MEMORANDUM FOR THE ASSISTANT TO THE SECRETARY OF DEFENSE (INTELLIGENCE OVERSIGHT)

SUBJECT: (U//FOUO) Required Actions for the CY 2010 Intelligence Oversight Report to Congress - INFORMATION MEMORANDUM

(U//FOUO) In accordance with your memorandum of 17 November 2010, the enclosed consolidation of the National Security Agency’s Quarterly Reports to the President’s Intelligence Oversight Board for calendar year 2010 is provided to assist the Secretary of Defense in preparation of his Annual Report to Congress.

GEORGE ELLARD
Inspector General

Encl:
Annual Report

This document may be declassified and marked “UNCLASSIFIED/For Official Use Only” upon removal of enclosure(s)

Approved for Release by NSA on 12-19-2014, FOIA Case # 70809 (Litigation)
(U) National Security Agency/Central Security Service Annual Intelligence Oversight Report

I. (U) Intelligence, Counterintelligence, and Intelligence-Related Activities that Violated Law, Regulation, or Policy and Were Substantiated during the Year, as Well as Actions Taken as a Result of the Violations

A. (U) Intelligence Activities under Executive Order (E.O.) 12333 Authority

(U) Unintentional Collection against U.S. Persons (USPs) or Foreign Persons in the United States

(U//FOUO) During calendar year 2010 (CY2010), National Security Agency/Central Security Service (NSA/CSS) analysts on occasions inadvertently targeted or collected communications to, from, or about USPs while pursuing foreign intelligence tasking. All intercepts and reports have been deleted or destroyed as required by United States Signals Intelligence (SIGINT) Directive (USSID) SP0018.

1. (U) Targeting

(U//FOUO) During CY2010, procedural and human errors contributed to violations wherein NSA/CSS analysts targeted communications to, from, or about USPs or foreign persons in the United States.

a. (U//FOUO) On occasions during CY2010, NSA/CSS analysts tasked selectors associated with USPs.

b. (U//FOUO) On occasions during CY2010, selectors for valid foreign intelligence targets were not detasked while the targets were in the United States.

(U//FOUO) * For purposes of this report, “foreignness” refers to a target’s status with respect to being located outside the United States.

(U//FOUO) Table 1: E.O. 12333 – Targeting Violations, CY2010

<table>
<thead>
<tr>
<th>Violation Description</th>
<th>No. of Occasions</th>
<th>No. of Selectors Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to review content of traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to verify foreignness* of the selector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human error – Analyst neglected to detask selectors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure by analyst(s) to share</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer failed to notify NSA/CSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selector was overlooked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to understand procedures</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* (U) Table 1 details the types and numbers of targeting violations that occurred during CY2010, categorized by the specific violation and the number of occasions and selectors affected.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20321123
2. (U) Database Queries

a. (S//REL TO USA, FVEY) During CY2010, NSA/CSS analysts on occasions performed overly broad or poorly constructed database queries that potentially targeted USPs. For example, queries used which

produced imprecise results.

b. (U//FOUO) On occasions, other errors contributed to violations. On occasions, NSA/CSS analysts used selectors associated with USPs. On occasions, NSA/CSS analysts used selectors associated with valid foreign targets located in the United States.

c. (U//FOUO) Note: Although the number of times an error occurred is noted, the number of times an analyst submitted a specific query to a raw database is not consistently known.

3. (U) Detasking Delays

(U//FOUO) On occasions during CY2010, USP selectors or selector s associated with valid foreign targets in the United States were not detasked as required.

(U//FOUO) Table 2: E.O. 12333 – Database Query Violations, CY2010

| Failure to verify foreignness of the selector | (b)(3)-P.L. 86-36 |
| Failure to understand proper procedures | |
| Failure by analyst to suspend the query | the United States |
| Analyst included in query dates during which target was known to be in the United States | |
| Analyst operating under erroneous guidance or information | |
| Failure by analyst(s) to share | the United States |
| Human error (analyst cut and pasted into query, or included known USP selector) | |

(U//FOUO) Table 3: E.O. 12333 – Detasking Delays, CY2010

| Failure to implement detask order | |
| Selector overlooked on a list of selectors to be detasked | |
4. (U) Retention

(U//FOUO) During CY2010, there was one instance of improper retention. Intercept of a valid foreign intelligence target in the United States was retained The improper retention occurred because an NSA/CSS analyst failed to mark the collection properly for deletion.

B. (U) Dissemination of U.S. Identities

(S//SI//REL TO USA, FVEY) NSA/CSS issued SIGINT product reports during CY2010. In those reports, SIGINT analysts disseminated communications to, from, or about USPs or entities on occasions while pursuing foreign intelligence tasking. A total of SIGINT products were found to be improper, and the reports were canceled as NSA/CSS analysts learned of the USPs, U.S. organizations, or U.S. entities named in products without authorization. All data in the canceled reports was deleted as required, and the reports were not reissued or were reissued with proper minimization.

C. (U) The Foreign Intelligence Surveillance Act (FISA)

1. (U) NSA/CSS Title I FISA

(U//FOUO) During CY2010, NSA/CSS incurred violations related to Foreign Intelligence Surveillance Court (FISC)-authorized targets.

(TS//SI//NF) Table 4: NSA/CSS Title I FISA Violations, CY2010

<table>
<thead>
<tr>
<th>No. of Occasions</th>
<th>No. of Selectors Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selector in use by an unauthorized target</td>
<td>(b)(1) (b)(3)-P.L. 86-36</td>
</tr>
<tr>
<td>Selector was misused</td>
<td>Raw traffic database, or other restricted data sources</td>
</tr>
<tr>
<td>USP selector included in NSA/CSS’s FISA application in error</td>
<td></td>
</tr>
<tr>
<td>Human error—Selector contained a typographical error</td>
<td></td>
</tr>
<tr>
<td>Target erroneously believed to belong to an entity authorized under a valid FISC Order</td>
<td></td>
</tr>
<tr>
<td>FISC Order was misunderstood</td>
<td></td>
</tr>
</tbody>
</table>

(TS//SI//NF) * The error occurred because an NSA FISC Order, which was renewed specified that only about which members were associated with authorized under the order could be tasked. The previous order allowed could be proved to be associated with authorized in the order were tasked and detasked.
(U) Detasking Delays

(FOUO) During CY2010, violations wherein the FISC-authorized target selectors were not detasked as required were discovered.

(FOUO) Table 5: NSA/CSS Title I FISA Violations – Detasking Delays, CY2010

<table>
<thead>
<tr>
<th>Miscommunication resulting in a failure to detask selector</th>
<th>No. of Occasions</th>
<th>No. of Selectors Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysts discovered targeted individuals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selectors were not fully detasked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human error – Analyst neglected to detask selector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional selector was overlooked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyst misunderstood detask requirements/procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selectors previously authorized had not been detasked prior to start of new FISC Order</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(FOUO) * The FISC directed that selectors for this target be verified every six months.

(FOUO) ** Applies to all blanks.

2. (TS//SI//NF) Business Records (BR) Order

During CY2010, there was one violation of the BR FISC Order. NSA/CSS discovered that BR metadata for a U.S. telephone identifier was queried on 9 March 2010 after authorization to target had expired on 7 March 2010. The incident occurred because the identifier was mislabeled authorized until 23 March 2010. In June 2010, NSA/CSS implemented a new program to revalidate automatically an identifier’s authorization status.

3. (U) FISA Amendments Act (FAA)

(U) Section 702

(FOUO) During CY2010, NSA/CSS analysts on occasions incurred violations of FAA §702 authority: targeting incidents, non-compliant database queries, detasking delays, and tasking errors.
a. (U) Targeting

(FOUO) Procedural or human error contributed to targeting violations.

<table>
<thead>
<tr>
<th>Occasions</th>
<th>Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyst misunderstood detask requirements/procedures</td>
<td></td>
</tr>
<tr>
<td>Selector was tasked using outdated foreignness</td>
<td></td>
</tr>
<tr>
<td>Selector was not detasked because of a software problem</td>
<td></td>
</tr>
<tr>
<td>Selector was detasked late because the United States</td>
<td></td>
</tr>
<tr>
<td>Citizenship was not reviewed (target was a U.S. citizen)</td>
<td></td>
</tr>
<tr>
<td>Failure by analyst to detask selector the United States by the target</td>
<td></td>
</tr>
<tr>
<td>Selector was tasked before approval</td>
<td></td>
</tr>
<tr>
<td>Incorrect selector was tasked – Insufficient research was conducted on selector</td>
<td></td>
</tr>
<tr>
<td>Failure to verify foreignness of the selector</td>
<td></td>
</tr>
<tr>
<td>Customer failed to notify NSA/CSS the United States</td>
<td></td>
</tr>
</tbody>
</table>

b. (U) Database Queries

(FOUO) On occasions, NSA/CSS analysts used selectors associated with USPs or a selector the United States in FAA §702 traffic database. On occasions, NSA/CSS analysts used selectors associated with FAA §702-authorized target(s) located in the United States.
c. (U) Detasking Delays

(U//FOUO) During CY2010, there were □ detasking delays wherein FAA §702-approved selectors were not detasked as required.
d. (U) Tasking Errors

(U//FOUO) There were FAA §702-related tasking errors in CY2010. In one instance, an NSA/CSS analyst inadvertently re-tasked selectors that had been detasked. Selectors were again detasked, and data collected from only of the selectors was purged. In the other instances, NSA/CSS analysts discovered that selectors for valid foreign intelligence targets had been tasked under the incorrect FAA §702 certification. The selectors were detasked.

e. (U) Retention

(U//FOUO) During the second quarter of CY2010, NSA/CSS implemented a new process to ensure that FAA collection that is required to be purged is purged from NSA/CSS databases. A to identify data that should be purged or aged off.

f. (U) Other

(S//SI//REL TO USA, FVEY) NSA/CSS reported to the Department of Justice (DoJ) and the Office of the Director of National Intelligence an instance in which

(S//SI//REL TO USA, FVEY) DoJ reported this to the FISC in accordance with the FISC Rules of Procedure.
(U) Section 704

(U/FOUO) There were violations of FAA §704 authority during CY2010. In instances, approved FAA §704 selectors were submitted to sites that were not approved for FAA §704 collection. The selectors were detasked, and there was no collection. The instance involved a non-compliant database query. The query was deleted, and there were no results. The final violation involved a 2-day detasking delay.

(U) Section 705b

(S//REL TO USA, FVEY) During CY2010, violations of FAA §705b authority were the result of non-compliant database queries, detasking delays, and one tasking error.

a. (U) Database Queries

(S//REL TO USA, FVEY) NSA/CSS is pursuing an initiative with DoJ to modify NSA/CSS’s §702 minimization procedures. If approved, this change would align NSA/CSS’s procedures with the Federal Bureau of Investigation’s (FBI) procedures, which permit such searches.

(S//REL TO USA, FVEY) Table 11: NSA/CSS FAA §705b – Database Query Violations, CY2010

<table>
<thead>
<tr>
<th>FAA §705b selectors used in query against FAA §702-authorized collection – Analyst was unaware target was under §705b authority</th>
<th>No. of Occasions</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAA §705b selectors used in query against FAA §702-authorized collection</td>
<td>(b)(1)</td>
</tr>
<tr>
<td>FAA §705b selectors used in query against FAA §702-authorized collection</td>
<td>(b)(3)-P.L. 86-36</td>
</tr>
<tr>
<td>FAA §705b selectors used in query against FAA §702-authorized collection – System problem</td>
<td></td>
</tr>
<tr>
<td>FAA §705b selectors used in query against FAA §702-authorized collection – Analyst was unaware list included §705b selectors</td>
<td></td>
</tr>
</tbody>
</table>
b. (U) Detasking Delays

(S//REL TO USA, FVEY) During CY2010, there were instances of detasking delays in which FAA §705b-authorized targets remained tasked after the authorization had expired.

<table>
<thead>
<tr>
<th>No. of Occasions</th>
<th>No. of Selectors</th>
<th>No. of Days Selector Tasked Past Required Detask Date</th>
<th>No. of Days Selector Tasked Past Required Detask Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selector overlooked on a list of selectors to be detasked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>was not instructed to detask selector</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(S//REL TO USA, FVEY) Table 12: NSA/CSS FAA §705b – Detasking Delays, CY2010

(c. (U) Tasking Errors

(TS//SI//F) NSA/CSS analysts discovered that selectors associated with an FAA §705b-authorized target were erroneously tasked. The selectors, remained on task before the selectors were detasked. There was no collection.

4. (U) Data Handling Errors

(U/FOUO) On occasions during CY2010, FISA- or FAA-derived information was available to NSA/CSS analysts not cleared for access. On of these occasions, NSA/CSS analysts inadvertently forwarded FISA- or FAA-derived information via e-mail to unauthorized recipients. On of these occasions, e-mail was sent to an alias that included NSA/CSS analysts not cleared for FISA- or FAA-derived information.
5. (U) Unauthorized Access

(U//FOUO) NSA/CSS reported during CY2010 seven instances in which database access to FISA- and FAA-derived information was not terminated when access was no longer required. Once identified, the accesses were terminated.

D. (U) Other

1. (U) Computer Network Exploitation (CNE)

2. (U) Consensual and Other Collection

(U//FOUO) In CY2010, there were instances in which consensual collection agreements expired and the selectors remained tasked. In instances, because of human error, tasking continued for one additional day. There was no collection. In the last instance, tasking continued for six days because the IC customer provided an incorrect date for the target’s return to the United States. All collection was deleted, and no reports were issued.

(U//FOUO) Also during CY2010, NSA/CSS analysts discovered that an incorrect selector was tasked in support of two IC agency-sponsored consensual orders. There was no collection, and no reports were issued.

(TS//SI//REL TO USA, FVEY) an NSA/CSS analyst queried a raw traffic database using a USP’s telephone selector outside the Director, NSA/CSS (DIRNSA)-authorized period to query and task the selector. DIRNSA had authorized collection on telephone selectors associated with two U.S. hostages. The authorization allowed tasking and querying on the
E. (U) Intelligence-Related Activities

(S//SI//NF) To reduce the risk of unauthorized telephony collection and prevent violations, NSA/CSS instituted a process that gives analysts greater and faster insight into a target’s location. When collection did occur, data was purged from NSA’s principal raw traffic repositories, when required.

(SI//NF) NSA/CSS analysts found instances of unauthorized access to raw SIGINT. When collection occurred, it was purged from NSA/CSS’s principal raw traffic repositories, when required.

(U//FOUO) Although not violations of E.O. 12333 and related directives, NSA/CSS reported during CY2010 instances in which database access was not terminated when access was no longer required. Once identified, the accesses were terminated. NSA/CSS also reported instances of unauthorized access to raw SIGINT.

II. (U) NSA Office of the Inspector General (OIG) Intelligence Oversight (IO) Inspections, Investigations, and Special Studies

A. (U) Intelligence Oversight Inspections
(U//FOUO) During CY2010, the OIG reviewed various intelligence activities of the NSA/CSS to determine whether they had been conducted in accordance with statutes, executive orders, Attorney General procedures, and Department of Defense (DoD) and internal directives. With few exceptions, the problems uncovered were routine and showed that operating elements understand the restrictions on NSA/CSS activities.

1. (U) NSA/CSS Georgia

(U//FOUO) The NSA/CSS Georgia IO program, although not fully mature, has significantly improved since the last inspection. The program lacks a review element to assess the adequacy of oversight controls within NSA/CSS Georgia and tenant organizations. Processes put in place are not evaluated for efficiency, effectiveness, or compliance. Mission elements do not receive risk management reviews through the IO program to evaluate oversight controls commensurate with high-risk mission areas. Reviews to assess effectiveness of processes used to add and remove employees from IO training tracking systems, assess training compliance, and conduct analysis of incorrectly answered IO test questions are not conducted. The NSA/CSS OIG will update actions taken by NSA/CSS Georgia to address the inspection findings in a future report.

2. (U//FOUO)

(U//FOUO) The IO program has undergone several leadership changes in the past few years and, as a result, is still maturing. The site’s program would benefit from continued attention to documentation of processes and procedures. The site does not have standard operating procedures (SOP) for IO. Records documenting compliance with IO training requirements for personnel are incomplete; however, compliance with the required IO annual refresher training is good.

3. (U//REL TO USA, FVEY) During an OIG review, NSA/CSS discovered that there was no formal process to verify whether individuals with access to had been appropriately trained. had deleted accounts because the individuals no longer required access to the data. account holders obtained required USSID SP0018 training, and account holders obtained required clearances. To prevent future unauthorized access, the established a formal account request process by which clearances are verified before accounts are created.

4. (U) Cryptologic Services Group (CSG)
CSG had no documented procedures for accomplishing IO training of and for completing IO quarterly reporting. Although the CSG Chief was designated as the IO Officer (IOO), no alternate IOO was designated. During the CSG Chief’s extended absence, the site had no official IO point of contact. An alternate IOO, who was designated before the inspection began, is drafting SOP for IO training and for incident and quarterly reporting.

5. (U)  

The IO program has improved significantly since the 2007 inspection. The IO Program Manager (IO PM), now a full-time employee, has been in the position for four years, providing continuity for the site’s IO program. The site’s IO processes and procedures have been shared as a best practice with IO PMs throughout the NSA/CSS extended enterprise. To assist in handling increased oversight responsibilities, the IO PM delegated certain IO functions to experienced personnel in key mission areas where there is risk for exposure to USP information. Despite the delegation of functions, the IO PM does not have an officially designated alternate, creating a single point of failure. This was noted as a program weakness in inspections in 2004 and 2007. The OIG will track corrective actions.

5. (U)  

with NSA Analysis and Production Managers, oversees the SIGINT mission performed a under the DIRNSA SIGINT authority. The IO Coordinator has established a viable IO Program that enables management of the extensive IO responsibilities. Forward-deployed personnel in AORs that are in constant flux follow documented procedures to manage data. Branch procedures are easily accessible to personnel with implementation responsibilities.

B. (U) IO Training

As a part of NSA/CSS’s Comprehensive Mission Compliance Program, NSA/CSS is working to modernize existing compliance and IO training programs. IO training consists of a review of laws, regulations, and policies pertaining to NSA/CSS. Effective 1 July 2010, review of DoD’s Directive Type Memorandum 08-052 became part of the NSA/CSS core IO training.
(U) ACRONYMS AND ORGANIZATIONS

(U) BR  Business Records
(U) CNE  Computer Network Exploitation
(U) CSG  Cryptologic Services Group
(U) CY  Calendar Year
(U) DIRNSA  Director, National Security Agency
(U) DoD  Department of Defense
(U) DoJ  Department of Justice
(U) E.O.  Executive Order
(U) FAA  Foreign Intelligence Surveillance Act Amendments Act
(U) FBI  Federal Bureau of Investigation
(U) FISA  Foreign Intelligence Surveillance Act
(U) FISC  Foreign Intelligence Surveillance Court
(U) IC  Intelligence Community
(U) IO  Intelligence Oversight
(U) IOO  Intelligence Oversight Officer
(U) IO PM  Intelligence Oversight Program Manager
(U) NSA/CSS  National Security Agency/Central Security Service
(U) OIG  Office of the Inspector General
(U) SIGINT  Signals Intelligence
(U) SOP  Standard Operating Procedures
(U) USP  U.S. person
(U) USSID  United States Signals Intelligence Directive

(b)(3)-P.L. 86-36