

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//FOUG)—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 Acting Inspector General

> 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 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

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	(b) (3)-P.L. 86-36
(1) (U// FOUO) Along with inspectors from	
	the NSA/CSS OIG completed a joint
inspection of the	Since was
recently designated as a joint organization, its	intelligence oversight (IO) program
needed adjustments to transition from an	to an NSA/CSS IO
program. Those adjustments were quickly com	pleted. The center has begun quarterly
reporting of intelligence activities to the NSA/C	
training materials to the NSA/CSS OGC for va	lidation. At the OIG recommendation,
the IO program manager is now included in ex	ercise planning and new mission
management meetings to establish manageme	nt controls to prevent IO violations.
(2) (S/REL) Inspectors from	(b) (\$)-P.L. 86-3
	and the NSA/CSS OIG completed
a joint inspection of the	
The documentation of the	O program and process was
commendable; however, an analysis of a samp	le of training records revealed that only
64% of the newly arrived employees received in	
the need for internal controls in oversight of tr	
	(b) (3) -P.L. 86-36
c. (U) Inquiries	
(TS//SI//NF) Reported in the first quarter	
information contained in a graphic chart was	
NSA/CSS. (Report dated 28 February 2006).	
had obtained a dissemination waiver. No viol	ation 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	(b) (1)
a. (S//SI) Collection Against U.S. Persons	(b) (3)-P.L. 86-36 (b) (3)-18 USC 798 (b) (3)-50 USC 3024(i)
(1) (U) Intentional	
a. (TS//SI) During this quarter, the Direction against approved non-consensual collection of	unst U.S. persons. DIRNSA/CHCSS
	Irva
agents of foreign powers citizens believed to have been held against the	U.S. citizen taken
hostage and U.S.	military member believed to have been
	DIRNSA/CHCSS-approved consensual
collection against U.S. persons was routine	ly terminated this quarter.
b. (S//SI) The AG granted authority to copersons overseas during this quarter.	ellect the communications of U.S.
7	(b) (1)
(2) (U) Unintentional	(b) (3)-P.L. 86-36
(S//SI//NF) instances in which S	SIGINT analysts inadvertently collected
communications to, from, or about U. S. perso	
tasking were reported this quarter. All of the	
oversight officials, and corrective actions were	

TOP SECRET//COMINT//NOFORN//MR

b. (U//FOUO) Dissemination of U.S. Ident
--

(1) (U) Intentional

(S//SI) In accordance with section 7 of United States Signals Intelligence	
Directive (USSID) SP0018, U.S. identities were disseminatedtimes 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. (b) (1)	- 20
identity was released to a user at the user's request.	5-36

JUSTIFICATION		Unmasked by Analyst	Unmasked at User Request TOTAL	
7.2.c Necessary			\	
7.2.c.1 Foreign Official	A. WARRANT WAR			,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
7.2.c.3 International Narcotic	28			
7.2.c.4 Criminal Activity		/		
7.2.c.7 U.S. Government Offi	cial			
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 ensu	res that the personnel are trained by the

TOR SECRET//COMPAT/NOFORN//MR

OGC on NSA/CSS's legal restrictions a	
SIGINT data	Such persons working in or with (b)(1)
SID during this quarter included repre	esentatives of (b)(3)-P.L. 86-36
b. (S//SI) Outside the SIGINT Pro	eduction Chain. a (b) (3)-P.L. 86-36
project manager within the NSA	inappropriately
discussed raw SIGINT containing a U.	/
At	t the direction of the NSA/CSS OGC, the
	The project manager was reeducated
47 2	the approval mechanisms required to release
U.S. person information.	(b)(1)
	(b)(3)-P.L. 86-36
4. (U) Other Activities	(b)(3)-50 USC 3024(i) (b) (1)
48 0.74mm are 3.1 are 5.20m	(b) (3)-P.L. 86-36
a. (U// FOUO) Foreign Intelligence \$	Surveillance Act (FISA) incidents
(1) (TS//SI/NF) There have been	Instances this quarter where FISA data was
accessed in	(b)(3)-P.L. 86-36
	e these incidents were not violations, they were
cases of misnandling very sensitive da	ita.
cases of mishandling very sensitive da	ata.
(a) (TS//SI//NF) The NSA	Branch allowed FISA
(a) (TS//SI//NP) The NSA data to be accessed	Branch allowed FISA
(a) (TS//SI//NP) The NSA data to be accessed	
(a) (TS//SI//NF) The NSA data to be accessed Altho	Branch allowed FISA ough the analyst was cleared for FISA access, the
(a) (TS//SI//NF) The NSA data to be accessed Altho	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No a FISA data. He did not query raw SIG	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the HINT databases, and the FISA-related files were
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No FISA data. He did not query raw SIG deleted A	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the HINT databases, and the FISA-related files were an astute intelligence oversight program manager
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No expressed FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area of	bugh the analyst was cleared for FISA access, the one other than the analyst had access to the HNT databases, and the FISA-related files were an astute intelligence oversight program manager uncovered the data mishandling incident and
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No FISA data. He did not query raw SIG deleted A	bugh the analyst was cleared for FISA access, the one other than the analyst had access to the HNT databases, and the FISA-related files were an astute intelligence oversight program manager uncovered the data mishandling incident and
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area was reported it to NSA/CSS Headquarters	bugh the analyst was cleared for FISA access, the one other than the analyst had access to the GINT databases, and the FISA-related files were an astute intelligence oversight program manager ancovered the data mishandling incident and s. (b) (3)-P.L. 86-36
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No expressed FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area of	bugh the analyst was cleared for FISA access, the one other than the analyst had access to the HNT databases, and the FISA-related files were an astute intelligence oversight program manager uncovered the data mishandling incident and
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No a FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area a reported it to NSA/CSS Headquarters (b) (TS//SI//NF) An NSA	bugh the analyst was cleared for FISA access, the one other than the analyst had access to the HINT databases, and the FISA-related files were in astute intelligence oversight program manager incovered the data mishandling incident and incovered the data mishandling incident and incident an
(a) (TS//SI//NF) The NSA data to be accessed Altho Was not. No a FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area a reported it to NSA/CSS Headquarters (b) (TS//SI//NF) An NSA FISA data from NSA addition to his work while detailed to	bugh the analyst was cleared for FISA access, the one other than the analyst had access to the HINT databases, and the FISA-related files were in astute intelligence oversight program manager incovered the data mishandling incident and incovered the data mishandling incident and incident an
(a) (TS//SI//NF) The NSA data to be accessed Altho Was not. No FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area w reported it to NSA/CSS Headquarters (b) (TS//SI//NF) An NSA FISA data from NSA addition to his work while detailed to performed quality control on land	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the HINT databases, and the FISA-related files were an astute intelligence oversight program manager ancovered the data mishandling incident and by (a) -P.L. 86-36 Branch language analyst accessed In an intelligence community the analyst periodically processed intercept and aguage collection.
(a) (TS//SI//NF) The NSA data to be accessed Altho Was not. No a FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area at reported it to NSA/CSS Headquarters (b) (TS//SI//NF) An NSA FISA data from NSA addition to his work while detailed to performed quality control on land the analyst accessed in	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the HINT databases, and the FISA-related files were an astute intelligence oversight program manager incovered the data mishandling incident and s. (b) (3)-P.L. 86-36 Branch language analyst accessed In an intelligence community the analyst periodically processed intercept and aguage collection. intercepts and intercepts. He reported
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No of the second	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the HINT databases, and the FISA-related files were an astute intelligence oversight program manager incovered the data mishandling incident and s. (b) (3)-P.L. 86-36 Branch language analyst accessed In an intelligence community the analyst periodically processed intercept and agguage collection. intercepts and intercepts. He reported aggement when he realized
(a) (TS//SI//NF) The NSA data to be accessed Altho Was not. No a FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area of reported it to NSA/CSS Headquarters (b) (TS//SI//NF) An NSA FISA data from NSA addition to his work while detailed to performed quality control on lian the analyst accessed in the mishandling of data to NSA mans that	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the FINT databases, and the FISA-related files were an astute intelligence oversight program manager ancovered the data mishandling incident and by (b) (3) -P.L. 86-36 Branch language analyst accessed In an intelligence community the analyst periodically processed intercept and aguage collection. Intercepts and Intercepts. He reported agement No one other than the cleared
(a) (TS//SI//NF) The NSA data to be accessed Altho was not. No of the second	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the FINT databases, and the FISA-related files were an astute intelligence oversight program manager ancovered the data mishandling incident and by (b) (3) -P.L. 86-36 Branch language analyst accessed In an intelligence community the analyst periodically processed intercept and aguage collection. Intercepts and Intercepts. He reported agement No one other than the cleared
(a) (TS//SI//NF) The NSA data to be accessed Altho Was not. No a FISA data. He did not query raw SIG deleted at an NSA/CSS field site in the area of reported it to NSA/CSS Headquarters (b) (TS//SI//NF) An NSA FISA data from NSA addition to his work while detailed to performed quality control on lian the analyst accessed in the mishandling of data to NSA mans that	Branch allowed FISA ough the analyst was cleared for FISA access, the one other than the analyst had access to the FINT databases, and the FISA-related files were an astute intelligence oversight program manager ancovered the data mishandling incident and by (b) (3) -P.L. 86-36 Branch language analyst accessed In an intelligence community the analyst periodically processed intercept and aguage collection. Intercepts and Intercepts. He reported agement No one other than the cleared

(b) (b) (b) (b)

(1) (3)-P.L. 86-36	TOP SECRET/COMINT	*//NOPORN//MR	(b) (1)	
(3)-18 USC 798 (3)-50 USC 3024(i)			(b) (3)-P.L. 86-36	
	Human error resulted in t			
butside the time (FISC). Although the	e period authorized by the		nce Surveillance Cou FISC order was	rt
signed signed	е	atter the	F15C order was	٦
rendering them unau			were deleted from the	
8	and the associated databas	e when the error	was discovered	(b)(3)-P.L. 86-3
citizen and an autho inadvertently collect		of the United Sta	tos wore (b) (3)-	P.L. 86-36 18 USC 798 50 USC 3024(i)
	cognition of the target's loc			,
reporting resulted fr	vas detasked and all interce	epted communica	tions were deleted. N	0
ropos mig roburou ir	om the consecution.		/ / \	
(4) (TS//SI// NF when an analy	reports issued in	were can	celled	(b)(3)-P.L. 86-3
,	, ,			
		The intercept	ted communications	-
were deleted when t	he reports were cancelled.	***************************************		
(5) (TS//SI//NF)	7 <u> </u>	· · · · · · · · · · · · · · · · · · ·		
(3) (2.3/1.34/1.42)			1	
	on was terminated, and the	e intercepts were	deleted or destroyed a	as
required by USSID	SP0018.		(b) (1)	
b. (U) Assistance to	o Law Enforcement		(b)(3)-P.L. 80	6-36
-(S//SI) During thi	is quarter, the SID respond	led to	for linguistic support	ŧ
from the			_	
c. (U) Working Aid	s			
	in this way of the second of t		-tring MTT C Taloutitie	~

(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.