



~~TOP SECRET//COMINT//NOFORN//MR~~
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-5000

21 November 2006

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 September 2006 were unlawful or contrary to Executive Order or Presidential Directive, and thus required to be reported pursuant to Section 1.7.(d) of Executive Order 12333.

(U//~~FOUO~~) The Inspector General and the General Counsel continue to exercise oversight of Agency activities by means of 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.

Brian R. McAndrew
BRIAN R. MCANDREW
Acting Inspector General

Vito T. Potenza
VITO T. POTENZA
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
KEITH B. ALEXANDER
Lieutenant General, U. S. Army
Director, NSA/Chief, CSS

Encl:
Quarterly Report

Approved for Release by NSA on 12-19-2014, FOIA Case # 70809 (Litigation)

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

This Memorandum is Unclassified
Upon Removal of Enclosure

~~TOP SECRET//COMINT//NOFORN//MR~~**1. (U) INSPECTOR GENERAL ACTIVITIES****a. Reviews**

~~(C//SI)~~ During this quarter, the Office of Inspector General (OIG) reviewed various intelligence activities of the National Security Agency/Central Security Service (NSA/CSS) to determine whether they were conducted in accordance with applicable statutes, Executive Orders (E.O.s), Attorney General (AG) procedures, and Department of Defense (DoD) and internal directives. With few exceptions, the issues presented were routine and indicated that the operating elements understand the restrictions on NSA/CSS activities.

b. (U) Inspections

(1) ~~(U//FOUO)~~ Along with inspectors from [redacted] the NSA/CSS OIG completed a joint inspection of the [redacted]. Since [redacted] was recently designated as a joint organization, its intelligence oversight (IO) program needed adjustments to transition from an [redacted] to an NSA/CSS IO program. Those adjustments were quickly completed. The center has begun quarterly reporting of intelligence activities to the NSA/CSS OIG, and has submitted the IO training materials to the NSA/CSS OIG for validation. At the OIG recommendation, the IO program manager is now included in exercise planning and new mission management meetings to establish management controls to prevent IO violations.

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

(2) ~~(S//REL)~~ Inspectors from [redacted] and the NSA/CSS OIG completed a joint inspection of the [redacted]. The documentation of the [redacted] IO program and process was commendable; however, an analysis of a sample of training records revealed that only 64% of the newly arrived employees received initial training. A finding documented the need for internal controls in oversight of training.

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

(b) (1)
(b) (3) - P.L. 86-36**c. (U) Inquiries**

~~(TS//SI//NF)~~ Reported in the first quarter fiscal year 2006, U.S. person information contained in a graphic chart was disseminated during briefings outside of NSA/CSS. (Report dated 28 February 2006). Research revealed that the originator had obtained a dissemination waiver. No violation occurred.

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 FEBRUARY 1998
DECLASSIFY ON: Source Marked X1,
Date of Source 20061106

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

2. (U) GENERAL COUNSEL ACTIVITIES

~~(C//SI)~~ The NSA/CSS OGC reviewed various intelligence activities of the NSA/CSS to determine whether they were conducted in accordance with applicable statutes, EOs, AG procedures, and DoD and internal directives. The OGC advised Agency elements on a number of questions, including the collection and dissemination of communications of or concerning U.S. persons; the reporting of possible violations of federal criminal law contained in Signals Intelligence (SIGINT) product; the testing of electronic equipment, and the applicability of the Foreign Intelligence Surveillance Act (FISA). With few exceptions, the issues presented were routine and indicated that the operating elements understand the restrictions on NSA/CSS activities.

3. (U) SIGINT ACTIVITIES

a. ~~(S//SI)~~ Collection Against U.S. Persons

(1) (U) Intentional

a. ~~(TS//SI)~~ During this quarter, the Director, NSA/Chief CSS (DIRNSA/CHCSS) granted approval for consensual collection against U.S. persons. DIRNSA/CHCSS also approved non-consensual collection of U.S. companies

agents of foreign powers U.S. citizens believed to have been held against their will U.S. citizen taken hostage and U.S. military member believed to have been taken hostage DIRNSA/CHCSS-approved consensual collection against U.S. persons was routinely terminated this quarter.

b. ~~(S//SI)~~ The AG granted authority to collect the communications of U.S. persons overseas during this quarter.

(2) (U) Unintentional

~~(S//SI//NF)~~ instances in which SIGINT analysts inadvertently collected communications to, from, or about U. S. persons while pursuing foreign intelligence tasking were reported this quarter. All of the incidents were reported to responsible oversight officials, and corrective actions were taken.

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

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

b. (U//~~FOUO~~) Dissemination of U.S. Identities

(1) (U) Intentional

~~(S//SI)~~ In accordance with section 7 of United States Signals Intelligence Directive (USSID) SP0018, U.S. identities were disseminated [] times during this quarter. The following table shows the justification and the number of instances of dissemination. In the "Unmasked by Analyst" column, the U.S. identity was revealed in a serialized end product; in the "Unmasked at User Request" column, a U.S. identity was released to a user at the user's request.

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

JUSTIFICATION	Unmasked by Analyst	Unmasked at User Request	TOTAL
7.2.c Necessary			
7.2.c.1 Foreign Official			
7.2.c.3 International Narcotics			
7.2.c.4 Criminal Activity			
7.2.c.7 U.S. Government Official			
TOTAL			

(2) (U) Unintentional

~~(S//SI)~~ During this quarter, [] SIGINT products were cancelled because they contained the identities of U.S. persons, organizations, or entities. In all instances, the reports were either not reissued or were reissued with the proper minimization.

(3) (U) Raw Traffic Dissemination

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

a. ~~(S//SI)~~ SIGINT Production Chain. []

[]

[] The SID ensures that the personnel are trained by the

OGC on NSA/CSS's legal restrictions and on proper handling and dissemination of SIGINT data [redacted] Such persons working in or with SID during this quarter included representatives of [redacted]

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

[redacted]

b. ~~(S//SI)~~ Outside the SIGINT Production Chain. [redacted] a project manager within the NSA [redacted] inappropriately discussed raw SIGINT containing a U.S. person's identity with [redacted] [redacted] At the direction of the NSA/CSS OGC, the [redacted] The project manager was reeducated on raw traffic handling procedures and the approval mechanisms required to release U.S. person information.

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

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

4. (U) Other Activities

a. ~~(U//FOUO)~~ Foreign Intelligence Surveillance Act (FISA) Incidents

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

(1) ~~(TS//SI//NF)~~ There have been [redacted] instances this quarter where FISA data was accessed in [redacted] [redacted] While these incidents were not violations, they were cases of mishandling very sensitive data.

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

(a) ~~(TS//SI//NF)~~ The NSA [redacted] Branch allowed FISA data to be accessed [redacted] [redacted] Although the analyst was cleared for FISA access, the [redacted] was not. No one other than the analyst had access to the FISA data. He did not query raw SIGINT databases, and the FISA-related files were deleted [redacted] An astute intelligence oversight program manager at an NSA/CSS field site in the area uncovered the data mishandling incident and reported it to NSA/CSS Headquarters.

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

(b) ~~(TS//SI//NF)~~ An NSA [redacted] Branch language analyst accessed FISA data from NSA [redacted] In addition to his work while detailed to an intelligence community [redacted] the analyst periodically processed intercept and performed quality control on [redacted] language collection. [redacted] the analyst accessed [redacted] intercepts and [redacted] intercepts. He reported the mishandling of data to NSA management [redacted] when he realized that [redacted] No one other than the cleared analyst was exposed to the intercept.

(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)

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

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

(2) ~~(TS//SI//NF)~~ Human error resulted in the collection of [redacted] outside the time period authorized by the Foreign Intelligence Surveillance Court (FISC). Although the [redacted] after the FISC order was signed [redacted] rendering them unauthorized for [redacted] were deleted from the [redacted] and the associated database when the error was discovered [redacted]

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

(3) ~~(TS//SI//NF)~~ Communications from a U. S. person, who was also an [redacted] citizen and an authorized target while outside of the United States, were inadvertently collected from [redacted] Upon recognition of the target's location on [redacted] was detasked and all intercepted communications were deleted. No reporting resulted from the collection.

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

(4) ~~(TS//SI//NF)~~ [redacted] reports issued in [redacted] were cancelled [redacted] when an analyst in the NSA [redacted]

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

[redacted] The intercepted communications were deleted when the reports were cancelled.

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

[redacted] All collection was terminated, and the intercepts were deleted or destroyed as required by USSID SP0018.

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

b. (U) Assistance to Law Enforcement

~~(S//SI)~~ During this quarter, the SID responded to [redacted] for linguistic support from the [redacted]

c. (U) Working Aids

~~(U//FOUO)~~ The SID Office of Oversight and Compliance maintains "U.S. Identities in SIGINT" and a matrix of dissemination authorities on its web page for use by the NSA/CSS Enterprise. The E.O., NSA/CSS Policy Number 1-23, DoD Regulation 5240.1-R, and USSID SP0018 are also available on-line.

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