the procedures, to include technical, physical and managerial safeguards such as: examining samples of call-detail records to ensure NSA is receiving only compliant data; ensuring analysts are trained in the querying, dissemination and storage

restrictions for the metadata; monitoring analytic access to the metadata; auditing queries on a weekly basis by O&C; monitoring audit functionality; reviewing the BR FISA raw database repositories; and examining the list of RAS-approved selectors.

~~(TS//SI//NF)~~ In light of the compliance issues that surfaced specific to the handling of the BR FISA metadata, NSA reviewed its minimization procedures as well as its oversight procedures, to include auditing, documentation, and training, to identify areas for potential improvement. All were identified as areas for enhancement to ensure that personnel handling the BR FISA metadata are aware of and compliant with the Court Orders governing its use and dissemination.

A. (U) Minimization

~~(TS//SI//NF)~~ Every NSA intelligence analyst is required to complete training and pass a test on USSID 18 minimization procedures every two years as a pre-requisite for access to unminimized/unevaluated SIGINT data. Additionally, intelligence analysts must receive an OGC compliance briefing and on-the-job training (OJT) regarding their responsibilities for handling metadata containing U.S. person information prior to being granted access to the BR FISA metadata. They also have on-line access to detailed working aids including required minimization procedures. NSA will continue to emphasize the critical importance of applying USSID 18 and the Court Order requirements as they relate to the handling and dissemination of BR FISA.

B. (U) Oversight

1. ~~(U//FOUO)~~ Oversight Auditing Mechanisms

~~(TS//SI//NF)~~ NSA assessed requirements for auditing of systems, tools, processes and analyst queries to ensure the proper compliance procedures were in place. A total of 13 audits related to BR FISA metadata access and querying were conducted either as the result of standing requirements or in response to issues identified through the end-to-end review. Descriptions of resultant anomalies are captured in Section II.

~~(TS//SI//NF)~~ NSA audits samples of queries conducted by BR FISA-authorized intelligence analysts and data integrity analysts in the [redacted] on a weekly basis. As a result of a review of its oversight processes, O&C created a dedicated senior intelligence analyst position to enhance auditing of BR FISA metadata queries.

2. ~~(U//FOUO)~~ Oversight Documentation and Procedures

~~(TS//SI//NF)~~ Oversight documentation and procedures governing BR FISA metadata handling consists of a set of SOPs that have been reviewed and revalidated. They are as follows:

- **"Access":** This SOP outlines the procedures for gaining and maintaining access to the BR FISA metadata in a way that is compliant with the BR FISA Court Order.
- **"BR FISA Audit Procedures":** This document outlines the procedures used to audit BR FISA analyst queries [redacted].
- **"Compliance Notification":** This document addresses the procedures to be followed when compliance issues are noted.
- **"DoJ and OGC Spot Checks":** This SOP addresses the procedures to be followed for the required, regular DoJ and/or OGC spot checks.
- **"Oversight":** This document outlines the roles and responsibilities of the DoJ, the NSA Director, the OGC, O&C, the Inspector General, [redacted] and those Counterterrorism Organization analysts approved for BR FISA metadata access.

3. (U) Oversight Training

~~(TS//SI//NF)~~ NSA's Associate Directorate of Education and Training (ADET) had already been working with O&C and OGC to redesign the required training for accessing BR FISA metadata to better enforce appropriate handling of this data and to introduce competency testing as part of the O&C curriculum. The curriculum will be administered on-line to allow students 24/7 access to the course material.

~~(TS//SI//NF)~~ The redesigned BR FISA portion of the training package addresses the knowledge and procedural components of handling BR FISA data, and now requires the analyst to read the most current Court Order and the OGC instructions, and in the future will require them to view an OGC video briefing about the BR FISA program and complete the following six lesson tutorials:

1. "Overview of the Reasonable Articulable Suspicion standard," as covered in OGC instructions
2. "Summary of the RAS standard," to aid NSA analysts in preparing RAS justifications
3. "Association with [redacted] to identify how associations are established in order to qualify a target for RAS justification
4. "First Amendment Considerations," to identify limitations and considerations when targeting U.S. persons within BR FISA data
5. "Sources of information," to identify the supporting information used to justify the RAS determination
6. "The BR FISC Order," which explains the content of the BR FISA Orders

~~(TS//SI//NF)~~ A computer-based competency examination will be administered upon completion of this training and remediation will be provided for missed questions. Once an analyst has demonstrated the necessary knowledge by successfully passing the exam, he or she will complete formalized OJT before O&C grants access to the data.

~~(TS//SI//NF)~~ The OJT component has always been administered by an experienced HMC or senior analyst experienced in conducting OJT. This training specifically addresses how analysts are permitted to use the BR FISA metadata, reinforces the unique privacy concerns and handling requirements of this data, and demonstrates the various tools that can be used to query the BR FISA metadata. In addition, each HMC and authorized intelligence analyst is required to sign a user agreement, documenting that he or she has read and understands the obligations associated with handling the BR metadata.

~~(TS//SI//NF)~~ NSA has also begun to provide tailored briefings to all technical personnel that have been granted access to the BR FISA metadata. The tailored briefings outline the categories of data obtained under the BR FISA Court Order and the restrictions associated with the technical personnel's duties. For example, the briefings make it clear that the Collection Managers and System Administrators are not authorized to query the BR FISA metadata for foreign intelligence purposes. The briefing also outlines the correct offices to contact if the technical personnel see possible compliance issues in the course of their duties.

~~(TS//SI//NF)~~ As part of the BR FISA training redesign, complete training records will be maintained by ADET for each individual. The documentation will include the test score, answers to individual test questions, and performance feedback from the OJT component. This documentation will allow for tracking of access to the BR data on an individual basis.

V. ~~(U//FOUO)~~ NSA's Future Architecture

~~(TS//SI//NF)~~ Using principles of system engineering, configuration management and access control, NSA has considered the future implementation of the BR FISA program including the automated activity detection process to be used should the Court authorize NSA to resume regular access to the BR FISA metadata.

A. (~~U//FOUO~~) Future BR FISA Activity Detection (Alerting) Process

~~(TS//SI//NF)~~ NSA could resume automated activity detection in a fully compliant manner should the Court approve. NSA would maintain an Activity Detection (alert) List containing *only* RAS-approved selectors. Only the RAS-approved selectors on this "BR Identifier List" would be compared to the BR FISA metadata. With Court approval to resume automated querying, NSA will work with NSD/DoJ to ensure the BR Identifier List will be populated with only those selectors that the Court has authorized. Should the Court grant NSA RAS decision authority, NSA would begin to augment the BR Identifier List with additional identifiers that NSA approves as having satisfied the RAS standard, using the improved processes and training identified in this document.

B. (U) Future of Overarching Architecture

~~(TS//SI//NF)~~ In the future, should the Court authorize NSA to resume regular access to the BR FISA metadata, NSA will migrate the dataflow and life cycle management of the BR FISA metadata to its next generation system architecture which offers more effective and efficient management and control. This architecture is designed to be flexible enough to adapt to changes in the legal and oversight requirements, while conforming to applicable governing authorizations such as EO 12333 and BR FISA.

~~(U//FOUO)~~ In the future architecture, the end-to-end BR FISA dataflow will be referred to as a system "thread." As such, NSA would manage the entire capability via a "Thread Engineering Team" to guide the requirements development, systems integration, use-case development, testing/validation and planning for current and future enhancements. Thread engineers would meet with representatives from the OGC and O&C to define and validate requirements prior to development. System-wide configuration management would be implemented to log the expected software builds and patches. Such practices exist now, but there is no thread focused on the Business Records process.

~~(TS//SI//NF)~~ The proposed systems supporting BR FISA dataflow and life cycle within the next generation architecture encompass both technical- and personnel-based strategies to ensure that data is accessed, retained and purged in full compliance with authorities granted to NSA by the FISC. Moreover, the implementation of centralized processes and databases will ensure that all aspects of the dataflow will continue to be tracked and audited to further ensure that any non-compliance issues can be promptly identified and addressed. Plans for addressing key requirements for BR FISA metadata are as follows:

1. **~~(U//FOUO)~~ Security / Access Control**

~~(TS//SI//NF)~~ A new access control application will be applied to all databases and systems supporting the BR FISA workflow. This application will validate the credentials of users to govern what systems they are approved to access, and validate that their required training is current. PKI, which offers security measures for identification and authentication, as well as for access control, and audit capability will be used to manage users with access to the raw data or query results.

2. **~~(U//FOUO)~~ Data Standardization**

~~(TS//SI//NF)~~ A data standardization platform will date-stamp the incoming BR metadata and ensure its consistent and accurate structure. This will allow quick and accurate date-based purging once the Court-ordered time frame has been reached.

3. **~~(U//FOUO)~~ Databasing RAS Selectors**

~~(TS//SI//NF)~~ An updated and improved centralized target knowledge database for storing telephony and email selectors has been under development since October 2008. This database will enable more efficient storage and retrieval of key information about each BR FISA telephony identifier such as its RAS status and the justification and OGC

approval as appropriate, for those that have been RAS-approved. These features are scheduled for completion during the fourth quarter of FY09.

4. ~~(TS//SI)~~ **Analytical Processing and Call Chaining**

~~(TS//SI//NF)~~ An enhanced call chaining function and data processing capability will support large volumes of automated algorithms, handle growing ingest rates and deliver faster query responses. Additionally, the metadata will be stored using security tags, a measure which can be used to restrict the visibility of individual entries in the database to personnel with the appropriate access credentials.

5. ~~(U//FOUO)~~ **Auditing and Monitoring**

~~(U//FOUO)~~ Enhanced auditing will provide a means to track a data user's activity patterns, the state of a user's operations, and the frequency and composition of queries. A formal metrics and monitoring system will also be used to monitor the status of the end-to-end processing and will alert management and operations personnel when processing anomalies are detected.

VI. (U) Conclusion

~~(TS//SI//NF)~~ As discussed above, NSA has thoroughly reviewed the technological systems, analytic workflows and processes associated with its implementation of the BR FISA Court Order, and has introduced corrective measures to address specific concerns and vulnerabilities. These new measures will ensure a balanced focus on technological solutions and management controls. The end-to-end review also revealed areas for improvement which have been documented and will continue to be addressed. Where changes were made impacting current manual operations, a combination of system evaluations, demonstrations and audits provided confidence that the technical fixes are actually configured and operating as intended.

~~(TS//SI//NF)~~ The remedial actions described in this report are subject to ongoing improvement and will support strict adherence to the Court Order. Although no corrective measure is infallible, NSA has taken significant steps designed to eliminate the possibility of any future compliance issues and to ensure that the mechanisms are in place to detect and respond quickly if one were to occur.

Figure 1: Overall BR FISA Process

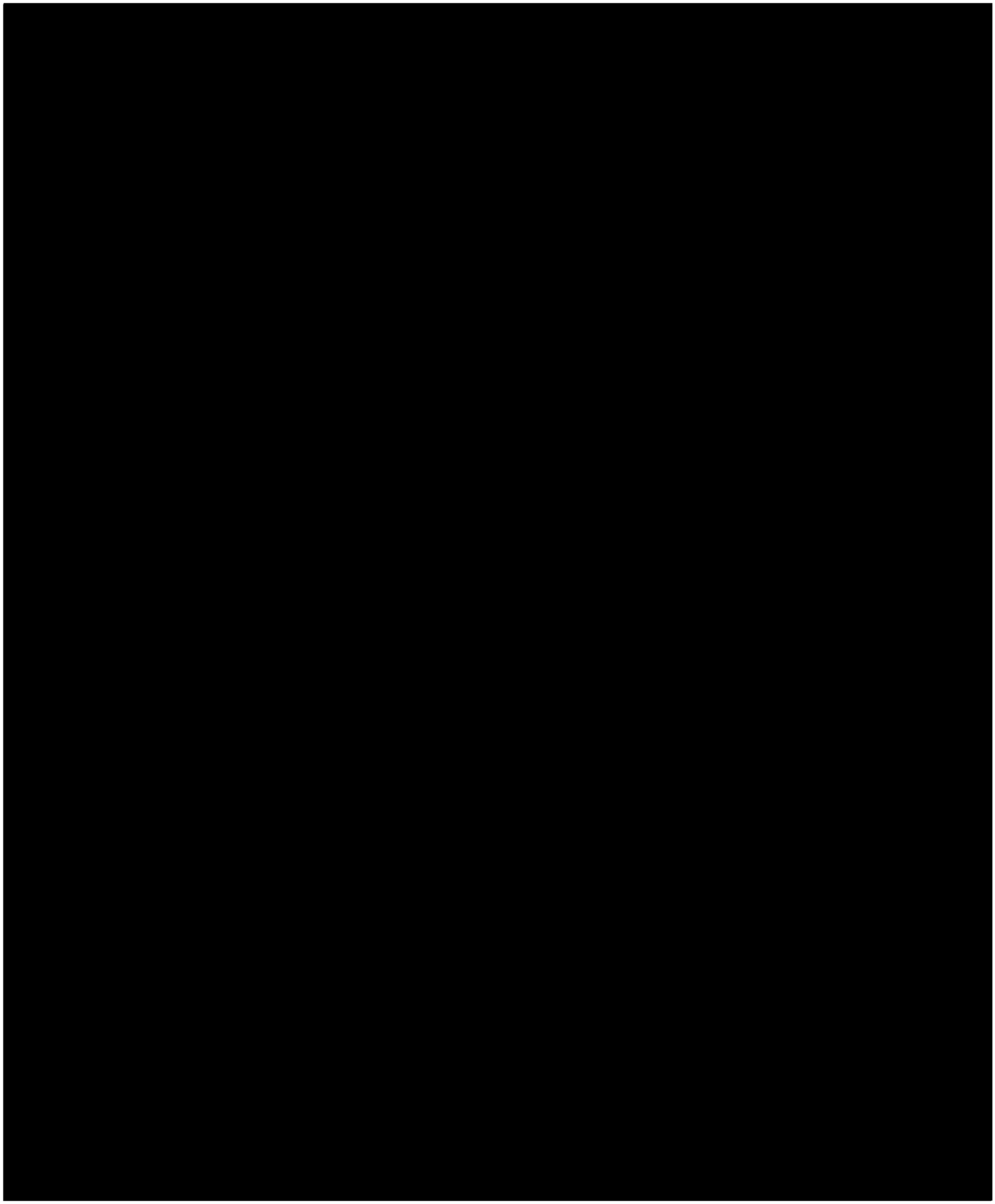


Figure 2: Components of BR FISA Process addressed in End-to-End Review

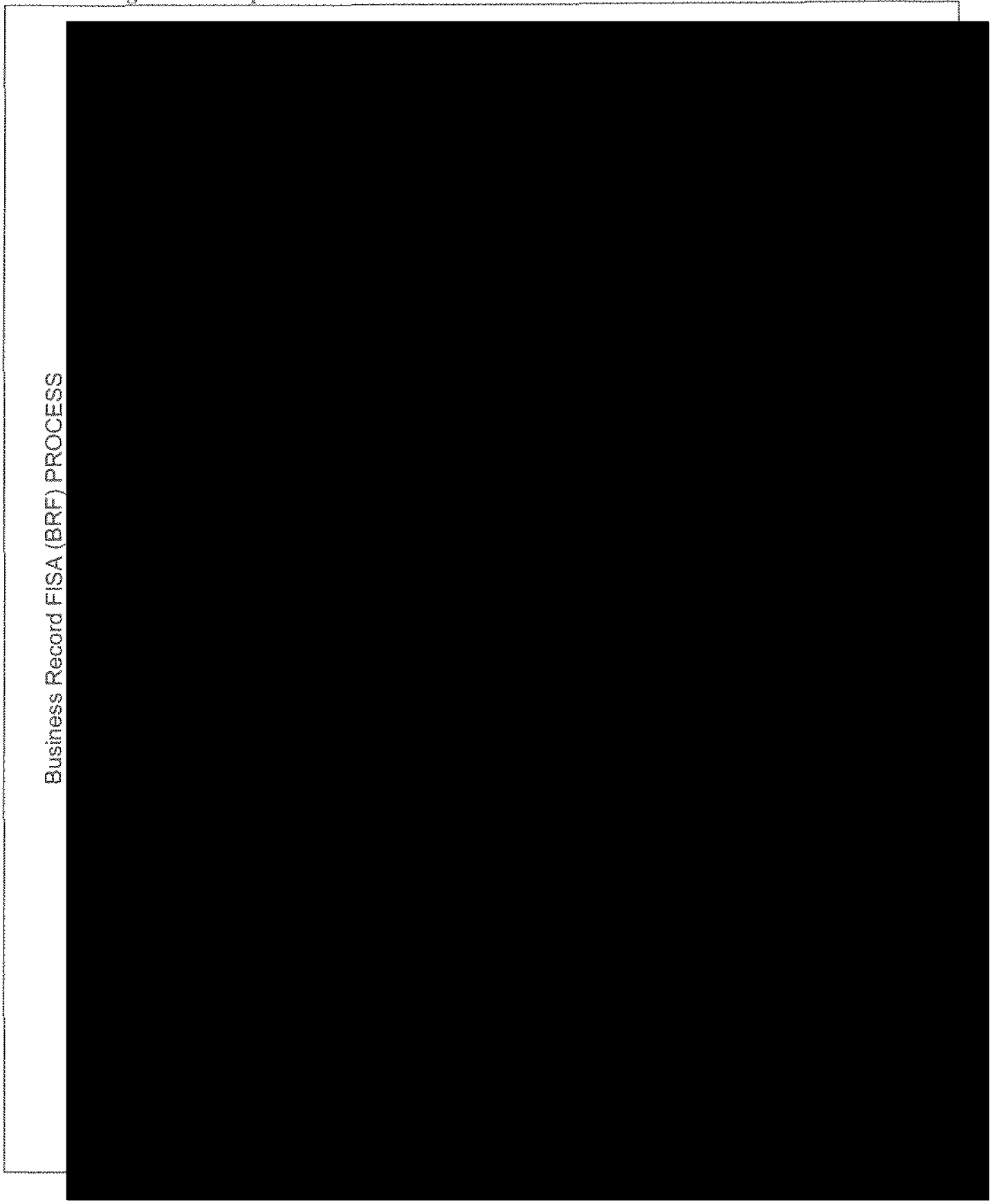


Figure 3: Component of BR FISA Process addressed in End-to-End Review

[redacted]

Figure 4: Component of BR FISA Process addressed in End-to-End Review

[redacted]

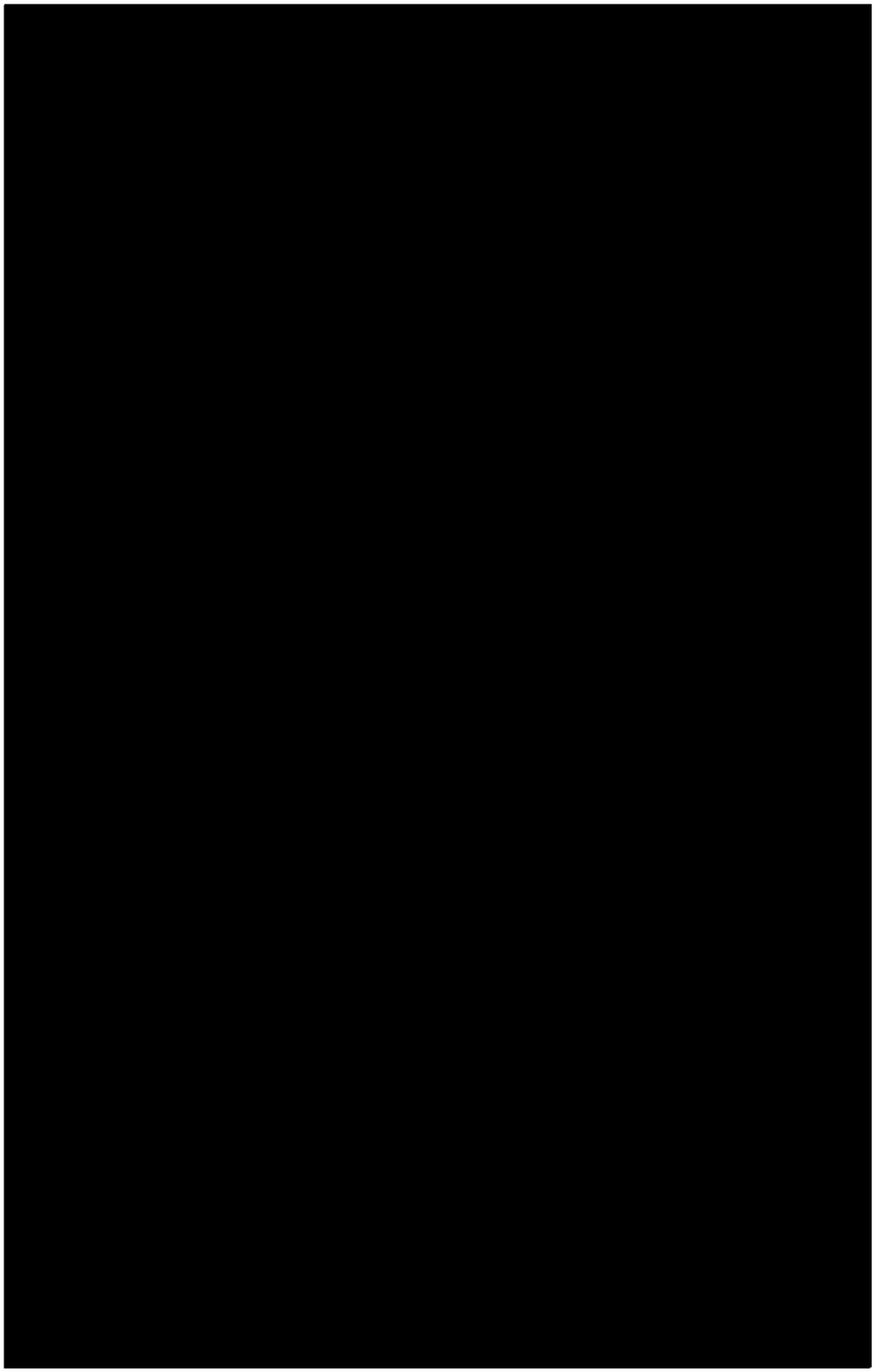


Figure 5: Component of BR FISA Process addressed in End-to-End Review

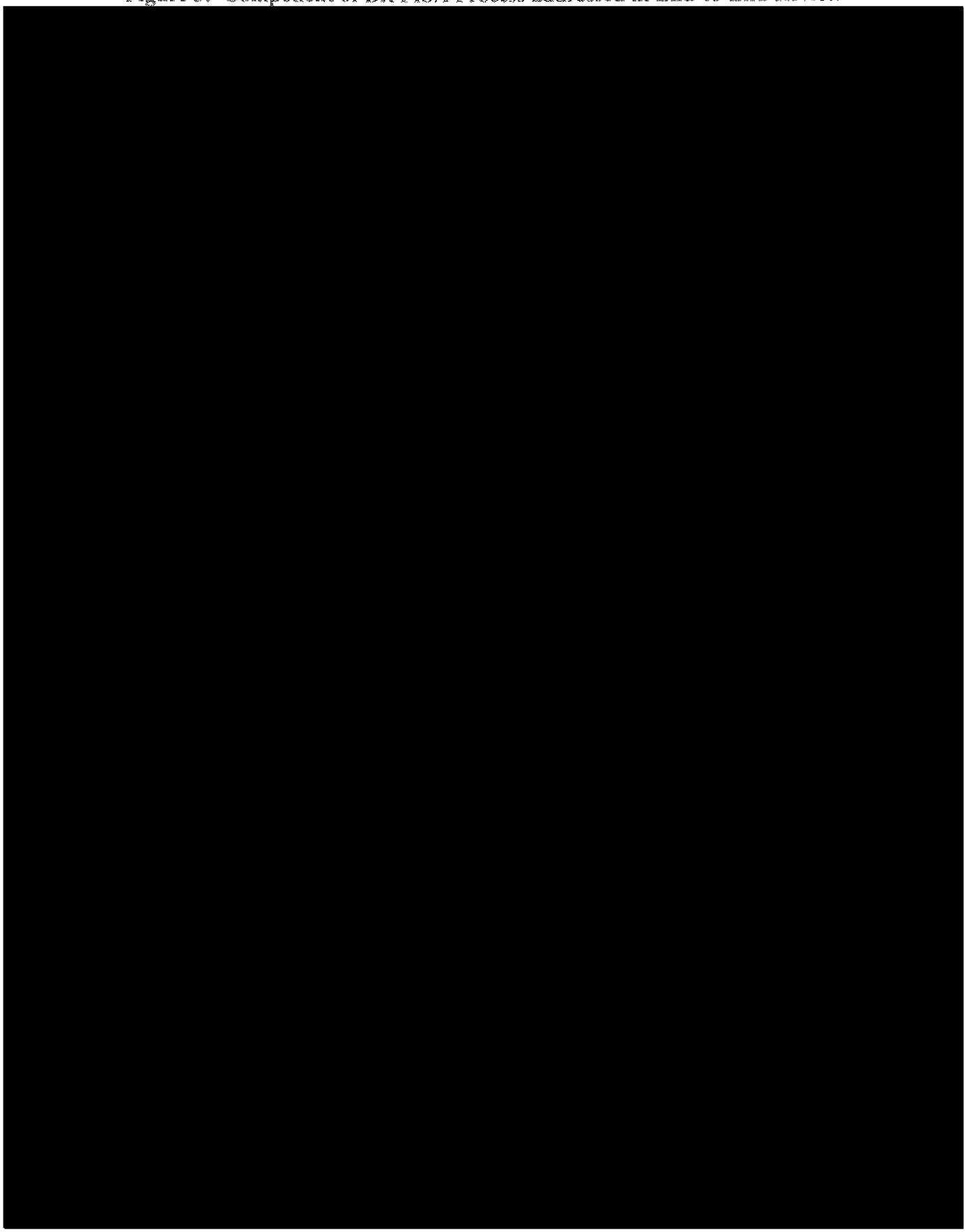


Figure 6: Component of BR FISA Process addressed in End-to-End Review

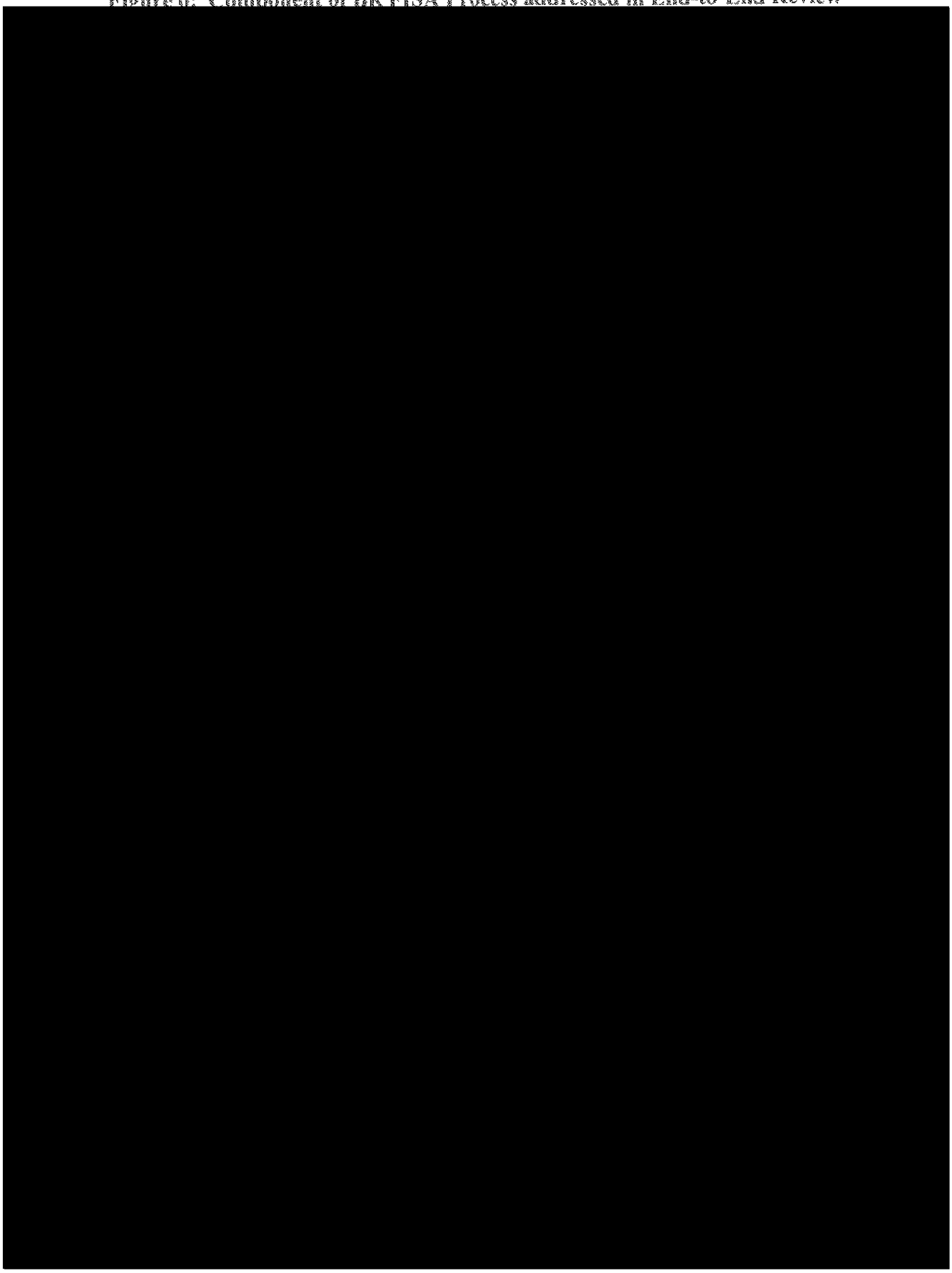


Figure 7: Component of BR FISA Process addressed in End-to-End Review
"Telephony Activity Detection Process"

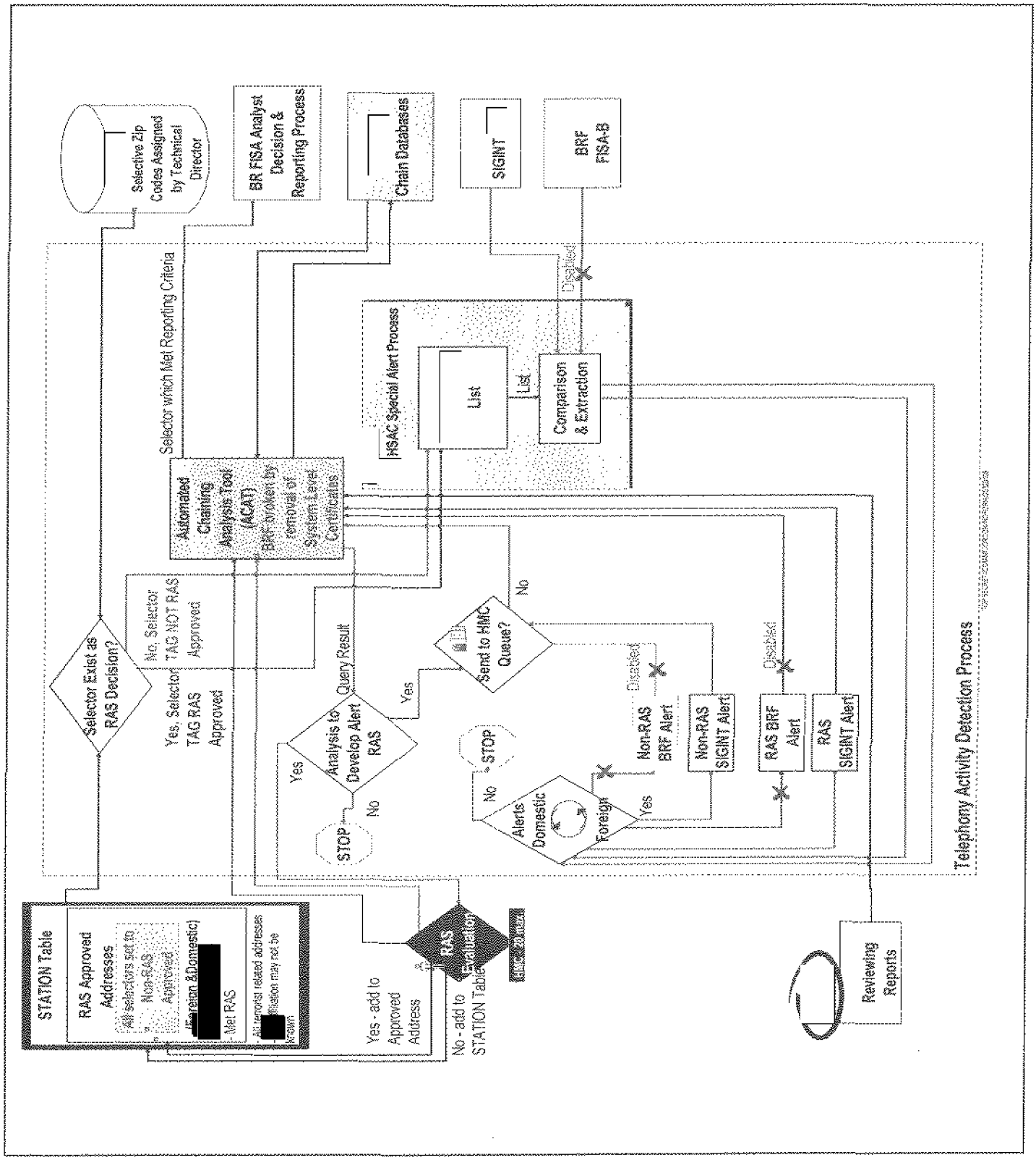
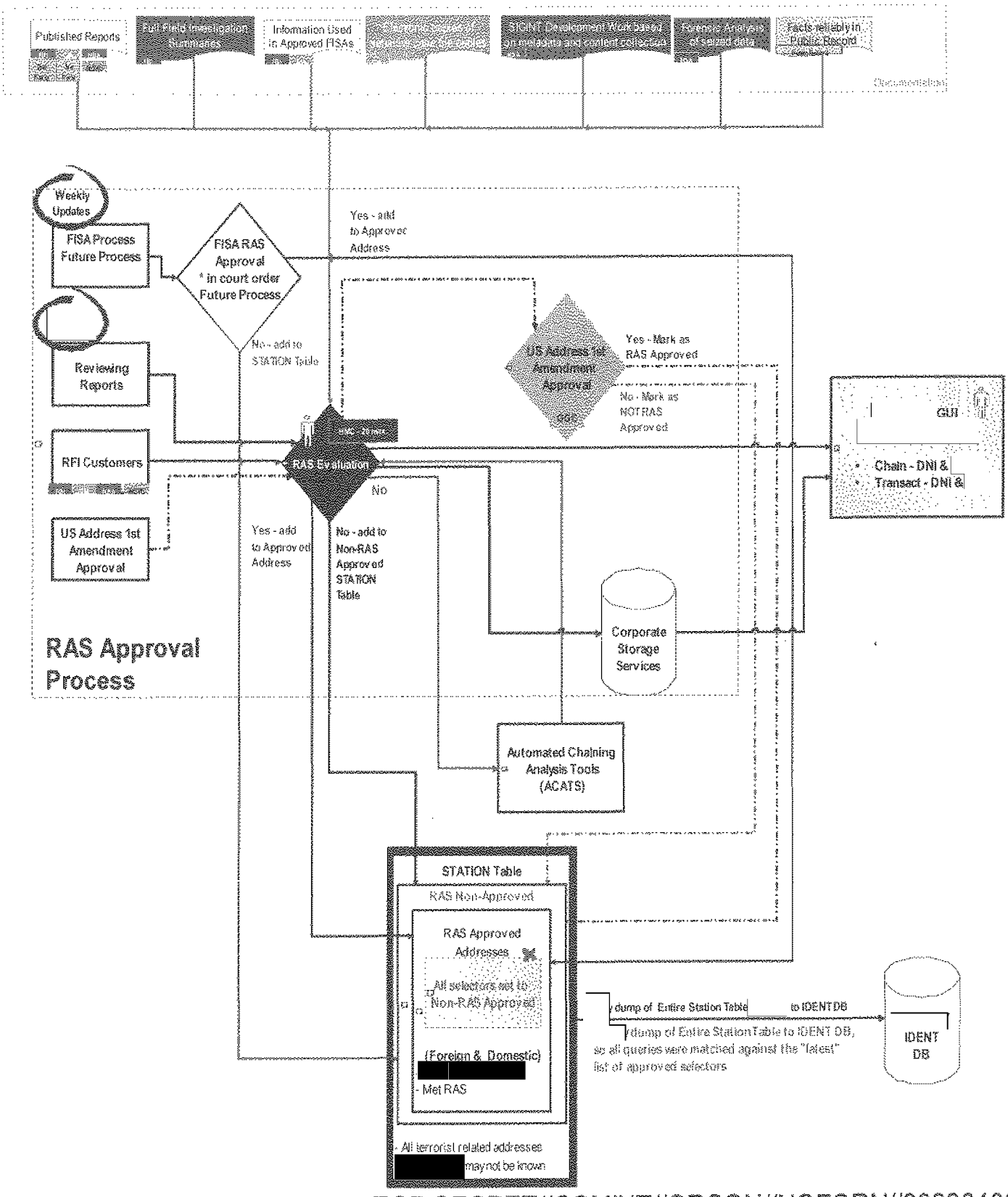


Figure 8: Component of BR FISA Process addressed in End-to-End Review
"RAS Approval Process"



~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

Figure 9: Component of BR FISA Process addressed in End-to-End Review "BR FISA Analytic Tools and Processes"

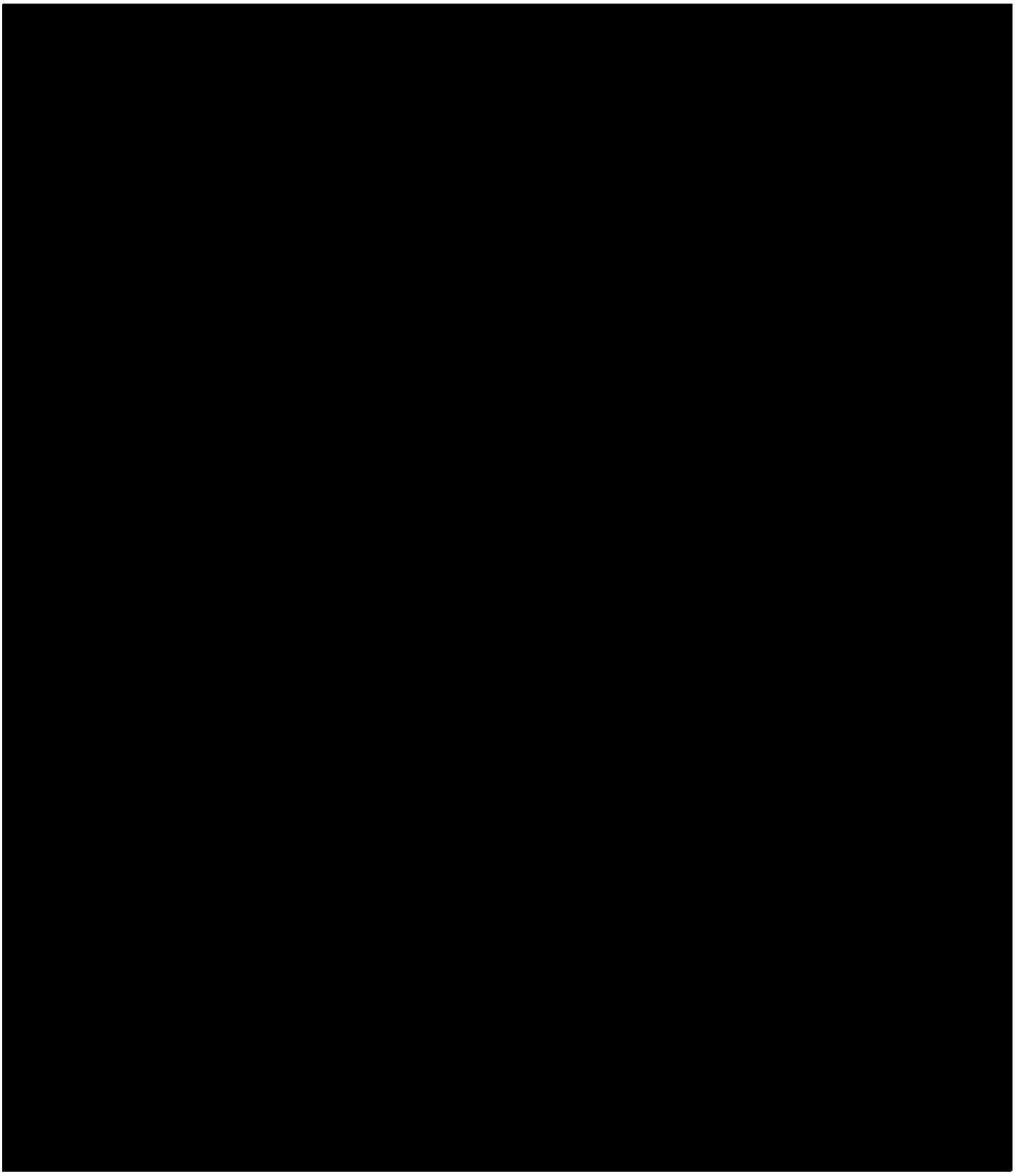
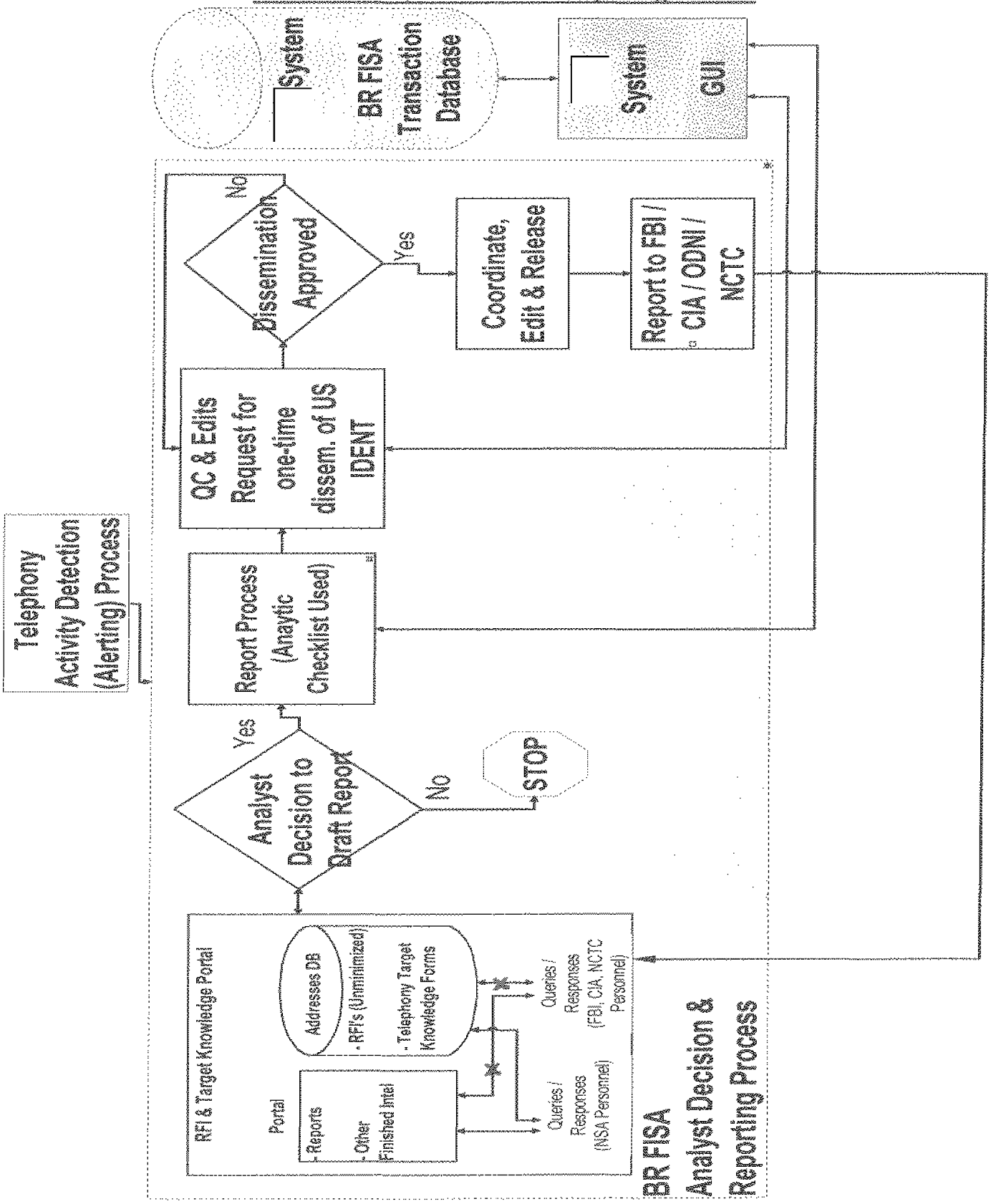


Figure 10: Component of BR FISA Process addressed in End-to-End Review
"BR FISA Analyst Decision and Reporting Process"



Appendix: Glossary of Terms

ACAT	*See Automated Chaining and Analysis Tool and GUI*
Activity Detection List	A list of foreign and domestic telephone selectors believed to be associated with terrorist targets. The Activity Detection List is independent of the Station Table. Formerly called the Alert List, this list is now more commonly referred to as the Activity Detection List in order to be more descriptive.
Alert List	*See Activity Detection List*
[redacted]	A database used to store correlations between selectors [redacted] It is one of the databases accessed by the [redacted] database.
Automated Chaining and Analysis Tool and GUI (ACAT)	ACAT provides automated chaining requests to [redacted] based on the occurrence of alerts [redacted] ad hoc query requests from BR FISA-authorized analysts [redacted]
Components	The core systems and processes identified as part of the BR FISA metadata workflow against which IPAs and PIAs were conducted.
Configuration Management	The process of tracking, controlling and documenting changes in software applications, including revision control and establishing baselines.
[redacted]	A database containing list of identifiers which, based on an analytic judgment, should not be tasked by the SIGINT system.
Defeat List	A list of selectors that are deemed of little analytic value for metadata analysis.
EAR	*See Emphatic Access Restriction*
[redacted]	
Emphatic Access Restriction (EAR)	A software restrictive measure written into the [redacted] middleware on 20

	February 2009 to prevent a non-RAS approved selector from being used for a chain query of the BR FISA metadata.
[redacted]	[redacted]
[redacted]	
Initial Privacy Assessment (IPA)	A review of a system or process which includes a standard set of questions used to determine, among other things, whether the system or process under review interacts with data that could contain information about U.S. persons.
IPA	*See Initial Privacy Assessment*
[redacted]	
	NSA's corporate file transfer/distribution system
	NSA's corporate contact chaining system.
	[redacted]
[redacted]	
Metadata	"Data about the data"; for example, information about a telephone call, to include the calling and called numbers, time of call, etc. Metadata does not include content.
[redacted]	The repository for individual BR FISA metadata call records for access by authorized Homeland Security Analysis Center (HSAC) and data integrity analysts

	to view detailed information about specific telephony calling events.
[redacted]	A selection management system used to manage and task selectors, such as telephone numbers, IMEIs, and IMSIs, to many different information collection systems worldwide.
Parsing Rules	A method for separating data into standardized data fields.
PIA	*See Privacy Impact Assessment*
PKI	*See Public Key Infrastructure*
Public Key Infrastructure (PKI)	An information assurance service that supports digital signatures and other public-key based security mechanisms, and offers security measures such as identification and authentication, access control and audit capability.
Privacy Impact Assessment (PIA)	An in-depth, standardized review of privacy concerns for a particular system or process
Requirements	The terms contained in the governing BR FISA metadata documents that must be satisfied as part the end-to-end workflow.
Sanitize	The process of disguising intelligence to protect sensitive collection sources, methods, capabilities or analytic procedures in order to disseminate to customers at a classification level they can use.
Seed	An initial selector used to generate a chain query.
Selector	An identifier, in BR FISA realm could be an IMEI, IMSI, or MSISDN, as well as a telephone number.
[redacted]	This tool is used by HMCs to conduct contact chaining against BR FISA metadata

	and provide the results to the team. HMCs only used RAS-approved selectors when using this tool. The team ultimately provided the results to NSA's
	The primary desktop graphical user interface (GUI) for access to data and services.
SOP	*See Standard Operating Procedure*
	NSA's mission element for access and exploitation o
SSP	*See System Security Plan*
Standard Operating Procedure (SOP)	Institutionalized documentation describing official processes and procedures.
Station Table	Historic reference of all telephony selectors that have been assessed for RAS – and their associated RAS determination (RAS Approved or Not RAS Approved) - since the BR FISA Order was first signed on 24 May 2006.
Sub-components	The logical and physical breakdowns of the BR FISA metadata workflow components that performed specific activities and/or functions.
	An analytic query tool used to seek out additional information on telephony selectors from and other knowledge bases and reporting repositories.
	A next generation metadata analysis graphical user interface (GUI) which is the replacement for
System Security Plan (SSP)	Formal document describing the implemented protection measures for the secure operation of a computer system.
Telephony Activity Detection (Alerting) Process	The process used to notify NSA analysts if there was a contact between a foreign telephone identifier associated with

	domestic telephone identifier.
[redacted]	The query tool which indicates whether a telephony selector is present in NSA data repositories, the total number of unique contacts, total number of calls, and "first heard" and "last heard" information for the selector.