UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, DC

IN RE PRODUCTION OF TANGIBLE THINGS
[redacted]

Docket Number: BR 08-13

NOTICE OF COMPLIANCE INCIDENTS (U)

The United States of America, pursuant to Rule 10(c) of the Foreign Intelligence Surveillance Court Rules of Procedure, advises the Court of the circumstances surrounding two compliance matters in docket number BR 08-13 and prior dockets in this matter. In support of this notice, the Government submits the attached Supplemental Declaration of Lt. General Keith B. Alexander, U.S. Army, Director of the National Security Agency (NSA) ("Supplemental Alexander Declaration"). ~~(TS)~~

In response to the Court's Order of January 28, 2009, the Director of NSA ordered end-to-end system engineering and process reviews (technical and operational) of NSA's handling of the call detail records collected pursuant to the Court's authorizations in this matter ("BR metadata"). See Declaration of Lt. General Keith B.

[redacted]

Alexander, U.S. Army, Director, National Security Agency, filed February 17, 2009, at 21 ("Alexander Declaration"). The Director also ordered an audit of all queries made of the BR metadata repository since November 1, 2008, to determine if any of the queries during that period were made using telephone identifiers for which NSA had not determined that a reasonable, articulable suspicion exists that they are associated with [redacted]nd [redacted]ns, as required by the Court's Primary Orders.[1] Id. at 22-23. These reviews identified the following two matters where NSA did not handle the BR metadata in the manner authorized by the Court.[2] ~~(TS//SI//NF)~~

Queries Using [redacted] On February 19, 2009, NSA notified the National Security Division (NSD) and the Office of the Director of National Intelligence that one of its analytical tools (known as [redacted]) may have been used to query the BR metadata and that such queries may have used non-RAS-approved telephone identifiers. Supp. Alexander Decl. at 5. According to the Supplemental Alexander Declaration, [redacted] determined if a record of a telephone identifier was present in NSA databases and, if so, provided analysts with certain information regarding the calling activity associated with that identifier. Id. at 3, 5-6. It did not provide analysts with the telephone identifiers that were in contact with the telephone identifier that

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

[2] NSD orally notified Court advisors of these two matters on February 20, 2009. ~~(S)~~

served as a basis for the query. Id. at 3, 6. Although [redacted] could operate as a stand-alone tool, it more often operated automatically in support of other analytic tools, namely [redacted] which is described more fully in the Supplemental Alexander Declaration. Id. at 3, 5-7. Since the Court's initial Order in May 2006, [redacted] would search the BR metadata and other NSA databases. Id. at 2-3, 5-6. ~~(TS//SI//NF)~~

According to the Supplemental Alexander Declaration, on February 18, 2009, NSA disabled portions of two analytic tools, including [redacted] that most often invoked [redacted] query mechanism. Id. at 7. On February 19, 2009, NSA confirmed that [redacted] was querying the BR metadata without requiring RAS-approval of the telephone identifiers used as query terms. Id. at 5. NSA then began to eliminate [redacted] access to the BR metadata. Id. at 3. On February 20, 2009, NSA restricted access to the BR metadata to permit only manual queries based on RAS-approved telephone identifiers and to prevent any automated processes from accessing the BR metadata. Id. at 7, 9. NSA also blocked access to the historical files that were generated from automated [redacted] queries. Id. at 7. Before re-instituting automated processes that would access the BR metadata, NSA and NSD will determine that any proposed automated process will access the BR metadata in a manner that complies with the Court's Orders. Id. at 9-10. ~~(TS//SI//NF)~~

Improper Analyst Queries Since November 1, 2008. On February 20, 2009, NSA notified NSD that NSA's audit of queries since November 1, 2008 had identified three analysts who conducted chaining in the BR metadata using fourteen telephone identifiers that had not been RAS-approved before the queries. According to the Supplemental Alexander Declaration:

- One analyst conducted contact chaining queries on four non-RAS-approved telephone identifiers on November 5, 2008;
- A second analyst conducted one contact chaining query on one non-RAS-approved telephone identifier on November 18, 2008; and
- A third analyst conducted contact chaining queries on three non- RAS-approved telephone identifiers on December 31, 2008; one non-RAS approved identifier on January 5, 2009; three non-RAS approved identifiers on January 15, 2009; and two non-RAS approved identifiers on January 22, 2009.

Id. at 8. None of the telephone identifiers used as seeds was associated with a U.S. person or telephone identifier, and none of the improper queries resulted in intelligence reporting. Id. at 8-9. According to the Supplemental Alexander Declaration, at the time of the improper queries, the three analysts were conducting queries of telephone metadata other than the BR metadata, and each appears to have been unaware that they were conducting queries of the BR metadata. Id. at 9. ~~(TS//SI//NF)~~

As stated in the Alexander Declaration, NSA began designing a software fix to prevent the querying of the BR metadata with telephone identifiers that had not been RAS-approved. Alexander Decl. at 23-24. On February 20, 2009, NSA installed that software fix; as a result, no non-RAS-approved telephone identifier may be used to query the BR metadata. Supp. Alexander Decl. at 9. ~~(TS//SI//NF)~~

-- Remainder of page intentionally left blank --

* * *

The Government acknowledges that in the above matters it did not handle the BR metadata in the manner authorized by the Court. These matters were identified as a result of the several oversight and investigative obligations that the Government voluntarily undertook as a result of the Court's Order of January 28, 2009. The Government also has implemented certain additional restrictions on the access to the BR metadata that are designed to prevent the recurrence of improper access to the BR metadata. Accordingly, the Government respectfully submits that the Court need not take any further remedial action. ~~(TS//SI//NF)~~

Respectfully submitted,

Acting Section Chief, Oversight

[redacted]

Office of Intelligence

National Security Division
United States Department of Justice

Attachment

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

(TS) In Re Production of Tangible Things)
[redacted])
)
)
)

Docket No.: BR 08-13

SUPPLEMENTAL 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 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.

(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.

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

I. (U) Purpose:

~~(TS//SI//NF)~~ Pursuant to a series of Orders issued by the Court since May 2006, NSA has been receiving telephony metadata from telecommunications providers. NSA refers to the Orders collectively as the "Business Records Order" or "BR FISA." Among other things, the Business Records Order requires NSA to determine that there is a reasonable articulable suspicion ("RAS") to believe that a telephone identifier that NSA wishes to use as a "seed" for accessing the BR FISA data is associated wi [redacted] This supplemental declaration describes two compliance matters that NSA has discovered while implementing the corrective actions the Government described to the Court in the brief and declaration filed with the Court on 17 February 2009 regarding a compliance matter that the Department of Justice ("DoJ") first brought to the Court's attention on 15 January 2009. *See, respectively,* Memorandum of the United States in Response to Court's Order Dated January 28, 2009, ("DoJ Memo") *and* Declaration of Keith B. Alexander ("Alexander Declaration"), Docket BR 08-13.

II. (U) Incidents:

A. (U) Summary

~~(TS//SI//NF)~~ During an end-to-end review of NSA's technical infrastructure that I ordered in response to the compliance incident that DoJ reported to the Court on 15 January 2009, NSA personnel determined on 18 February 2009 that an NSA analytical tool known as was querying both E.O. 12333 and the Business Records data and that such queries would not have been limited to RAS approved telephone identifiers. As explained further below, [redacted] was automatically invoked to support certain types of analytical research. Specifically, to help analysts identify a phone number of interest. If an analyst conducted research supported by [redacted] the analyst would receive a generic notification that NSA's signals intelligence ("SIGINT") databases contained one or more references to the telephone identifier in which the analyst was interested; a count of how many times the identifier was present in SIGINT databases; the dates of the first and last call events associated with the identifier; a count of how many other unique telephone identifiers had direct contact with the identifier that was the subject of the analyst's research; the total number of calls made to or from the telephone identifier that was the subject of the analyst's research; the ratio of the count of total calls to the count of unique contacts; and the amount of time it took to process the analyst's query. [redacted] did not return to the analyst the actual telephone identifier(s) that were in contact with the telephone identifier that was the subject of the analyst's research and the analyst did not receive a listing of the individual NSA databases that were queried by [redacted]

~~(TS//SI//NF)~~ After identifying that [redacted] was allowing non-RAS approved telephone identifiers to be used to conduct queries of the BR FISA metadata to generate the statistical information that [redacted] returned to individual analysts, NSA personnel immediately began to eliminate [redacted] ability to access the BR FISA data. As of 20 February 2009, no automated analytic process or analytical tool can access the telephony metadata NSA receives pursuant to the Business Records Order. Moreover, the system's change of 20 Feburary 2009 ~~also~~ prevents manual queries of the BRFISA metadata unless NSA has determined that the telephone identifier that is being used to query the data has satisfied the RAS standard.

~~(TS//SI//NF) In~~ addition to the problem NSA identified regarding [redacted] during a 100% audit of individual analyst queries of the BR FISA metadata, NSA personnel discovered that three analysts inadvertently accessed the Business Records data using fourteen different non-RAS approved selectors between 1 November 2008 and 23 January 2009. None of the improper queries resulted in any intelligence reporting and none of the identifiers were associated with a U.S. telephone identifier or U.S. person. The technical change NSA implemented on 20 February 2009 to correct the problem of automated BR FISA queries also included another software change that prevents manual queries against non-RAS approved identifiers. Thus, the 20 February 2009 system upgrades should prevent recurrences of the improper analyst queries that are also discussed in detail below.

B. (U) Details

~~(S) In~~cident 1: [redacted]

~~(TS//SI//NF) As~~ part of the response to the compliance problem described to the Court in my 17 February 2009 declaration, I ordered an examination "to ensure that NSA's technical infrastructure has not allowed, and will not allow, non-approved selectors to be used as seeds for contact chaining [redacted] of the BR FISA data." Alexander Declaration at 22. I also stated that NSA would "report to DoJ and the

Court if this examination of the technical infrastructure reveals any incidents of improper querying of the BR FISA data repository." *Id.*

~~(TS//SI//NF) O~~n 18 February 2009, NSA technical personnel notified NSA's Office of General Counsel that, as part of the review of NSA's technical infrastructure that I ordered, they discovered that the use of [redacted] may have resulted in queries of NSA's BR FISA data and that such queries would not have been limited to the use of RAS approved telephone identifiers. On 19 February 2009, NSA personnel confirmed that this was, in fact, the case. NSA informally notified DoJ and the Office of the Director of National Intelligence of this problem later that same day.

~~(S//SI) A~~s I stated above, NSA uses [redacted] to support analytical research regarding telephone identifiers that are of intelligence interest to NSA's SIGINT personnel. [redacted] determines if a telephone identifier is present in NSA data repositories and also reports the level of calling activity associated with any particular telephone identifier. Although [redacted] can be used as a stand-alone tool, it is used more often as a background process in support of other NSA analytical tools.

[redacted]

[redacted]

[redacted] The results of the [redacted] queries (the number of unique contacts found for each expanded telephone identifier; the total number of calls made to or from the telephone identifier that served as the basis for the query; the ratio of total calls to unique calls; the date of the first call event recorded; the date of the last call event; and the amount of time it took to process the query) would be displayed to the analyst [redacted]

[redacted] Although [redacted] no longer can access the BR FISA data, [redacted] greatly assists analysts to choose selectively the best identifiers for further target development. As I stated above, [redacted] does not return the telephone identifier(s) that were in contact with the telephone identifier that was the subject of the analyst's research.

~~(TS//SI//NF)~~ NSA has determined that the Agency had configured [redacted] to include the BR FISA data repository as one of the sources of SIGINT data that [redacted] queried since the issuance of the first Business Records Order in May 2006.

[redacted]

This configuration remained in place until NSA identified this problem on 18 February 2009. As noted previously, [redacted] did not tell individual analysts which SIGINT databases [redacted] was querying nor did the tool provide analysts with the actual telephone numbers that had been in direct contact with the identifiers that served as the basis for [redacted] queries. In other words, if an analyst wanted to construct a chain [redacted] of the contacts associated with an identifier that had been the subject of a [redacted] query, the analyst was required to query the appropriate data repositories directly. For BR FISA data, this meant that only an analyst approved for access to BR FISA material could conduct such a query.

~~(TS//SI//NF)~~ Upon identification of this problem, NSA took immediate corrective actions. First, on the evening of 18 February 2009, NSA's Signals Intelligence Directorate disabled portions of two analytical tools used most often to invoke [redacted] automatic query mechanism. Second, on the morning of 19 February 2009, NSA shut down [redacted] itself. Third, after conducting further examination of the problem, on the morning of 20 February 2009, the Signals Intelligence Directorate installed a technical safeguard called Emphatic Access Restriction, which is the equivalent of a firewall that prevents any automated process or subroutine from accessing the BR FISA data.[2] Fourth, on the evening of Friday, 20 February 2009, NSA blocked access to the historical files that were generated from automated [redacted] queries.

[2] ~~(TS//SI//NF)~~ This technical safeguard had been under development since mid-January 2009, following the initial discovery of compliance issues associated with the Business Records Order. The safeguard also prevents analysts from performing manual chaining on numbers that have not been marked as RAS approved.

~~(S)~~ Incident 2: Improper Analyst Queries

(~~TS//SI//NF~~) Among the other corrective actions described to the Court in the Government's filing on 17 February 2009, NSA also initiated an audit of all queries made of the BR FISA data between 1 November 2008 and 23 January 2009. *See* Alexander Declaration at 22-23. As part of this audit, NSA has identified additional instances of improper analyst queries of the BR FISA data. None of the improper queries resulted in any intelligence reporting and none of the identifiers were associated with a U.S. telephone number or person.

~~(TS//SI//NF)~~ Prior to 15 January 2009, audits of BR FISA queries were implemented as spot checks of analyst queries or would be limited to a single day's worth of queries. After one of these spot checks identified improper queries conducted by two analysts, the Agency decided to conduct a more comprehensive audit of all analysts queries of the BR FISA metadata conducted between 1 November 2008 to 23 January 2009. *See* Alexander Declaration at 22-23. When NSA oversight personnel completed the first round of this comprehensive audit, they discovered that three analysts were responsible for fourteen instances of improper querying of the BR FISA data. The fourteen seed identifiers did not meet RAS approval prior to the analysts' queries. The first analyst conducted one query on one non-RAS approved seed identifier on 18 November 2008. The second analyst chained on four different non-RAS approved seeds on 5 November 2008. The third analyst chained on three different non-RAS approved seeds on 31 December 2008; one non-RAS approved identifier on 5 January 2009; three different non-RAS approved identifiers on 15 January 2009; and two different non-RAS approved identifiers on 22 January 2009. None of the improper queries resulted in any intelligence reporting and none of the identifiers were associated with a U.S. telephone identifier or U.S. person.

~~(TS//SI//NF)~~ Each of the analysts responsible for these improper queries did not realize they were conducting queries in the BR FISA data. .This conclusion is based on an audit of other queries they were conducting at the same time as well as questioning of the analysts by NSA's Oversight and Compliance Office. Each analyst thought they were conducting queries of other repositories of telephony metadata that are not subject to the requirements of the Business Records Order.[3] On 20 February 2009, software changes were made to ensure analysts could only access the BR data using this new version of the chaining tool.

~~(TS//SI//NF)~~ As the Government reported in its filing of 17 February 2009, NSA decided to design new software to prevent the querying of any telephone identifier within the BR FISA data unless the identifier has been RAS-approved. See Alexander Declaration at 23-24. On 20 February 2009, the software change NSA made to prevent automated tools from access the BR FISA metadata also prevents any non-RAS approved selector from being used as a seed for manual querying of the BR FISA data.

III. (U) Conclusion:

~~(TS//SI//NF)~~ NSA's implementation of Emphatic Access Restriction should prevent recurrences of both types of compliance incidents that are the subject of this supplemental declaration to the Court. NSA's BR FISA data repository is currently only able to accept manual queries based on a RAS-approved telephone identifier. Prior to

[3] ~~(TS//SI//NF)~~ At the time of the improper queries, each of these analysts were using dual screen computer equipment that provided the analysts with simultaneous access to BR FISA data and metadata that is not subject to the Business Records Order.

reinstituting any automated process that would provide any sort of access to, or comparison against, the BR FISA data, NSA's Office of General Counsel and the Department of Justice will review and approve the process.

~~(TS//SI//NF)~~ Notwithstanding implementation of Emphatic Access Restriction, NSA continues to examine its technical infrastructure to ensure that queries of BR FISA metadata are restricted to the use of RAS approved telephone identifiers. I expect that any further problems NSA personnel may identify with the infrastructure will be historical in nature. However, as indicated in my previous declaration to the Court, NSA will report any further problems Agency personnel may identify (whether current or historical) to both DoJ and the Court.

(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 25TH day of Febuary, 2009