

~~TOP SECRET~~

CONTROL NO. \_\_\_\_\_  
COPY \_\_\_\_\_ OF \_\_\_\_\_

~~Handle Via  
COMINT  
Channels~~

~~NATIONAL SECURITY INFORMATION  
Unauthorized Disclosure Subject to Criminal Sanctions~~

~~TOP SECRET~~



U.S. Department of Justice

National Security Division

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

2012 AUG 28 PM 2:59

LEEANN FLYNN HALL  
CLERK OF COURT

~~TOP SECRET//SI//NOFORN~~

Office of the Assistant Attorney General

Washington, D.C. 20530

August 28, 2012

The Honorable John D. Bates  
Presiding Judge  
United States Foreign Intelligence Surveillance Court  
Washington, D.C. 20001

Dear Judge Bates:

~~(TS//SI//NF)~~ In response to your request, I am pleased to enclose a memorandum by the National Security Agency (NSA), memorializing representations made by the Department of Justice (DOJ) and NSA to the Court on July 24, 2012, regarding a compliance incident related to NSA's implementation of Section 5 (waiver provision) of its minimization procedures governing data acquired pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA).

~~(TS//SI//NF)~~ Specifically, the memorandum describes the facts and circumstances under which the incident occurred and confirms NSA's appropriate use and implementation of the waiver provision in other cases in which it was invoked. The memorandum also describes steps being taken by NSA, in coordination with DOJ, to ensure that NSA's interpretation and implementation of its authorities conducted pursuant to FISA are consistent with the statute, Court orders, and Court-approved procedures.

~~(TS//SI)~~ In addition to the steps being taken by NSA, DOJ reviewed its internal processes for reporting this incident. As described to the Court on July 24, 2012, DOJ recognizes that in light of related filings being presented to the Court at the same time this incident was discovered and the significance of the incident, DOJ should have reported this incident under our immediate notification process rather than in our Quarterly Report to the Court.

~~(TS//SI//NF)~~ The reviews conducted by NSA and DOJ into this particular incident have provided a valuable opportunity to identify areas in which the organizations can work together to enhance current processes with greater transparency and coordination. The initiatives described

~~TOP SECRET//SI//NOFORN~~

Classified by: ~~Lisa O. Monaco, Assistant Attorney General,  
National Security Division, Department of Justice~~

Reason: ~~1.4(c)~~

Declassify on: ~~28 August 2037~~

ACLU 16-CV-8936 (RMB) 000754

~~TOP SECRET//SI//NOFORN~~

in the attached memorandum reflect lessons learned from past compliance issues and are designed to strengthen NSA's compliance processes from a structural, managerial, and training perspective. Specifically, these initiatives are intended to help prevent systemic compliance issues, improve processes to identify and correct issues that may arise as early as possible, and create a framework to review existing practices, policies and training going forward.

(U) Let me thank you and your staff for your attention to these matters, and the opportunity to discuss them with you. We look forward to additional opportunities to brief the Court on our continued progress in this area. Should the Court have any additional questions or concerns, please do not hesitate to contact me.

Sincerely,



Lisa O. Monaco  
Assistant Attorney General for  
National Security

Enclosure

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~



NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755-6000

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

28 August 2012 2012 AUG 28 PM 2:59

LEE AIN FLYNN HALL  
U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

MEMORANDUM FOR ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY,  
UNITED STATES DEPARTMENT OF JUSTICE

SUBJECT: ~~(S//NF)~~ Discussion with the Foreign Intelligence Surveillance Court on 24 July 2012 regarding the waiver provisions of NSA's minimization procedures governing data acquired pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended.

~~(S//NF)~~ This memorandum memorializes the discussion between the Department of Justice (DOJ), the National Security Agency (NSA), and the Foreign Intelligence Surveillance Court (Court) on 24 July 2012 describing the facts and circumstances behind NSA's issuance of [redacted] waiver determination pursuant to Section 5 of NSA's minimization procedures relating to Section 702 of the Foreign Intelligence Surveillance Act, as amended,<sup>1</sup> confirming NSA's appropriate use and implementation of that provision in other cases, and detailing additional steps being taken by NSA, in coordination with DOJ, to ensure that NSA's interpretation and implementation of its authorities conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) are consistent with the statute, Court orders, and Court-approved procedures.

~~(S//NF)~~ Background Facts and Circumstances Regarding [redacted] Waiver Determination

~~(TS//SI//NF)~~ Since August 2008, Section 5 of NSA's FISA Amendments Act (FAA) 702 Minimization Procedures has permitted the Director of NSA (DIRNSA) to waive destruction of certain FAA 702 data, the destruction of which is otherwise required by the procedures, if DIRNSA "specifically determines, in writing" that one of the waiver criteria listed in the minimization procedures applies. One such criterion applies when a communication is "reasonably believed to contain significant foreign intelligence information."<sup>2</sup>

~~(TS//SI//NF)~~ Destruction waivers are most frequently sought when [redacted], [redacted] [redacted] has traveled to the United States, and NSA has acquired the target's communications before realizing the target entered the U.S. Even without a waiver, under these circumstances a separate provision of Section 5 of the minimization procedures provides that "if

<sup>1</sup> ~~(S)~~ See Section 5(1)-(4), Exhibit B, In re DNI/AG [redacted] "Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978," as Amended (hereinafter "NSA's FAA 702 Minimization Procedures" or "minimization procedures").

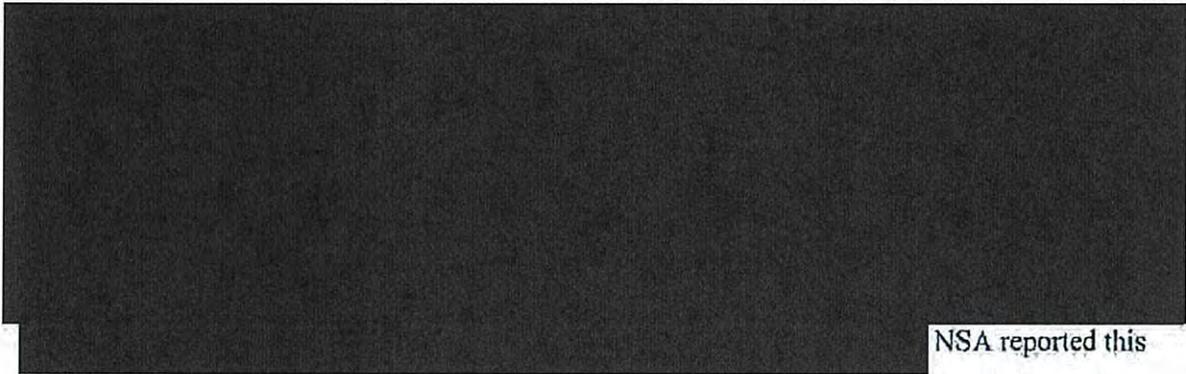
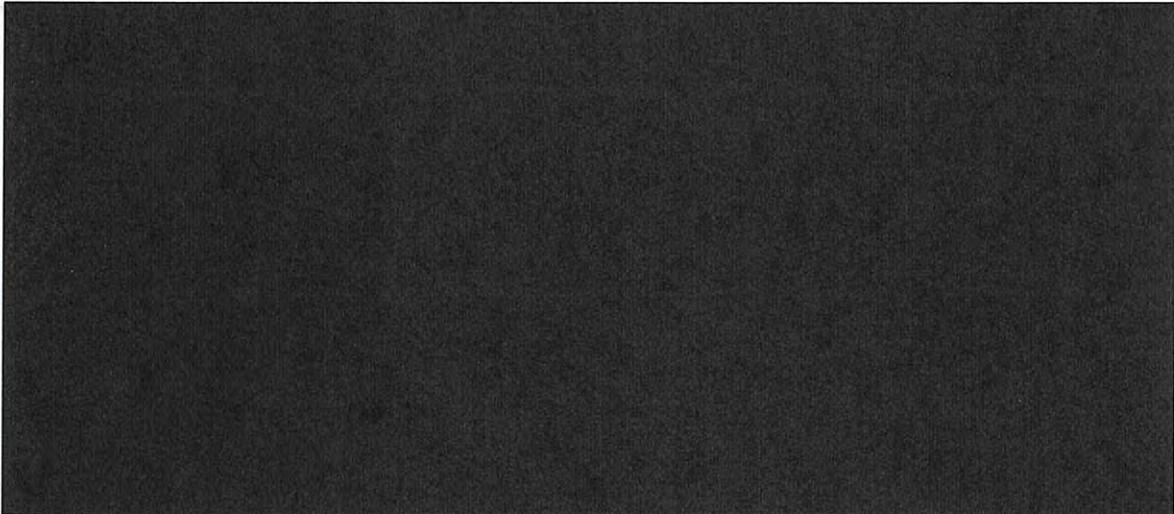
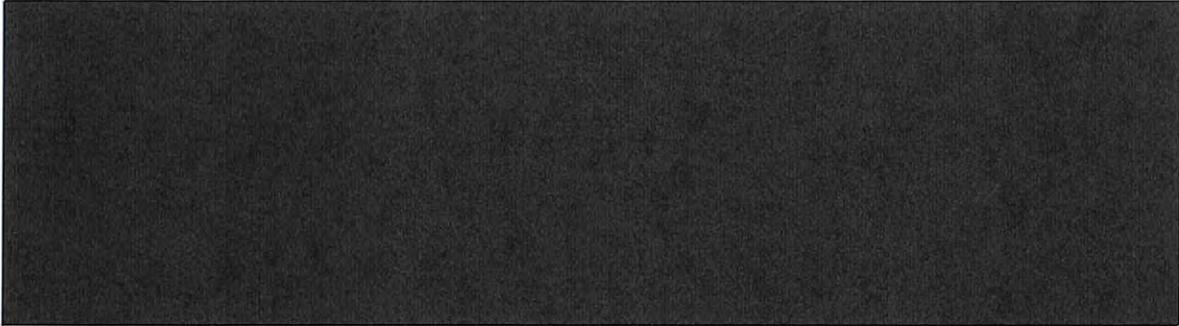
<sup>2</sup> ~~(S)~~ See Section 5(1), NSA's FAA 702 Minimization Procedures.

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 2037 [redacted]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

a domestic communication indicates that a target has entered the United States, NSA may advise FBI of that fact."<sup>3</sup>



NSA reported this

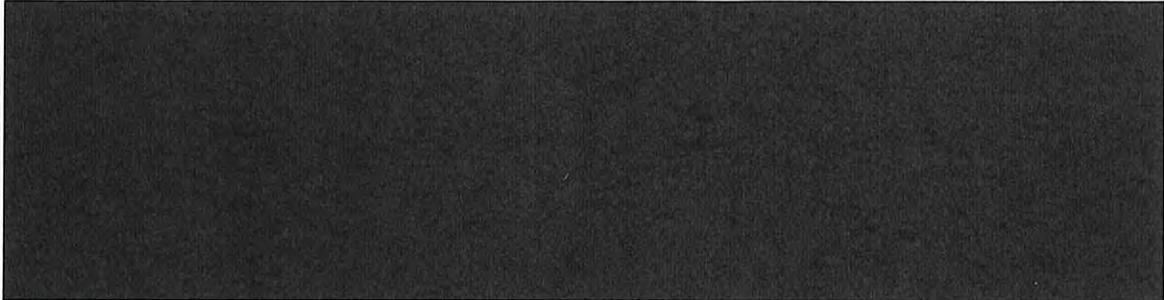
<sup>3</sup> (U//FOUO) See Section 5, NSA's FAA 702 Minimization Procedures.

<sup>4</sup> (U//FOUO) Although the focus of this correspondence is NSA's consultation with DOJ, both the Office of the Director of National Intelligence and the Department of Defense have important oversight roles with respect to NSA's intelligence activities.

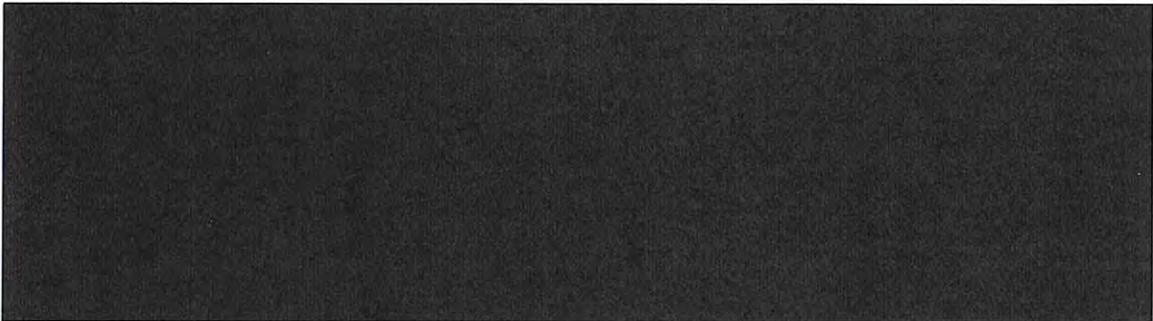
~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

incident and the results of the investigation to the Court in the December 2011 and March 2012 Quarterly Reports of FAA 702 compliance matters.



~~(S//NF)~~ Additional Waivers Issued Pursuant to Section 5 of NSA's Minimization Procedures



~~(TS//SI//NF)~~ Steps to Ensure that NSA's Interpretation and Implementation of its FISA Authorities are Consistent with the Statute, Court Orders, and Court-Approved Procedures

~~(S//NF)~~ NSA, in coordination with DOJ, has taken a number of steps to improve overall coordination of guidance involving significant interpretations of the FISA and to ensure a common understanding of the implementation requirements arising from such interpretations. Additionally, NSA continues to move forward with several internal initiatives to enhance the compliance infrastructure and strengthen NSA's visibility across its components from a programmatic level.

*1. (U) Coordination between NSA and DOJ in advance of significant FISA interpretations*

~~(TS//SI//NF)~~ NSA is committed to working with DOJ in advance of any decision that involves a significant interpretation of the FISA, a Court order, or Court-approved procedures. This advance coordination applies across all of NSA's activities executed pursuant to FISA, not

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

just those activities conducted pursuant to Section 702. NSA has a number of efforts underway to implement this enhanced coordination. For example, NSA has invited DOJ to participate in pre- and post-order reviews that NSA's Office of General Counsel hosts with NSA's operational, technical, and compliance personnel to ensure that there is a shared understanding of the collection activities conducted pursuant to Title I of the FISA; what is required by the applicable Court order; what is required by NSA's minimization procedures; and other requirements.<sup>5</sup> DOJ has participated in a number of these reviews already and anticipates participating in additional reviews on an ongoing basis. This builds on the experience NSA and DOJ have gained in participating in joint sessions to discuss and review complex collection activities, such as the bulk business record and pen register applications, and, more recently, drafting and implementing amendments to NSA's Section 702 minimization procedures to allow [REDACTED]

[REDACTED] These joint sessions create a formalized process to discuss new issues that may arise as well as ensure a common understanding of existing collection and implementation activities.

~~(TS//SI//NF)~~ NSA has seen the benefit of advanced coordination in its operational environment. [REDACTED]

~~(S//NF)~~ NSA and DOJ also conduct management coordination teleconferences to monitor pending FISA matters as well as to discuss progress on outstanding legal issues. These efforts help coordinate priorities and projects that advance mission and compliance objectives.

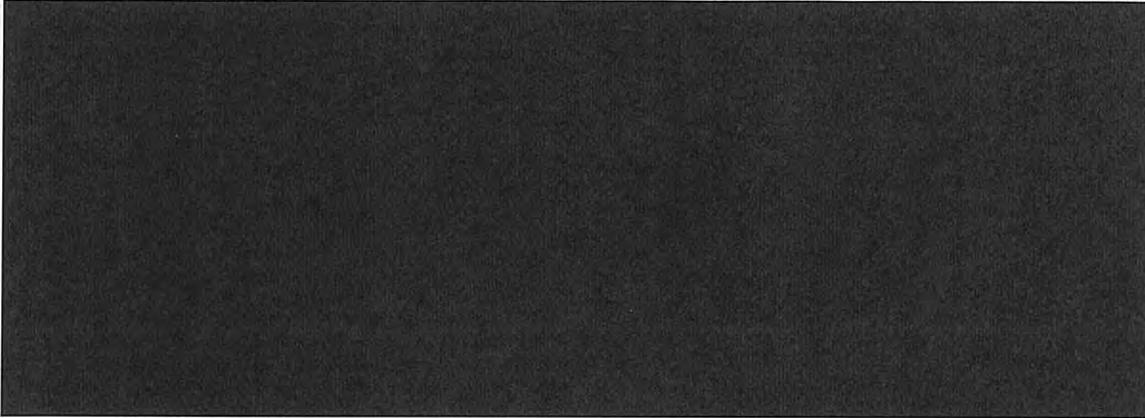
2. *(U) Coordination between NSA and DOJ to ensure a common understanding of implementation requirements*

~~(S//NF)~~ NSA and DOJ continue to work together to develop a process to coordinate official guidance and training materials on an ongoing basis. For example, although DOJ has [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

previously reviewed some of NSA's existing FAA 702 training materials, NSA has been identifying additional internal training and employee guidance related to its implementation of Section 702 of the FISA and sharing it with DOJ. In addition, NSA and DOJ personnel are increasing participation in each others' internal training, including training on general operational matters in addition to FISA-related training.



~~(S//NF)~~ NSA, in coordination with DOJ, is also working to develop processes to more effectively memorialize and track substantive representations to the Court that may not be expressly captured in the Government's written filings or the Court's resulting orders. 

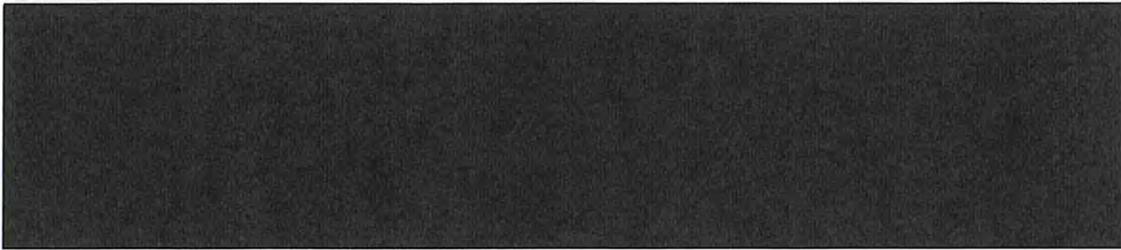


3. *(U) Ongoing NSA Initiatives and Programmatic Improvements*

~~(S//NF)~~ NSA has taken several steps to improve its management and understanding of the rules and interpretations of the FISA statute, FISC orders, and FISC-approved procedures.  efforts are intended to provide NSA's attorneys, policy officers, and compliance officers with a common set of searchable documents that will provide the basis to ensure shared understanding and interpretations of the applicable law, Court orders, and Court-approved minimization procedures, develop internal policies, and further build NSA's compliance program. NSA's Office of the Director of Compliance is spearheading an effort to manage, organize, and maintain the authorities, policies, and compliance requirements that govern NSA mission activities. 



~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

~~(S//NF)~~ Additionally, NSA has established an Authorities Integration Group, which is accountable to the DIRNSA for managing authority-related changes/additions/deletions across NSA in a holistic manner that integrates mission operations, technology, legal, policy, and compliance elements. The Authorities Integration Group includes individuals designated as Authority Leads to manage the activities within a particular authority, e.g., a Title I FISA Authority Lead, a Section 702 Authority Lead, etc. The Chair of the Authorities Integration Group reports to NSA's Deputy Director.

(U) Conclusion

~~(S//NF)~~ In sum, these efforts are intended to strengthen NSA's overlapping compliance safeguards from a structural, managerial, and training perspective. NSA is a large organization with many diverse components serving specialized and complex functions. The intent of the steps described herein is to ensure representations made to the Court reflect an accurate and shared understanding of how NSA's FISA-related authorities are being interpreted and implemented, both within NSA as well as with DOJ and NSA's other external partners. NSA has always viewed DOJ as a critical partner, and both organizations are working closely together to enhance current processes with greater transparency. Although mistakes can never be entirely avoided in a complex operational environment, the steps described herein will help prevent systemic problems, create mechanisms to expeditiously identify and correct mistakes that may occur, and create a framework to review existing practices and policies. NSA will continue to inform both DOJ and the Court of the status of NSA's efforts to improve its overall compliance posture.

  
JOHN C. INGLIS  
Deputy Director

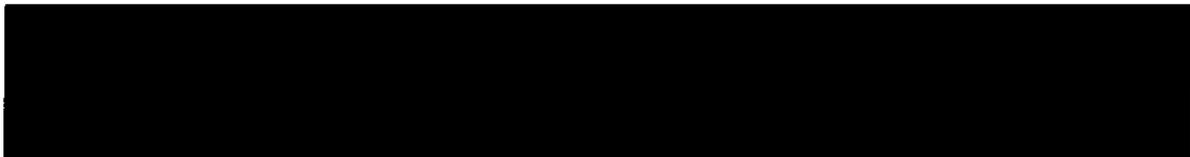
~~TOP SECRET//COMINT//NOFORN~~

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

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

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

MAR 17 AM 11:40  
CLERK OF COURT



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] 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

~~TOP SECRET//COMINT//NOFORN//20320108~~**(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]

[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”).<sup>1</sup>

~~(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]

<sup>1</sup> (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~~

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

ACLU 16-CV-8936 (RMB) 000763

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

Internet Service Providers (“ISPs”) provide information contained in targeted accounts under the ISP’s control;

[REDACTED]

[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]

<sup>2</sup> (U) Examples of [REDACTED]

<sup>3</sup> (U) As used in this context, [REDACTED]

<sup>4</sup> ~~(TS//SI//NF)~~ [REDACTED]

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

[REDACTED]

~~(TS//SI//NF)~~ Not only does [REDACTED] compensate for [REDACTED]  
[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]  
[REDACTED] may help NSA ascertain [REDACTED]  
previously unknown individuals who may also possess and/or communicate valuable foreign  
intelligence information. Additionally, [REDACTED]

[REDACTED]

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

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

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

<sup>5</sup> ~~(TS//SI//NF)~~ [REDACTED]

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

[REDACTED]

III ~~(TS//SI//NF)~~ [REDACTED] **Overcollection and the Evolution of NSA's [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.<sup>6</sup> As described previously, the [REDACTED] provides unique foreign intelligence information. However, it also comes with the potential for producing overcollection, including [REDACTED] Overcollection ("O"). [REDACTED] 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]

<sup>6</sup> ~~(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.

<sup>7</sup> ~~(TS//SI//REL)~~ [REDACTED]

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

[REDACTED]

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

[REDACTED]

B. ~~(TS//SI//NF)~~

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

[REDACTED]

<sup>8</sup> ~~(TS//SI//NF)~~

[REDACTED]

<sup>9</sup> ~~(TS//SI//NF)~~

[REDACTED]

<sup>10</sup> ~~(TS//SI//NF)~~

[REDACTED]

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

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

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

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

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

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

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

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

[REDACTED]

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

[REDACTED]

D. ~~(TS//SI//NF)~~

~~(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].

[REDACTED]

<sup>12</sup> ~~(TS//SI//NF)~~

[REDACTED] Table I briefly summarizes each incident.

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

[REDACTED]

(TS//SI//NF) A summary of all [REDACTED] recent overcollection incidents is provided in Table 1. The [REDACTED] additional incidents referenced on page 15 of the Government's Response<sup>14</sup> 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]

[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]

[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]

<sup>13</sup> (U//FOUO) [REDACTED]

<sup>14</sup> (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.

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

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

[REDACTED]

[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]

[REDACTED] NSA continues to track and routinely monitor [REDACTED] looking for anomalies [REDACTED] that 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.

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

## 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]

[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]. 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

<sup>15</sup> ~~(TS//SI//NF)~~ [REDACTED]

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

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.<sup>16</sup> 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.<sup>17</sup>

~~(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 all 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

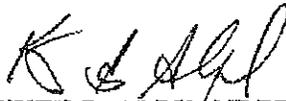
~~(TS//SI//NF)~~ As discussed above, NSA has developed new generation [REDACTED] and new generation [REDACTED] which greatly reduce the likelihood of overcollection or the extent to which it might occur. NSA has also developed [REDACTED] as an additional layer of protection against [REDACTED] O incidents. 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).

<sup>16</sup> ~~(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] that may occur would involve even smaller volumes of overcollected communications.

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

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

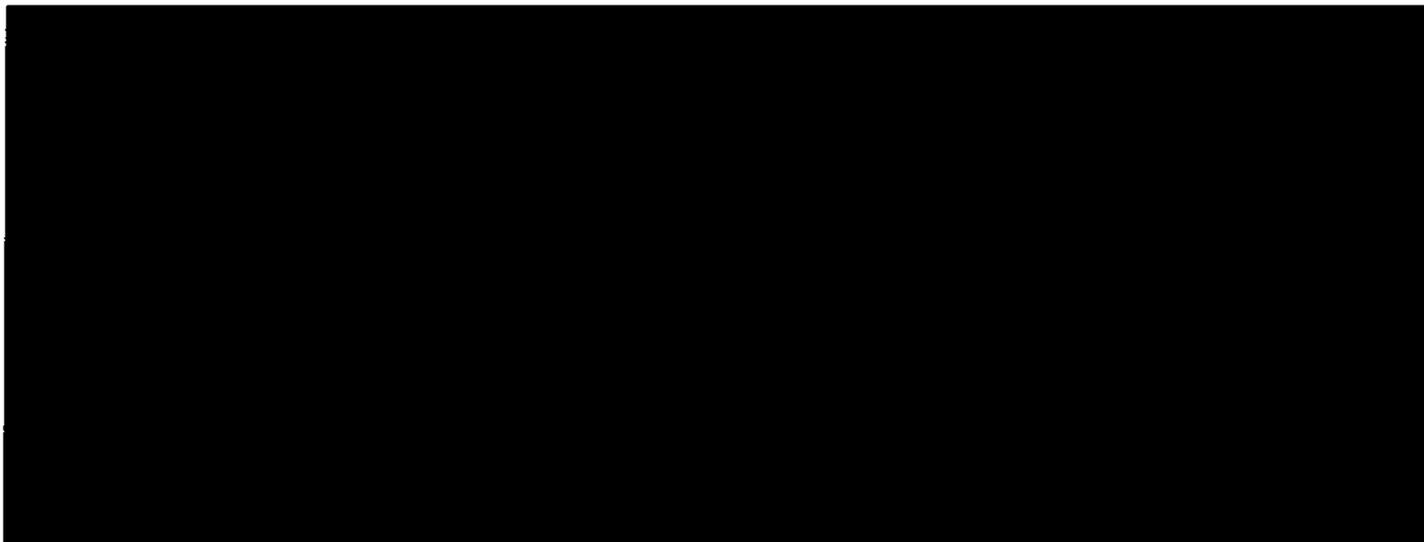
~~(TS//SI//NF)~~ Except in the [REDACTED] NSA has been able to identify the causes of the incidents of overcollection and has taken extensive and multi-layered steps to prevent similar incidents in the future. NSA has purged all of the data it has identified as overcollection. There is no guarantee that future [REDACTED] problems will not occur, or that future [REDACTED] changes, which NSA may not have anticipated, and which [REDACTED] [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.



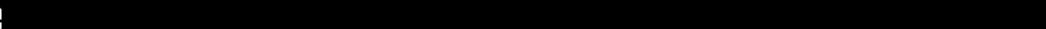
KEITH B. ALEXANDER  
Lieutenant General, U.S. Army  
Director, National Security Agency

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

**Table 1. Summary of Overcollection Incidents**



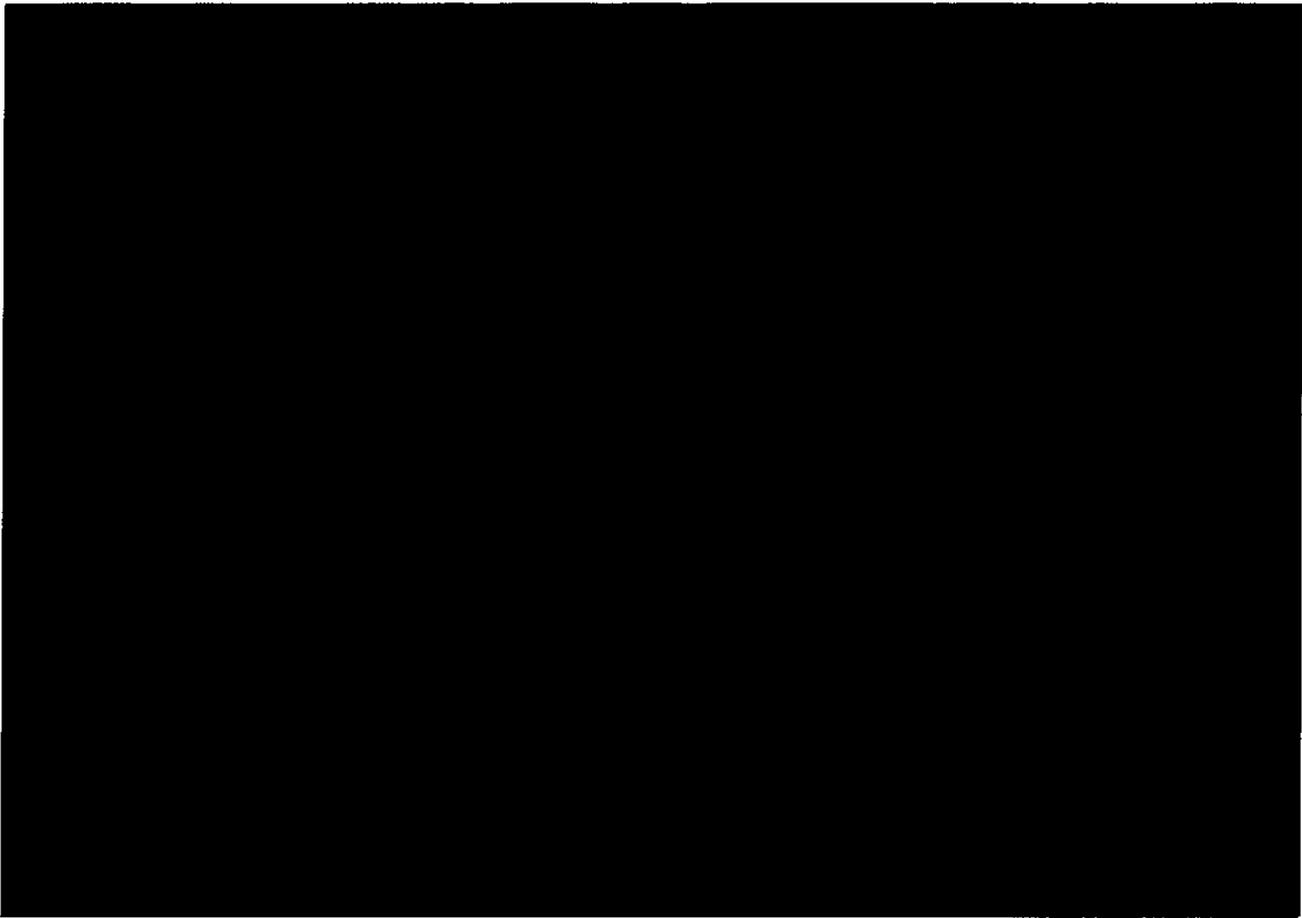
<sup>18</sup> ~~(TS//SI//NF)~~ 

<sup>19</sup> ~~(TS//SI//NF)~~ 

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

**Table 2:**

**January 16, 2009**



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