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

[redacted]

GOVERNMENT'S SUPPLEMENT TO ITS RESPONSE TO THE COURT'S ORDER OF JANUARY 16, 2009

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached supplement to the government's January 26, 2009, response to the Court's Order of January 16, 2009, concerning [redacted] [redacted] and the targeting and minimization procedures submitted therewith. The Government may seek to augment and/or modify the information provided in its January 26, 2009, response, and this supplement thereto, as appropriate during any hearing that the Court may hold in the above-captioned matter. (S//OC,NF)

Respectfully submitted,
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Deputy Unit Chief
National Security Division
United States Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by:	~~Matthew G. Olsen, Deputy Assistant Attorney General, NSD, DOJ~~
Reason:	~~1.4(c)~~
Declassify on:	~~17 March 2034~~

(U) Executive Summary

~~(TS//SI//NF)~~ This report for the Foreign Intelligence Surveillance Court describes a circumstance where the National Security Agency ("NSA" or "Agency") acquires more communications than intended ("overcollection") during signals intelligence activities authorized pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, and the steps NSA has taken to correct such incidents of overcollection. In order to fully describe the problem and NSA's corrective measures, this report also describes relevant aspects of the Agency's collection methods, technical architecture, and the equipment, systems, and procedures NSA employs to identify and correct instances of overcollection. NSA is confident that the corrective measures NSA has designed, tested, and fielded to correct the overcollection problem form a reasoned and appropriate response to past instances of overcollection. There remains one known instance of overcollection for which NSA is developing a corrective measure as discussed herein. These corrective measures are subject to continuing improvement and NSA personnel also continue to monitor the Agency's collection activities for signs of overcollection. Although no corrective measure is perfect, NSA has taken significant steps to mitigate the possibility of any future overcollection and to ensure that the detection mechanisms in place to identify overcollection will allow NSA to respond quickly if and when it does occur.

I. ~~(TS//SI//REL USA, FVEY)~~ Description of NSA's Upstream Collection

~~(TS//SI//REL)~~ Pursuant to the signals intelligence authority provided to the National Security Agency ("NSA" or "Agency") by Executive Order 12333, as amended; National Security Council Intelligence Directive No. 6; the NSA Act of 1959, as amended; and other applicable law and policy direction, [redacted] NSA has developed and evolved techniques for selecting and processing Internet communications for the purpose of obtaining foreign intelligence. [redacted] NSA uses [redacted] collection techniques to acquire communications whose acquisition is regulated by the FISA, to include collecting communications pursuant to certifications executed in accordance with Section 702 of the FISA Amendments Act of 2008 ("FAA").[1]

~~(TS//SI//NF)~~ NSA's FAA collection of Internet communications (e.g., e-mail communications to, from, or about a targeted e-mail selector) is accomplished [redacted]

[1] (U) NSA personnel frequently refer to the Agency's non-FISA collection activity as "12333 collection." In contrast, NSA personnel frequently refer to collection accomplished pursuant to Section 702 of the FAA as "FAA collection."

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

Internet Service Providers ("ISPs") provide information contained in targeted accounts under the ISP's control; [redacted] collection listed above are referred to as "Upstream Collection" in the government's response to the Court's January 16, 2009 Order concerning DNI/[redacted] ("Government's Response").

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

[redacted]

[redacted]

[2] (U) Examples of [redacted]

[3] (U) As used in this context, [redacted]

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

[redacted]

~~(TS//SI//NF)~~ Not only does [redacted] compensate for [redacted] is uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information [redacted] For example, [redacted] Similarly, it allows NSA to [redacted] In both of these examples, the communications acquired through [redacted] may help NSA ascertain [redacted] previously unknown individuals who may also possess and/or communicate valuable foreign intelligence information. Additionally, [redacted]

II. ~~(TS//SI//NF)~~ Description of [redacted]

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

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

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

[redacted]

III. ~~(TS//SI//NF)~~ [redacted] Overcollection and the Evolution of NSA's [redacted] [redacted] Systems

~~(TS//SI//NF)~~ Any collection technique that NSA employs may result in the inadvertent collection of communications NSA did not intend to acquire.[6] As described previously, the [redacted] provides unique foreign intelligence information. However, it also comes with the potential for producing overcollection, including [redacted] Overcollection ("[redacted]O"). [redacted]O occurs when, while collecting communications [redacted] the Agency also inadvertently acquires other communications that [redacted]

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

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

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

[6] ~~(S//SI//REL)~~ NSA handles any inadvertent collection of US person information in accordance with the Court-approved minimization procedures corresponding to the specific FAA certification under which NSA acquired the information.

[7] ~~(TS//SI//REL)~~ [redacted]

[redacted]

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

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

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

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

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

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

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

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

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

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

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

[11] ~~(TS//SI//NF)~~ NSA technical personnel evaluated approximately [redacted] files during this week long test, and approximately [redacted] additional files in subsequent testing.

[redacted]

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

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

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

IV. ~~(TS//SI//NF)~~ Review of Overcollection Incidents

~~(TS//SI//NF)~~ In recent notices the Department of Justice filed with the Court pursuant to Rule 10(c) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, the Government described [redacted] overcollection incidents arising from NSA's use of [redacted][12] [redacted] of these [redacted] incidents were examples of [redacted]O. [redacted]

[12] ~~(TS//SI//NF)~~ [redacted] Table 1 briefly summarizes each incident.

[redacted]

~~(TS//SI//NF)~~ A summary of all [redacted]ecent overcollection incidents is provided in Table 1. The [redacted] additional incidents referenced on page 15 of the Government's Response[14] were also incidents of [redacted]O. Specifically, in [redacted] 2007 while conducting foreign intelligence acquisition in accordance with the Protect America Act of 2007 ("PAA"), NSA discovered [redacted]O resulting from [redacted] To be clear, NSA discovered this [redacted] in [redacted] 2007 and took immediate steps to [redacted] NSA has purged every file collected [redacted] during the time period [redacted]

~~(TS//SI//NF)~~ The [redacted] that resulted in [redacted] overcollection (also discovered by NSA in [redacted] 2007) is described on page 15 of the Government's Response, and again here, as the [redacted] Specifically, in [redacted] 2007, during NSA's implementation of foreign intelligence acquisition authorized under the PAA, NSA implemented [redacted] at the request of the Agency's Office of Oversight and Compliance. [redacted]

[13] (U//FOUO) [redacted]

[14] ~~(TS//SI//NF)~~ In addition to the overcollection incidents resulting from NSA's upstream collection techniques, there have been other isolated incidents involving 702 acquisitions of a substantially different nature. For example, as has been previously reported to the Court, there have been a few incidents in which the selectors of a United States person subject to traditional FISA coverage or a Section 704 order have been erroneously targeted under Section 702. Additionally, there have been other incidents involving the targeting or minimization procedures, including several selectors mistasked due to typographical errors in the targeting process and human errors that caused delays in the detasking of accounts where the user was known to be arriving in the United States. These latter incidents are reported to the Court in the Section 702(l) joint Department of Justice/Office of the Director of National Intelligence assessment and/or in the Section 707 Semiannual Report to Congress Concerning Acquisitions Under Section 702 of the FISA Amendments Act, a courtesy copy of which will be provided to the Court.

[redacted] In response, NSA purged every communication collected [redacted] during the relevant timeframe [redacted] 2007). NSA also [redacted] remedy for this problem by [redacted] 2007, [redacted] Subsequent testing revealed this remedy was successful, [redacted]

V. ~~(TS//SI//NF)~~ Additional Steps to Identify Overcollection

~~(TS//SI//NF)~~ In addition to [redacted] NSA continues to track and routinely monitor [redacted] looking for anomalies [redacted]hat are indicative of [redacted]O.

~~(TS//SI//NF)~~ NSA has also made analysts aware of the potential for these [redacted]O events and is providing instruction and training on how to recognize and report potential cases. Prior to being granted access to any FAA data, NSA analysts undergo formal training and competency testing on the FAA targeting and minimization procedures. This training is augmented by informal on-the-job training conducted by technical personnel as well as oversight personnel. The end result is that NSA analysts are trained to verify that the communications they are reviewing are, in fact, associated with the intended target and that the target remains a non-United States person located outside of the United States. Analysts have also been alerted to the possibility of overcollection of communications and have been provided hypothetical examples of what to look for when conducting post-collection reviews. In the event of possible overcollection, analysts are instructed to contact their organization's FAA Point of Contact who initiates an internal NSA review of a possible compliance incident. Samples of the data are then evaluated by technical personnel to confirm or refute that overcollection may have occurred. Confirmation of any occurrence of overcollection results in notification to NSA's Office of General Counsel which in turn reports these to the Department of Justice and the Office of the Director of National Intelligence in accordance with NSA's FAA Targeting Procedures. In addition, proper application of the minimization and targeting procedures that govern NSA's FAA collection also helps ensure that overcollection does not result in improper dissemination of information that may have been obtained through overcollection.

VI. ~~(TS//SI//NF)~~ NSA's Handling of Information Resulting from Overcollection

~~(TS//SI//NF)~~ Once an overcollection incident has been confirmed, NSA takes the required steps to isolate and purge all unminimized data from its repositories. Overcollected data can be purged from on-line databases using a variety of methods, all of which render it inaccessible in any new analyst queries. This may involve purging data that was appropriately acquired in addition to the data that was inadvertently acquired. For example, regarding the [redacted] incident, NSA purged all data collected as a result of targeting that selector during the entire timeframe of this incident. [redacted]

~~(TS//SI//NF)~~ Regarding dissemination, although the likelihood that any minimized FAA data resulting from overcollection would be disseminated in serialized product reporting is extremely small, in view of the fact that the inadvertent collection was unrelated to any targeted communications, NSA confirms that no such reporting occurred. In the case of the reported FAA overcollection incidents discussed here and in the Government's Response, NSA determined that no serialized product reports had been disseminated. This was accomplished by searching NSA's [redacted] If any information had been disseminated in serialized product, NSA would take the required steps to cancel/recall such reporting.

VII. ~~(TS//SI//NF)~~ The Five-Year Retention Period Established by NSA's Minimization Procedures is Reasonable Notwithstanding the Overcollection

~~(TS//SI//NF)~~ NSA submits, for the following reasons, that the five-year data retention period established by NSA's minimization procedures is reasonable notwithstanding the overcollection incidents described herein. As discussed above in detail, NSA has taken considerable steps to identify and purge overcollected communications acquired as a result of these incidents -- regardless of whether such communications contain information of or concerning United States persons -- and to prevent any future occurrences of [redacted]D. Furthermore, the NSA minimization procedures work to dramatically reduce, if not eliminate, the impact of any incidental and inadvertent intrusions into the privacy of United States persons in the event that NSA retains any unidentified overcollected communications. Indeed, the likelihood that NSA analysts would even come across a previously unidentified overcollected communication of

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

or concerning a United States person during the regular course of their duties is minimal. As noted above, the amount of overcollected data, relative to the overall amount of properly acquired data collected by the NSA pursuant to the FAA, is quite small.[16] In addition, section 3(b)(5) of the NSA minimization procedures requires that all computer queries of collected communications stored in NSA data repositories "shall be limited to those selection terms reasonably likely to return foreign intelligence targets." Inasmuch as the overcollection described herein resulted in the inadvertent acquisition of communications wholly unrelated to targeted selectors used by properly targeted foreign intelligence targets, it is unlikely that NSA analysts, using appropriately tailored queries, would retrieve -- let alone analyze and disseminate -- any previously unidentified overcollected communication for review.[17]

~~(TS//SI//NF)~~ Moreover, even in the unlikely event that an NSA analyst's query does retrieve an overcollected communication of or about a United States person, section 3(b)(1) of the NSA minimization procedures requires the destruction of that communication as soon as it is recognized. NSA analysts are being trained to identify overcollection incidents and promptly report them to oversight personnel so that appropriate measures -- including the destruction of <u>all</u> communications inadvertently acquired as a result of such incidents (regardless of whether they contain information of or concerning a United States person) -- can be taken.

~~(TS//SI//NF)~~ In sum, NSA's minimization procedures operate to dramatically reduce, if not eliminate, the impact of any incidental and inadvertent intrusions into the privacy of United States persons that may result from NSA's retention of unidentified overcollected communications for the five-year period established by those procedures. Accordingly, NSA submits that this retention period is reasonable.

VIII. (U) Conclusion

~~(TS//SI//NF)~~ As discussed above, NSA has developed new generation [redacted] and new generatio[redacted] which greatly reduce the likelihood of overcollection or the extent to which it might occur. NSA has also developed [redacted] as an additional layer of protection against [redacted]O incidents. NSA has further educated and sensitized its work force to the problem of overcollection, how to identify possible instances of it and how to report it when it is identified. It is important to note that NSA has not been able to identify any circumstance where an overcollection incident resulted in the dissemination of overcollected information outside of the NSA SIGINT production chain (analysts and others authorized with access to unminimized FAA data).

[16] ~~(TS//SI//NF)~~ Given the efficacy of the measures NSA has taken to date in response to the incidents described herein, NSA expects that any future occurrences of [redacted]O that may occur would involve even smaller volumes of overcollected communications.

[17] ~~(TS//SI//NF)~~ Moreover, analysts' queries are routinely audited by trained personnel in the various SIGINT product lines and superaudited by NSA oversight and compliance personnel to ensure that all such queries are consistent with NSA's minimization procedures.

~~(TS//SI//NF)~~ Except in the [redacted] NSA has been able to identify the causes of the incidents of overcollection and has taken extensive and multi-layered steps to prevent similar incidents in the future. NSA has purged all of the data it has identified as overcollection. There is no guarantee that future [redacted] problems will not occur, or that future [redacted] changes, which NSA may not have anticipated, and which [redacted] Nonetheless, NSA has reason to be confident that [redacted] work as designed. In sum, NSA has taken significant steps to mitigate the possibility of any future overcollection and to ensure that the detection mechanisms in place to identify overcollection will allow NSA to respond quickly if and when it does occur.

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

Table 1. Summary of Overcollection Incidents

[redacted]

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

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

Table 2: [redacted]
January 16, 2009 [redacted]

[redacted]