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

18 February 2010

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 any intelligence activities of the National Security Agency during the quarter ending 30 June 2009 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.

(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. These activities and other data requested by the Board or members of the staff of the Assistant to the Secretary of Defense (Intelligence Oversight) are described in the enclosure.

George Ellard
GEORGE ELLARD
Inspector General

PATRICK J. REYNOLDS
Acting 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
Lieutenant 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)

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

1. (U//~~FOUO~~) Intelligence, counterintelligence, and intelligence-related activities that violate law, regulation, or policy substantiated during the quarter, as well as actions taken as a result of the violations

(U) Intelligence Activities

~~(TS//SI//REL TO USA, FVEY)~~ **Unintentional collection against United States persons** This quarter, there were [redacted] instances in which Signals Intelligence (SIGINT) analysts inadvertently targeted or collected communications to, from, or about U.S. persons while pursuing foreign intelligence tasking. All intercepts and reports have been deleted or destroyed as required by United States SIGINT Directive (USSID) SP0018.

(U) Unauthorized Targeting

~~(TS//SI//NF)~~ A National Security Agency (NSA) analyst discovered [redacted] that [redacted] Electronic Mail (e-mail) selector remained tasked after an Attorney General authorization had expired on [redacted] The NSA analyst detasked all selectors on [redacted] before the authorization expired, but was not aware [redacted] [redacted] The unauthorized targeting took place from [redacted] when Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) 705b authorization was obtained. No collection occurred between [redacted] A review of the incident resulted in a change in operating procedures.

~~(S//SI//REL TO USA, FVEY)~~ A software update caused a [redacted] failure in one [redacted] resulting in collection of [redacted] between [redacted] The old version of the software was reloaded, and the [redacted] was rebuilt to correct the [redacted] problem. The collection was purged from the NSA database [redacted]

~~(TS//SI//NF)~~ [redacted] human error caused [redacted] [redacted] The mistake was found and corrected [redacted] [redacted] NSA Attorney General-approved minimization procedures do not permit NSA to use U.S. person identifiers as selection terms in repositories of collected communications. It is unknown how much, or even if, unauthorized data was collected, and it is not possible to sort the [redacted] [redacted] results from valid foreign intelligence targeting results or purge the data by referencing the U.S. person selector without further Executive Order (E.O.) 12333 violations.

~~(TS//SI//NF)~~ [redacted] selectors belonging to a U.S. person were retasked by mistake. The telephone selectors had been detasked [redacted] when NSA analysts learned of the target's U.S. citizenship, but the detasking analyst failed to [redacted] Consequently, the selectors were retasked [redacted] [redacted] intercepts were collected. The selectors were detasked and appropriately marked to

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

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

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

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

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

prevent tasking, and the related collection was purged from the NSA database [redacted] No reports were issued.

~~(TS//SI//NF)~~ Human error resulted in the targeting of [redacted] while he was in the United States between [redacted] The NSA analyst learned of [redacted] but forgot to detask the selector. On [redacted] the analyst learned from collateral intelligence that the target had been in the United States since [redacted] The targeted selector was detasked on [redacted] with no collection noted between [redacted]

~~(TS//SI//NF)~~ On [redacted] an NSA analyst authorized to conduct Communications Security (COMSEC) Monitoring operations identified possible criminal activity of child abuse. After the discovery had been reported, the analyst incorrectly reviewed other collection from the U.S. person looking for more evidence of child abuse. The analyst was not authorized to search the COMSEC data for a purpose unrelated to COMSEC.

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

~~(TS//SI//NF)~~ The target of a tasked selector was in U.S. territorial waters for one day before the selector was removed from tasking. [redacted] The two analysts responsible for monitoring [redacted] the target were on leave when the target entered U.S. territorial waters on [redacted] The selector was removed from collection on [redacted] No collection occurred while the vessel was in U.S. waters. No reports were issued. As a result of this process weakness, additional analysts were added to the [redacted] to prevent future oversights.

~~(S//SI//NF)~~ [redacted] while reviewing skills learned in a database training class, an NSA analyst queried the personal e-mail address he shares with his wife. The analyst explained that he used the familiar e-mail address because a query for target selector data did not produce results, and he was concerned that he was not formatting the query properly. This violation was found by the analyst's auditor [redacted] No collection resulted from the mistake. The analyst reviewed USSID SP0018 and completed additional database training.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA analyst found that a targeted selector [redacted] the United States on [redacted] This was discovered during a Department of Justice directed audit of [redacted] The selector was detasked on [redacted] No collection or reporting occurred while the target was in the United States.

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

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

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] selector remained on tasking during a target's visit to the United States. [redacted]

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

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

[redacted] The [redacted] selector was detasked on [redacted] when an NSA analyst found the mistake. No queries were made on the selector from [redacted] and no reports were issued while the target was in the United States.

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

~~(TS//SI//NF)~~ During a selector review [redacted] NSA analysts found [redacted] [redacted] The selector was detasked [redacted] and [redacted] related intercepts were purged from an NSA database the same day. Additionally, NSA analysts found [redacted] selectors also tasked since [redacted] remained on tasking after the target entered the United States in [redacted] [redacted] The selectors were detasked, and [redacted] intercepts were purged from an NSA database on [redacted] No reporting resulted from the collection. The risk of recurrence has been reduced through changes in the detasking notification process. No reports were issued on the intercepts.

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

~~(TS//SI//NF)~~ An NSA analyst failed to check a target's U.S. person status prior to tasking. [redacted] selectors were tasked: [redacted] The analyst found his mistake [redacted] while conducting target research. All [redacted] selectors were detasked on [redacted] and the resulting collection was purged from an NSA database. No reports were issued on the collection.

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

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

~~(TS//SI//NF)~~ [redacted] NSA analysts found that a valid foreign target's selector was [redacted] [redacted] The selector was detasked [redacted] A database check revealed no collection, and no reporting occurred on the U.S. telephone number.

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

(U) Database Queries

~~(TS//SI//NF)~~ On [redacted] occasions, analysts constructed poor database queries that targeted U.S. persons, and on [redacted] of those occasions, the queries returned results from the database. The returned results from the overly broad or incomplete queries were deleted, and no reports were issued. Procedural errors contributed to [redacted] of the [redacted] violations.

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

- ~~(TS//SI//NF)~~ [redacted] an NSA analyst queried what he believed to be a foreign [redacted] which resulted in collection on a [redacted] Foreign intelligence indicated that [redacted] and the analyst queried the selector without confirming [redacted] The analyst's auditor found the mistake [redacted]

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

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

2009, and the related collection was purged from the NSA database [redacted] No reporting occurred from the collection.

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

- ~~(TS//SI/NF)~~ On [redacted] an NSA Signals Development analyst queried [redacted] [redacted] in an effort to obtain [redacted] foreign intelligence targets. The violation was found by the analyst's auditor [redacted] [redacted] The [redacted] results obtained were deleted [redacted] and the analyst was counseled on unauthorized searches. No reporting occurred from the collection.

- ~~(TS//SI//NF)~~ On [redacted] while pursuing a target related to the [redacted] [redacted] an analyst failed to [redacted] prior to conducting a query [redacted] was located in the United States. Found by an auditor [redacted] [redacted] the query did not produce results.

- ~~(TS//SI//NF)~~ On [redacted] an NSA analyst queried a list of selectors not related to his current office's mission. He had used the list during a previous assignment in another office. [redacted] of the selectors were found to be in the United States. No collection resulted from the query. The selector list was destroyed [redacted]

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

- ~~(TS//SI//NF)~~ On [redacted] while pursuing a target related to a [redacted] [redacted] an NSA analyst failed to [redacted] prior to conducting a query. [redacted] was located in the United States. Found by the analyst's auditor [redacted] the query and results were deleted from the NSA database [redacted] [redacted] No reports were issued on the query results, and the analyst was counseled on due diligence.

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

- ~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA analyst used the [redacted] [redacted] with no other qualifiers. [redacted] the analyst realized her mistake when the query returned approximately [redacted] results. The results were deleted without review [redacted]

- ~~(TS//SI//NF)~~ On [redacted] an NSA analyst queried a target selector after it had been detasked. Unknown to the analyst, the target selector had been detasked when it was [redacted] the United States. When the analyst learned of the incident, he deleted the resulting collection [redacted] No reports were issued on the collection.

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

- ~~(TS//SI//NF)~~ [redacted] human error resulted in the targeting of [redacted] U.S. telephone numbers related to a foreign [redacted] The NSA analyst forgot that the database he queried contained unminimized and unevaluated SIGINT data. No collection resulted from the [redacted] queries, which were deleted [redacted]

- ~~(TS//SI//NF)~~ [redacted] an NSA analyst performed a database query on a U.S. e-mail address while researching a valid foreign target. [redacted] [redacted] [redacted] The mistake was found by the analyst's auditor on

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

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

[redacted] and the query results were deleted [redacted] The auditor provided additional query training to the analyst. No reports were issued.

~~(TS//SI//NF)~~ **Unintentional dissemination of U.S. identities** The NSA Enterprise issued [redacted] SIGINT product reports during this quarter. In these reports, SIGINT analysts improperly disseminated communications to, from, or about [redacted] U.S. persons or entities while pursuing foreign intelligence. All data have been deleted or destroyed as required. A total of [redacted] SIGINT products were cancelled as NSA [redacted] analysts learned of the U.S. persons, organizations, or entities. The reports were either not reissued or were reissued with proper minimization.

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

(U) The Foreign Intelligence Surveillance Act (FISA)

(U) Unintentional Access

~~(S//SI//NF)~~ On 1 June 2009, DoJ notified the FISA Court (FISC) of a possible compliance incident under the [redacted]

[redacted]

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

[redacted]

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

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

(U) Unauthorized Targeting

~~(TS//SI//NF)~~ Targeting continued on a FISC-authorized target's e-mail selector after [redacted] [redacted] An NSA analyst noticed the lack of collection on [redacted] Research revealed the target [redacted] The selector was removed from collection on [redacted] No collection or reporting occurred.

~~(TS//SI//NF)~~ An NSA analyst misinterpreted the provisions of a FISC Order and initiated targeting of cellular telephone numbers that were not specified on the Order. [redacted] [redacted] The selectors were detasked [redacted] as the mistakes were identified. NSA purged [redacted] intercepts from the NSA database.

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

~~(TS//SI//NF)~~ On [redacted] NSA learned that a FISC-approved selector had not been removed from collection when the target [redacted] [redacted] The selector was detasked [redacted] and all related collection was purged from NSA databases the same day. No reporting resulted from the unauthorized collection.

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

(U) Database Queries

~~(TS//SI//NF)~~ [redacted] an NSA analyst queried non-FISA data [redacted] [redacted] The mistake was found by the analyst's auditor [redacted] The unauthorized collection was not reviewed and deleted from the query results [redacted] No reporting occurred on the non-FISA data.

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

~~(TS//SI//NF)~~ [redacted] NSA analysts queried non-FISA data [redacted] [redacted] The analysts copied the wrong e-mail selector into their query. [redacted] error was found the same day by the analyst's auditor, and [redacted] mistake was discovered by the analyst [redacted] All associated results were deleted on [redacted] when the mistakes were identified. No reports were issued on the non-FISA data.

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

~~(TS//SI//NF)~~ [redacted], an NSA analyst queried non-FISA data [redacted] [redacted] The analyst did not [redacted] when crafting the query. The query results were deleted [redacted] when the errors were identified. No reports were issued on the non-FISA data.

~~(TS//SI//NF)~~ Human error resulted in the targeting of [redacted] selectors [redacted] [redacted] [redacted] an NSA analyst mistakenly selected an option [redacted] [redacted] The mistake was noticed by the analyst and corrected [redacted] The results associated with the unauthorized collection were deleted [redacted] and no reports were issued on that data.

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

~~(TS//SI//NF)~~ [redacted] [redacted] [redacted] In all instances, the calls were deleted immediately upon recognition, in accordance with USSID SP0018 guidelines, and no reports were issued.

~~(TS//SI//NF)~~ Business Records Order

(U) Nothing to report.

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

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

~~(TS//SI//NF)~~ Pen Register/Trap and Trace Order

(U) Nothing to report.

(U) The Protect America Act (PAA)

~~(TS//SI//REL TO USA, FVEY)~~ During a tasking record review [redacted] NSA analysts found that an incorrect [redacted] target selector. [redacted] [redacted] The incorrect selector was detasked [redacted] NSA analysts do not know if the incorrect selector is a valid e-mail address. No collection resulted from the typing error. No reports were issued.

(U) The FISA Amendments Act (FAA)

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

(U) Section 702

(U) Tasked under an incorrect FAA Certification

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA analyst discovered that [redacted] selectors associated with a valid foreign target had been incorrectly tasked under the [redacted] Certification [redacted] Because there was insufficient information to link the targets to [redacted] the selectors were removed from tasking and the associated collection was purged from the NSA database.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA analyst discovered that a selector had been tasked under two authorities. The target selector was incorrectly tasked under the [redacted] Certification [redacted] Instead of replacing the [redacted] Certification with the corrected [redacted] Certification, the [redacted] certification was added. The [redacted] Certification was removed from the tasking information [redacted] and collection under the [redacted] Certification was purged from NSA databases [redacted] [redacted]

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

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

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

(U) Detasking Delay

~~(S//SI//REL TO USA, FVEY)~~ An NSA analyst did not detask a [redacted] target selector when the target entered the United States on [redacted] Over [redacted] intercepts were purged from the NSA database without review [redacted] when the mistake was identified. The analyst was counseled on detasking procedures.

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

(U) Section 704

(U) U.S. Person Status

~~(TS//SI//NF)~~ On two occasions, not all selectors were detasked when NSA analysts learned that an FAA Section 704 target was in the United States. In the first instance, when an inexperienced NSA analyst learned on [redacted] that a target was in the United States, the analyst mistakenly removed [redacted] from tasking the same day. No FAA-related collection occurred between [redacted] and [redacted] when the target was in the United States. Collection [redacted] was purged from [redacted] NSA databases [redacted] As a result of this violation, the mission area amended analytic training to reinforce tasking and detasking procedures. The branch also implemented [redacted] The second instance occurred [redacted] when another analyst detasked selectors [redacted] [redacted] was discovered and terminated [redacted] and the resulting collection was purged from the NSA database the same day. No reporting resulted from either violation.

(U) Section 705b

(U) Unauthorized targeting

~~(TS//SI//NF)~~ [redacted] an NSA analyst mistakenly queried a selector while the target was in the United States. The target, authorized for overseas collection under FAA section 705b, was in the United States [redacted] No collection or reporting resulted from the unauthorized targeting.

(U) Database Queries

~~(TS//SI//NF)~~ [redacted] an NSA analyst constructed a poor database query, which [redacted] The analyst had been using unfamiliar analysis tools as she was pursuing a FAA 705b-authorized target. The query [redacted] and the query results were deleted by the analyst's auditor [redacted]

~~(TS//SI//NF)~~ [redacted] an NSA analyst mistakenly queried PAA data while pursuing a FAA 705b-authorized target. Her mistake was compounded when she searched timeframes preceding the [redacted] authorization. The query [redacted] [redacted] intercepts were destroyed

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

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

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

[redacted] when the violation was identified by the analyst's auditor. No reports were issued.

~~(TS//SI//NF)~~ [redacted] an NSA analyst mistakenly queried a database for data outside the authorization date. The 705b authorization was granted on [redacted] Data queries for dates before [redacted] were not authorized. Queries on [redacted] targeted selectors were conducted to obtain target data between [redacted] No data was obtained from the query.

(U) Unauthorized Targeting

~~(TS//SI//NF)~~ NSA analysts left a target's [redacted] telephone selectors on collection while [redacted] NSA analysts were notified by the FBI [redacted] U.S. person in [redacted] [redacted] NSA analysts should have [redacted] No collection occurred between [redacted]

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

(U) Detasking Delays

~~(TS//SI//NF)~~ Human error caused a [redacted] detasking delay, which resulted in collection while the target was in the United States. The NSA analyst learned on [redacted] that the target [redacted] the United States [redacted] The analyst detasked the target's telephone selectors on [redacted] This oversight was found on [redacted] The resulting collection was purged from NSA databases on [redacted] No reports were issued from that collection.

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

~~(TS//SI//NF)~~ A target selector remained on collection [redacted] after an NSA analyst learned that the selector was not associated with the intended target. [redacted] the request to detask the target selector was overlooked by the analyst responsible for the detasking. This error was brought to light [redacted] when the e-mail selector, tasked under the FAA [redacted] Certification, [redacted] the United States [redacted] The selector was detasked on [redacted] and the data was purged from NSA databases on [redacted] 2009. The delay between recognition of the violation and detasking and purging action occurred because the analyst responsible for the action was on leave.

~~(TS//SI//NF)~~ On [redacted] an NSA analyst learned that a targeted selector remained tasked [redacted] after the selector [redacted] The analyst responsible for detasking was on leave when the initial detasking notification was submitted on [redacted] The analyst was notified again [redacted] when the selector was again [redacted] The selector was detasked [redacted] the data was purged from NSA databases [redacted] No reports were issued from the collection.

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

~~(TS//SI//NF)~~ Not all the selectors were detasked [redacted] the United States on [redacted] telephone numbers associated with the

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

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

target were detasked because of an analyst's oversight. The [redacted] selectors were detasked on [redacted] and resulting collection was purged from NSA databases [redacted] No reporting occurred from the unintentional collection.

~~(TS//SI//NF)~~ [redacted] NSA analysts learned that a target selector [redacted] the United States on [redacted] but the selector was not detasked until [redacted] The [redacted] intercepts were purged from NSA databases on [redacted]

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

(U) Destruction Delay

~~(TS//SI//NF)~~ U.S. person data was not purged from [redacted] NSA databases in a timely manner. Collection obtained while an FAA target was in the United States was purged [redacted] after NSA analysts learned that the e-mail selector [redacted] The data was purged [redacted] the U.S. location. [redacted] and because of staffing shortfalls, a backlog for purging occurred. [redacted] No reports were issued.

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

~~(TS//SI//NF)~~ A target tasked under FAA [redacted] Certification [redacted] the United States for [redacted] before a request to purge NSA databases of collection was obtained. [redacted] the target's e-mail selector [redacted] The request to purge the data was submitted [redacted] Purging commenced immediately and was completed [redacted] and because of staffing shortfalls, a backlog for purging occurred. [redacted] No reports were issued.

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

~~(TS//SI//NF)~~ A targeted selector remained on tasking [redacted] after NSA analysts learned that the target was a U.S. Green Card holder. [redacted] when an NSA analyst learned of the U.S. person status, he submitted a detasking request on the selector. Action was not taken on the detasking request. This mistake was compounded by delays in purging the data from NSA databases. Data was not purged from [redacted] after NSA analysts learned of the target's U.S. person status.

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

~~(TS//SI//NF)~~ A [redacted] delay in purging data from a NSA database occurred after an NSA analyst learned on [redacted] that a targeted e-mail selector [redacted] the United States. After the selector was detasked [redacted] action to complete purging of the data from the NSA database was not completed until [redacted] and because of staffing shortfalls, a backlog for purging occurred. [redacted] No reports were issued.

~~(TS//SI//NF)~~ A foreign target's selector was not detasked on [redacted] when the authorization expired. The selector [redacted] the United States on [redacted] The analyst [redacted] on the selector, but failed to detask it. Consequently, the selector [redacted] when FAA tasking was enacted. The selector was detasked [redacted]

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

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

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

(U) Dissemination

~~(TS//SI//NF)~~ On 24 June 2009, during the end-to-end review of the FISA Business Record (BR) Order implementation, the review team found that NSA disseminated one SIGINT product report in a manner not authorized by the FISA BR Court Order. The report, containing [redacted] U.S. telephone numbers, was forwarded to [redacted] [redacted] At the request of NSA, [redacted] purged the data from its repositories [redacted]

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

(U) Other

(U) Unauthorized Access

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

~~(TS//SI//NF)~~ [redacted] analyst working in the NSA [redacted] [redacted] was permitted access to unminimized SIGINT and U.S. person data for almost two years with training credentials that had been allowed to lapse by his organization. The security violation was compounded when NSA did not confirm the analyst's training before allowing him access to unminimized SIGINT. Employees with access to unminimized SIGINT data are to successfully complete USSID SP0018 training bi-annually. The [redacted] USSID SP0018 training was two years out of scope. The analyst's access to unminimized SIGINT data was terminated [redacted] when the oversight was identified by an [redacted] Staff Officer. The analyst returned to the [redacted]

~~(TS//SI//NF)~~ [redacted] NSA technology developers and analysts working with [redacted] accessed a shared metadata database account from [redacted] in violation of NSA/CSS Manual 130-1, NSA/CSS Operational Information Systems Security Manual. The discovery was made by a database manager who questioned the running time of a query while monitoring the data system. The database contained [redacted] which [redacted] of the users were not authorized to access. Several procedures were not followed properly, leading to the access of unminimized and unevaluated data, including FISA data, without appropriate database access authorizations or database oversight requirements. First, the project activities had not been vetted through the NSA Office of General Counsel. Second, compliance advice from NSA SIGINT Directorate's Oversight and Compliance had not been sought. Third, some employees had not completed training necessary for data handling. Of the [redacted] employees [redacted] had not completed training for handling [redacted] data, and [redacted] of the [redacted] had not completed training for handling [redacted] data. The division chief misunderstood that access to the data was permitted upon submission of access requests. [redacted] [redacted] metadata were purged from the [redacted]

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

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA analyst forwarded a PowerPoint slide containing unminimized SIGINT from E.O. 12333 collection to [redacted] [redacted] recipients before the slide was reviewed and revised by the [redacted] [redacted] Branch. The PowerPoint slide was part of an integrated graphics and multi-media report and did not contain U.S. person information. When the analyst saw that the

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

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

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

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

text of the report had been released he assumed that the slide could be disseminated. All [redacted] recipients confirmed deletion of the PowerPoint slide.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] An NSA [redacted] incorrectly forwarded a spreadsheet containing FAA data to an NSA [redacted] who had not been cleared for the FAA-obtained metadata. The linguist mistakenly believed that the [redacted] had been cleared for FAA data. [redacted] The access violation was compounded when the [redacted] did not notice the FAA data handling caveat and further disseminated the spreadsheet to others within the SIGINT Production Chain by e-mail. An analyst recognized the handling caveat and notified the [redacted] of the improper disseminations. [redacted] recipients not authorized access to FAA data confirmed deletion of the e-mail.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA cryptanalyst showed FAA data to another cryptanalyst [redacted] The other cryptanalyst was not cleared for FAA data. When the cryptanalyst realized that the content was derived from FAA collection, he removed the data from his computer screen [redacted]

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

(U) Computer Network Exploitation (CNE)

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

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

(U) Dissemination

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

~~(S//SI//REL TO USA, FVEY)~~ [redacted] SIGINT intercept containing U.S. person information was [redacted] While reviewing [redacted] a U.S. analyst noticed U.S. person information [redacted]

~~(S//REL TO USA, FVEY)~~ [redacted] an NSA analyst forwarded an e-mail containing FAA data to recipients [redacted] of whom had not completed training required for access to FAA information. Within one hour of recognizing the mistake, the [redacted] analysts not authorized access to FAA data had deleted the e-mail.

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

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

(U) Counterintelligence Activities

(U) Nothing to report.

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

(U) Intelligence-related Activities

~~(S//SI//NF)~~ To reduce the risk of unauthorized telephony collection and prevent violations, NSA instituted a process to give analysts greater and faster insight into a target's location. [redacted] In the [redacted] instances when collection occurred, it was purged from NSA databases.

~~(TS//SI//NF)~~ [redacted] NSA analysts found [redacted] e-mail selectors [redacted] Collection occurred in only [redacted] of the [redacted] instances and was purged from NSA databases.

~~(C//REL TO USA, FVEY)~~ Although not violations of E.O. 12333 and related directives, NSA/CSS reports [redacted] instances in which database access was not terminated when access was no longer required. Once identified, the accesses were terminated.

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

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

~~(C//SI//REL TO USA, FVEY)~~ While developing a brief to present to the [redacted] in [redacted] a [redacted] containing data not releasable to foreign nationals (NOFORN). Research revealed that one of the four graphical user interface (GUI) tools [redacted] the GUI. This security matter occurred [redacted] and was discovered by an auditor [redacted] The GUI authentication access was corrected [redacted] No NOFORN data was retained by the analyst.

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

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

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

2. (U//~~FOUO~~) NSA Office of the Inspector General Intelligence Oversight Inspections, Investigations, and Special Studies

(U//~~FOUO~~) During this quarter, 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 and internal directives. With few exceptions, the problems uncovered were routine and showed that operating elements understand the restrictions on NSA/CSS activities.

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

(U//~~FOUO~~) NSA/CSS Texas (NSAT)

(U//~~FOUO~~) Joint IG inspectors examined intelligence oversight (I/O) program management, I/O training, I/O knowledge, and application of I/O. Despite fragmented oversight of I/O training, NSAT operates well in the application of the NSA authorities. The recently appointed I/O Program Manager is well known and has begun to make improvements to the site's I/O processes. The governing Mission Directive does not encompass responsibilities for the oversight of reservists working NSAT missions or delineate Service Cryptologic Components' responsibilities. A highlight of the inspection was the meticulous tracking of sensitive SIGINT database accesses within several mission product lines. The OIG will track corrective actions.

(U//~~FOUO~~) Investigation of Alleged Improprieties at NSA Georgia (NSAG)

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

~~(S//REL TO USA, FVEY)~~ In 14 August 2009, the NSA OIG completed an investigation into an allegation that the [redacted] program at NSAG unlawfully intercepted and processed U.S. person communications. [redacted]

[redacted] Our investigation involved [redacted] interviews of the complainant, more than [redacted] witness interviews, [redacted] and the forensic analysis of almost [redacted] records. We found no targeting of U.S. persons by [redacted].

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

[redacted]

(U//~~FOUO~~) Additionally, the NSA OIG substantiated an allegation that an NSAG analyst, at the request of the [redacted] had queried a SIGINT raw traffic database on the selector of a person in the United States. The person was a relative of a valid foreign intelligence target.

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

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

(U//~~FOUO~~) Misuse of the U.S. SIGINT System (USSS)

~~(S//SI//REL TO USA, FVEY)~~ [redacted] a soldier within a U.S. Army [redacted] used the USSS to target his wife, also a soldier stationed [redacted] He queried an NSA database for her [redacted] Following questions from his auditor, the soldier confessed his actions. After investigation by the unit substantiated the misuse, the soldier received non-judicial punishment. Through a Uniformed Code of Military Justice Field Grade Article 15, the soldier's rank was reduced from Sergeant to Specialist; he was given 45 days extra duty and forfeited one half month's pay for two months (suspended for 180 days). The unit has revoked the soldier's access to classified information.

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

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

(U) Congressional, IOB, and DNI Notifications

~~(TS//SI//NF)~~ [redacted] NSA notified the Congressional Oversight Committees of a data retention compliance problem [redacted] NSA officials moved immediately to remedy the error and implemented [redacted] to ensure that additional FISA-derived [redacted] would be sent only to a repository that has the correct age-off period for FISA [redacted] data. An update to explain remedial steps NSA will take to bring the repositories into compliance was forwarded [redacted] Copies of the notifications are included as an addendum to this report.

~~(S//SI//NF)~~ [redacted] NSA notified the Congressional Oversight Committees of journalists' claims of NSA's irresponsibility in executing its mission pursuant to E.O. 12333 or FISC Orders. In the letters, NSA provided factual data to refute the claims. The notification is enclosed.

~~(TS//SI//NF)~~ [redacted] NSA provided a notification and update on the handling of Business Records and Pen Register/Trap and Trace data obtained under FISC Orders. Reviews conducted over the past several months have uncovered inadequate attention to internal systems and systems architecture that resulted in a failure to fully comply with Court imposed procedures documented in the FISC Order. The notification describes several compliance matters and remediation actions that have been disclosed to the Court and Congressional Oversight Committees. The notification and End-to-End Review of Business Records FISA Report is enclosed.

3. (U) Substantive Changes to the NSA/CSS Intelligence Oversight Program

(U) Nothing to report.

4. (U) Changes to NSA/CSS published directives or policies concerning intelligence, counterintelligence, or intelligence-related activities and the reason for the changes

(U) Nothing to report.

5. (U) Procedures governing the activities of Department of Defense (DoD) intelligence components that affect U.S. persons (DoD Directive 5240.1-R, Procedure 15) Inquiries or Matters Related to Intelligence Oversight Programs

(U) Nothing to report.

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

06-17-09 P06:49 OUT

MEMORANDUM FOR STAFF DIRECTOR, SENATE SELECT COMMITTEE ON INTELLIGENCE

SUBJECT: (U) Congressional Notification – New York Times article "E-Mail Surveillance Renews Concerns in Congress" – INFORMATION MEMORANDUM

(U) On 17 June 2009 *The New York Times* published an article by James Risen and Eric Lichtblau entitled "E-Mail Surveillance Renews Concerns in Congress." The article contains many assertions that make it seem as if NSA is broadly irresponsible in executing its mission pursuant to Executive Order or Foreign Intelligence Surveillance Court (FISC) Orders. The opposite is true.

(U//~~FOUO)~~ As you know, and we have acknowledged, NSA has recently identified and reported compliance issues with FISC orders. However, the article's assertion that NSA has deliberately and illegally collected domestic communications of U.S. persons is patently false. The accusations are far afield of the compliance matters we have experienced which largely relate to deficiencies in the way NSA systems managed data that was lawfully collected. Moreover, the fact that the compliance issues have been identified, reported to the FISC and Congressional overseers, and that steps were taken to remedy them testifies to NSA's commitment to oversight.

(U) While it is difficult to know exactly what the article's anonymous sources are referring to in regards to each of their claims, given the gross mischaracterizations of the article it is important to state for the record what we know to be true.

- ~~(S//SI//NF)~~ Early in the article it states that in 2005 a former NSA analyst was trained on a program in which NSA routinely examined large volumes of Americans' email messages without court warrants. Given the lack of context provided relating to this claim, it is difficult to know what is actually alleged to have occurred. However, if this refers to the previously well documented and publicly aired allegations of David Faulk, the allegations are false – a conclusion that NSA's IG will soon report out.

- (U) The article goes on to suggest that NSA is not up to the challenge of protecting the privacy rights of U.S. person communications that are encountered as a result of lawful collection of foreign intelligence. To the contrary, NSA has robust minimization procedures and mechanisms in place to limit to the greatest possible extent the impact on privacy rights. These procedures are subject to either approval of the Attorney General, in relation to collection pursuant to EO 12333, or to the FISC, in relation to collection pursuant to FISA.

- ~~(S//SI//NF)~~ Later, the article provides an illustration of a supposed compliance problem in which NSA's attempts to target 1,000 emails result in the collection against those 1,000 plus another 1,000 that are not intended. [redacted] NSA has employed significant resources and effort to counter [redacted] These mitigation efforts involve continuous process improvements to prevent and/or detect [redacted] at the earliest possible point and the application of our targeting and collection minimization procedures.

  [redacted]

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

- (U//~~FOUO~~) The article also identifies a 30% threshold for the inclusion of U.S. person information within NSA databases. There is no truth to this statement, as the existence of U.S. person information in NSA databases is limited not by a percentage number but by the NSA's targeting practices that seek foreign intelligence only.

- ~~(S//SI//NF)~~ The additional allegation that NSA has "…improperly accessed the personal email of former President Bill Clinton" is an inaccurate portrayal of an event that dates from 1992. NSA's records of the event demonstrate NSA's commitment to oversight and compliance.

  - ~~(S//SI//NF)~~ On November 3 1992, an analyst wondering how foreign targets were reacting to Bill Clinton's election typed in a query [redacted] The query was made against the [redacted] There were probably very few emails of any kind in there at that time, and there would not

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

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

about Bill Clinton. Immediately after the query was entered, the co-worker sitting next to the analyst identified that this was a query on a U.S. person. The analyst immediately realized that the query was wrong and contrary to authorities. The matter was quickly reported to NSA leadership and resulted in notifications outside of NSA pursuant to Executive branch guidelines. As a result of this incident the analyst's access was suspended while the analyst attended mandatory re-training.

- (U) Although this activity occurred 17 years ago, we have used it in our oversight training, even in the last several years, as an illustrative example of queries that are inappropriate and must be reported and investigated. This type of query remains as inappropriate today as it was then and will not be tolerated under any circumstances.

(U) NSA remains committed to providing transparency in these matters – a promise made by the DIRNSA. We would be pleased to meet with the Committee to address any concerns that may remain.

JONATHAN E. MILLER
Associate Director
Legislative Affairs Office

Copy Furnished:
Minority Staff Director, Senate Select
Committee on Intelligence