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

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

16 May 2013

MEMORANDUM FOR THE CHAIRMAN, INTELLIGENCE OVERSIGHT BOARD

THRU: Assistant to the Secretary of Defense (Intelligence Oversight)

SUBJECT: (U//~~FOUO~~) Report to the Intelligence Oversight Board on NSA Activities - INFORMATION MEMORANDUM

(U//~~FOUO~~) Except as previously reported to you or the President or otherwise stated in the enclosure, we have no reason to believe that intelligence activities of the National Security Agency during the quarter ending 31 March 2013 were unlawful or contrary to Executive Order or Presidential Directive and, thus, should have been reported pursuant to Section 1.6(c) of Executive Order 12333, as amended.

(U//~~FOUO~~) The Inspector General and the General Counsel continue to exercise oversight of Agency activities by inspections, surveys, training, review of directives and guidelines, and advice and counsel.

George Ellard

DR. GEORGE ELLARD
Inspector General

RAJESH DE
General Counsel

(U//FOUO) I concur in the report of the Inspector General and the General Counsel and hereby make it our combined report.

KEITH B. ALEXANDER
General, U. S. Army
Director, NSA/Chief, CSS

Encl:
Quarterly Report

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

(U) REPORT TO THE INTELLIGENCE OVERSIGHT BOARD ON NSA ACTIVITIES FIRST QUARTER CY2013

(U//~~FOUO~~) Pursuant to Executive Order 12333 (E.O. 12333), as amended, National Security Directive No. 42, and other legal and policy directives, the National Security Agency (NSA/Agency) conducts signals intelligence (SIGINT) and information assurance (IA) activities on behalf of the U.S. government. NSA's SIGINT and IA operations, as well as activities in support of those operations, might result in the acquisition of non-public information about or concerning U.S. persons (USPs). Agency personnel are required to follow procedures designed to protect USP privacy, consistent with the Fourth Amendment to the U.S. Constitution and other law. NSA has also established internal management controls to provide reasonable assurance that NSA personnel are complying with procedures for handling USP information, such as minimization procedures adopted by the Attorney General (AG) and approved by the Foreign Intelligence Surveillance Court (FISC) to govern USP information acquired during SIGINT operations conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) of 1978, as amended. This report summarizes incidents of non-compliance with NSA's USP procedures, as well as other matters required to be reported to the Intelligence Oversight Board, that were identified during the first quarter of CY2013.

I. (U) SIGINT Incidents

(U//~~FOUO~~) Section 1.7(c)(1) of E.O. 12333 authorizes NSA to collect (including through clandestine means), process, analyze, produce, and disseminate SIGINT data for foreign intelligence and counterintelligence purposes to support national and military missions. However, FISA regulates the intentional acquisition of communications to or from unconsenting USPs, wherever such persons may be located, and also regulates certain collection techniques, particularly techniques used against persons located inside the United States. As a result, NSA personnel distinguish between E.O. 12333 SIGINT operations and activities that NSA conducts pursuant to FISA authorizations.

I.A. (U) E.O. 12333 SIGINT Incidents

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//NF)~~ During the reporting period, NSA determined that [redacted] incident reports indicated non-compliance with AG-approved procedures in Department of Defense (DoD) Regulation 5240.1-R, including the regulation's Classified Annex, as well as incidents of non-compliance with internal control procedures that govern NSA's acquisition, processing, retention, and dissemination of USP information acquired during E.O. 12333 SIGINT operations. [redacted] incidents involved acquisition errors, such as the mistaken or inadvertent targeting of a USP; [redacted] concerned improper queries of NSA raw SIGINT databases (unminimized and unevaluated for foreign intelligence), such as queries that were overly broad or not reasonably designed to restrict the return of non-pertinent or unauthorized USP information or were performed without first conducting the necessary research; [redacted] involved unauthorized access to or improper handling of raw SIGINT data; and [redacted] involved

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380501

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

(b)(1)
(b)(3)-P.L. 86-36

system errors. In light of the scope and scale of NSA's E.O. 12333 SIGINT operations [redacted] e-mail addresses, telephone numbers, and other "selectors" were tasked for E.O. 12333 SIGINT collection during the reporting period), the overall error rate was extremely low.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024

~~(S//SI//REL TO USA, FVEY)~~ [redacted]

(U//~~FOUO~~) The vast majority of E.O. 12333 incidents during the reporting period occurred because of human error and were addressed through remedial training of the responsible personnel. Noteworthy E.O. 12333 SIGINT incidents included the following:

- ~~(TS//SI//NF)~~ During this quarter, the NSA Office of the Inspector General (OIG) learned that a data spillage had occurred [redacted] involving communications intelligence (COMINT). Approximately [redacted] time-sensitive reports containing TOP SECRET COMINT information [redacted] the reports were available to personnel cleared only for SECRET information. All of the reports have been removed from the known locations, and a damage assessment is under way.
- ~~(TS//SI//REL TO USA, FVEY)~~ [redacted] database query ran against [redacted] selector that contained a typographical error. The analyst attempted to stop the query [redacted] but did not follow the correct process, [redacted] when the database auditor discovered the error. [redacted] No query results were returned.

(b)(1)
(b)(3)-P.L. 86-36

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-
(b)(3)-50 USC 3

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an auditor discovered that an analyst had queried [redacted] selectors without performing the necessary foreignness checks. No results were returned, and no reports were issued.
- ~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query in a raw SIGINT database [redacted] The query results were deleted, and no reports were issued. [redacted] has been suspended.

(b)(1)
(b)(3)-P.L. 86-36

- (S//SI//NF) it was discovered that a systems error mistakenly allowed selectors identified as USPs to be approved for tasking No collection occurred.
- (TS//SI//NF) an analyst discovered a glitch in a tasking tool that resulted in selectors All selectors were detasked
- (TS//SI//NF) it was discovered that selectors all improperly routed data was deleted. An error in the configuration files caused the incident.
- (U//FOUO) it was discovered that a file containing raw SIGINT had been uploaded into a repository that unauthorized personnel could have accessed The file was deleted.
- (TS//SI//NF) an analyst discovered collection acquired during a target's visit to the United States from a selector The incident was isolated to a particular
- (TS//SI/TK//REL TO USA, FVEY) Purging of the collected data was completed
- (TS//SI//REL TO USA, FVEY) it was discovered that a selector determined to be associated with a USP because of a miscommunication Upon discovery of the incident, the analyst immediately stopped the query and deleted the results.
- (S//REL TO USA, FVEY) was discovered to have been conducting SIGINT without proper authority. conducted an unapproved collection exercise, did not understand the importance of obtaining the proper legal authority for conducting SIGINT exercises before Moreover, the Program Manager had been fielding it to without the knowledge or oversight of the at Fort Meade. is contacting as currently possessing SIGINT systems or scheduled to receive a SIGINT system in the near future to make them aware of SIGINT oversight requirements.

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

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-
(b)(3)-50 USC 3

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

I.B. (U) FISA Incidents

~~(S//SI//NF)~~ During the reporting period, the Department of Justice (DOJ) filed [ ] notices with the FISC concerning incidents of non-compliance with authorizations issued to NSA pursuant to FISA, including incidents of non-compliance with NSA's Court-approved FISA minimization procedures. There were [ ] incidents of non-compliance with NSA internal control procedures. A total of [ ] of the incidents involved acquisition errors, such as the delayed detasking of targets; [ ] concerned improper queries of NSA raw SIGINT databases, such as queries that were overly broad or not reasonably designed to restrict the return of non-pertinent or unauthorized USP information; [ ] involved unauthorized access to or improper handling of raw SIGINT data; and [ ] involved systems errors. (Some incidents might cause more than one notice to DOJ, and some notices did not involve incidents. Consequently, the number of notices does not correspond to the number of incidents.)

(U//~~FOUO~~) The vast majority of FISA incidents during the reporting period occurred because of human error and were addressed through remedial training of the responsible personnel. Noteworthy FISA incidents included:

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

I.B.1. (U//~~FOUO~~) NSA/CSS Title I FISA

- ~~(TS//SI//NF)~~ While renewing the authority [ ] NSA discovered [ ] No communication to or from these numbers was acquired.
- ~~(TS//SI//NF)~~ [ ] NSA discovered that a [ ] had not been detasked [ ] All collection has been purged, and no reporting occurred.
- ~~(TS//SI//NF)~~ [ ] All communications [ ] have been purged, and no reporting based on the non-compliant collection occurred.
- ~~(TS//SI//NF)~~ [ ] the FISC granted a motion to amend the Order to address this situation.
- ~~(TS//SI//NF)~~ [ ]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

All of the non-compliant data was marked for purging, and no reporting occurred.

- ~~(S//SI//NF)~~ it was discovered that files possibly containing information acquired pursuant to FISA had been inadvertently placed on a Upon discovery, all files were deleted.

(b)(1)
(b)(3)-P.L. 86-36

- ~~(S//SI//NF)~~ an analyst discovered some FISA-acquired information A final notice on the matter was filed with the FISC

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36

I.B.2 ~~(S//REL TO USA, FVEY)~~

- ~~(S//SI//REL TO USA, FVEY)~~ an analyst executed query of identifiers provided to NSA by with a high risk of terrorist connections. NSA queries non-USP identities against its collection and reports to results of those queries. When the NSA analyst executed the query, he was unaware NSA deleted the results from the query and confirmed that the results had not been disseminated or otherwise used.

- ~~(TS//SI//REL TO USA, FVEY)~~ NSA discovered that analysts without training might have been able to see data Although no data was found in pursuant to authorization. The analysts have since attended training.

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

I.B.3. ~~(TS//SI//NF)~~ Business Records (BR) Order

- ~~(TS//SI//NF)~~ an NSA analyst executed a valid query in NSA's BR repository using a reasonable articulable suspicion-approved selector belonging to a USP currently subject to The analyst then sent the results of the query via an e-mail alias to personnel who did not have the required training to handle the BR data. The analyst's supervisor rectified the situation.

- ~~(TS//SI//NF)~~ NSA technical personnel discovered that NSA had inadvertently retained files containing call detail records that exceeded the five-year retention period. These records, which had been produced pursuant to the FISC's Primary Orders, The records were among those used in connection with a migration of call detail records to a new system in or about The call detail records could be accessed or used only by technical personnel who had received appropriate and adequate training. NSA

(b)(1)
(b)(3)-P.L. 86-36

technical personnel destroyed the call detail records used in the migration of records that had been retained past the five-year limit.

I.B.4. (U) FISA Amendments Act (FAA)

- (TS//SI//REL TO USA, FVEY) On occasions during the first quarter, collection occurred on the United States

- (TS//SI//REL TO USA, FVEY) FAA §702 data was erroneously distributed have been marked for deletion from the repository.

(b)(1)
(b)(3)-P.L. 86-36

- (TS//SI//REL TO USA, FVEY) it was discovered that NSA personnel had learned that the user of selectors had the United States The selectors had inadvertently remained tasked All non-compliant data collected from has been marked for purging. No reports were issued.

- (TS//SI//REL TO USA, FVEY) NSA personnel discovered that selectors had been incorrectly re-tasked under FAA §702 without adjudication, selectors were detasked upon discovery. All non-compliant FAA §702 data for each selector was marked for purging.

(b)(1)
(b)(3)-P.L. 86-36

- (TS//SI//NF) an NSA analyst erroneously tasked selectors without ascertaining whether the selectors were in the United States. Upon discovery of this error, the selectors were emergency detasked and all non-compliant FAA §702 data for each selector was marked for purging. No reports were issued.

- (TS//SI//REL TO USA, FVEY) NSA discovered that a database technical error, caused by unknown circumstances had prevented the complete processing of files. NSA provides for review for all new FAA §702 tasking. The are the subject of the under FAA targeting procedures. The database prevented certain from being loaded into database. Another technical error occurred also preventing from being loaded into the database. After being alerted to the situation, the NSA database team loaded the missing into the database

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

- (TS//SI//NF)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- ~~(TS//SI//REL TO USA, FVEY)~~ it was discovered that a detasking request had been made for a selector deemed to be no longer of interest. Further analysis revealed that the detasking request had not been carried out. The selector was in the United States The selector was detasked All non-compliant FAA §702 data collected from has been marked for purging. No reports were issued.

(b)(1)
(b)(3)-P.L. 86-36

- ~~(TS//SI//REL TO USA, FVEY)~~ it was discovered that between an analyst had e-mailed to as many as unauthorized analysts at a field location files containing data collected pursuant to FAA §702. Upon discovery of this incident, all sharing of raw SIGINT was stopped and was instructed to purge the erroneously shared FAA §702 data from
- ~~(TS//SI//REL TO USA, FVEY)~~ an analyst downloaded FAA §702 data from a raw traffic repository and stored it in a local computer directory that could be accessed by analysts who are not authorized for FAA §702 data. Upon discovery, the analyst moved the traffic to a directory where access can be limited to only analysts who are authorized for FAA §702 access.
- ~~(TS//SI//REL TO USA, FVEY)~~ During the week of a manager discovered that FAA §702 traffic had been shared with an unauthorized analyst since the beginning of The sharing was halted and the analyst was instructed to return the FAA §702 data. Management reminded division personnel that the sharing of FAA §702 data with unauthorized personnel is not permitted.

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

- ~~(TS//SI//REL TO USA, FVEY)~~ NSA discovered that an analyst without the proper FAA §702 training had the potential to see FAA §702 data The unauthorized user was removed from the until FAA §702 training is completed.
- ~~(TS//SI//REL TO USA, FVEY)~~ it was discovered that a file containing data collected under FAA §702 had not been restricted to allow only those trained for access to FAA §702 data. It is not known whether anyone without appropriate training had accessed the file. The file permissions were changed to restrict access to only analysts who have completed appropriate FAA §702 training.

(b)(1)
(b)(3)-P.L. 86-36

I.C. (U) Dissemination of U.S. Identities

~~(TS//SI//NF)~~ The NSA/CSS enterprise issued SIGINT product reports during the first quarter of CY2013. product reports incorrectly disseminated USP information, and the reports were recalled as NSA/CSS analysts learned of USPs.

(b)(1)
(b)(3)-P.L. 86-36

U.S. organizations, or U.S. entities named without authorization. All data in the recalled reports was deleted as required, and the reports were not re-issued or were re-issued with proper minimization.

(b)(1)
(b)(3)-P.L. 86-36

I.D. (U) Detection and Prevention of Violations

~~(TS//SI//NF)~~ NSA continues its process to identify when the users of properly tasked [redacted] the United States. NSA's [redacted] process identified [redacted] in the first quarter. Collected data was purged from NSA/CSS's raw traffic repositories. NSA's process for [redacted] in the first quarter. In all cases, information acquired during the period [redacted] the United States was purged.

II. (U) IA Incidents

(U//~~FOUO~~) National Security Directive No. 42 and §1.7(c)(6) of E.O. 12333 designate the Director of NSA as the U.S. government's National Manager for National Security Systems. NSA's Information Assurance (IA) responsibilities include authority for NSA to intercept encrypted or other official communications of U.S. Executive Branch entities or U.S. government contractors for communications security purposes; perform technical security countermeasure surveys to determine whether unauthorized electronic surveillance is being conducted against the United States; examine U.S. government national security systems and evaluate their vulnerability to foreign interception and exploitation; and assess the security posture of and disseminate information on threats to and vulnerabilities of national security systems. NSA's IA activities often result in the acquisition of non-public communications or other non-public information about or concerning USPs.

(U//~~FOUO~~) During the reporting period, NSA identified [redacted] incidents of non-compliance with the AG-approved procedures and NSA internal control procedures that govern the handling of USP information acquired during NSA's IA activities. The incidents were attributed to human error and were addressed through remedial training of the responsible personnel. Noteworthy IA incidents included:

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

- (U//~~FOUO~~) [redacted] an analyst released a tipper containing a hyperlink that provided recipients of the tipper access to a repository for analyzed Communications Security (COMSEC) data, even if the recipients lacked access credentials. A hyperlink had been provided in [redacted] additional tippers [redacted] All tippers have been recalled, and new procedures for issuing tippers have been established to prevent future occurrences. A security update has been developed to eliminate the bug that allowed the live link to function for those without authorized access to the COMSEC data.

III. (U) NSA/CSS OIG IO Inspections, Investigations, and Special Studies

(U//~~FOUO~~) During the first quarter of CY2013, the OIG reviewed NSA/CSS intelligence activities to determine whether they had been conducted in accordance with statutes, E.O.s, AG-approved procedures, and DoD and internal directives. The problems uncovered were routine, and the reviews showed that operating elements understand the restrictions on NSA/CSS activities.

- **(U) Joint Inspection: NSA/CSS Texas (NSAT)**

  ~~(S//REL TO USA, FVEY)~~ During the joint inspection of NSAT [redacted] (b)(1) (b)(3)-P.L. 86-36 [redacted] IO inspectors reviewed IO program management, IO training for site personnel, and application of IO standards in SIGINT mission activities performed at the site. The IO inspectors found an overall lack of IO documentation and noted the need for increased physical protection in mission spaces given NSAT's open architecture. Managing training at a site with significant military presence and ensuring compliance in SIGINT activities performed under multiple authorities pose challenges for NSAT leadership.

- **(U) Field Inspection:** [redacted]

  (U//~~FOUO~~) During the field inspection of [redacted] (b)(3)-P.L. 86-36 the IO inspector reviewed IO program management, tracking of IO training for site personnel, and general awareness of IO within the workforce. The inspector found that the site had not formally documented the IO program and that IO-related information was not readily accessible to site personnel. The OIG recommended that the site establish a web presence to provide IO information. The inspector also found that database accesses were not terminated when personnel moved to new assignments. The OIG recommended that the Intelligence Oversight Officer verify that database accesses associated with previous assignments be terminated.

- **(U) Special Study: Assessment of Management Controls Over FAA §702—Revised and Reissued**

  (U//~~FOUO~~) [redacted] the NSA OIG published a revised report on the results of a review of the management controls implemented to provide reasonable assurance of compliance with FAA §702. The original report, [redacted] was revised for classification discrepancies and because new information had been received after release of the original report. The study found that NSA control procedures are adequately designed to comply with FAA §702. Eleven recommendations were made for improving those controls.

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

- **(U) Ongoing Studies**

(U//~~FOUO~~) The following special studies were in progress during the quarter and will be summarized in subsequent quarterly reports:

- (U//~~FOUO~~) FAA §702 [redacted] (b)(3)-P.L. 86-36
- (U) [redacted] Auditing Control Framework for Signals Intelligence System Queries
- (U) [redacted] System
- (U) Technology Directorate Mission Compliance Program
- (U) Information Assurance Directorate Office of Oversight and Compliance Mission Compliance Program

IV. (U) Notifications

(U//~~FOUO~~) During the first quarter, a number of notifications were provided to Congress, including:

(b)(1)
(b)(3)-P.L. 86-36

- ~~(TS//SI//NF)~~ [redacted] NSA notified Congressional intelligence committees about an unauthorized disclosure of properly classified national security information derived from SIGINT. NSA became aware of this disclosure on [redacted] The NSA Office of General Counsel has filed a Crime Report with the DOJ on this unauthorized disclosure.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] NSA notified Congressional intelligence committees about a potential retention and dissemination compliance incident involving an NSA corporate database designed for long-term retention [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i

- ~~(TS//SI//NF)~~ [redacted] NSA notified Congressional intelligence committees about the FISC's opinion relating to [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

NSA purged the unauthorized collection and recalled all reporting based on those communications. [redacted] the FISC authorized such collection to be undertaken prospectively. (b)(1) (b)(3)-P.L. 86-36

V. (U) NSA/CSS IO Program Initiatives

- (U//~~FOUO~~) As reported in the second quarter CY2011 report, NSA/CSS is developing a tool to automate submission of mission compliance incident reports across the NSA/CSS enterprise. The [redacted] will become the Agency's central tool for reporting potential mission compliance incidents and will provide a streamlined management process, a central repository, and metrics data to support root cause identification and trend analysis. The [redacted] is expected to be implemented [redacted] With the implementation of the [redacted] NSA will be able to perform comprehensive trend analysis [redacted] (b)(3)-P.L. 86-36

VI. (U) Other Matters

(U//~~FOUO~~) During the reporting period, NSA identified two questionable intelligence activities of a serious nature and one potential crime, as defined in Directive-Type Memorandum 08-052. Each activity has been reported to Congress and has been described in Section IV.

(~~S//NF~~) The NSA OIG has concluded its investigation into an allegation mentioned in the third quarter CY2012 report that activity associated with [redacted] The allegation was unsubstantiated.

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

(~~TS//SI//NF~~) During the first quarter of CY2013, the AG was involved in [redacted] instances of intelligence-related collection activities associated with USP hostage and detainee cases.

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)