DOCID: 4165172

~~TOP SECRET//COMINT//NOFORN//20320108~~
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

29 February 2007

This date is incorrect and should read 29 February 2008.

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

SUBJECT: (U//~~FOUO~~) Required Actions for the CY 2007 Intelligence Oversight Report to Congress – INFORMATION MEMORANDUM

(U//~~FOUO~~) In accordance with your memorandum of 15 November 2007, the enclosed consolidation of the National Security Agency's Quarterly Reports to the President's Intelligence Oversight Board for calendar year 2007 is provided to assist the Secretary of Defense in preparation of his Annual Report to Congress.

[redacted]
for
GEORGE ELLARD
Inspector General

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

Encl:
Annual Report

This document may be declassified and marked "UNCLASSIFIED//~~For Official~~

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

~~TOP SECRET//COMINT//NOFORN//20320108~~

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

(U) Intelligence Activities (b)(1) (b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ **Unintentional collection against United States (U.S.) persons.** On [ ] occasions Signals Intelligence (SIGINT) analysts inadvertently collected communications to, from, or about U. S. persons while pursuing foreign intelligence tasking were reported in calendar year 2007.

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

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

~~(S//SI//REL TO USA, FVEY)~~ There were [ ] instances of unintentional collection resulting from poorly constructed database queries, and two incidents resulting from human error. In one case, the analyst neglected [redacted] and in the other a typing mistake was made.

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

~~(S//SI//REL TO USA, FVEY)~~ On [ ] occasions, targets initially thought to be legitimate and foreign were found to hold U.S. citizenship or permanent resident status after they had been tasked for collection.

~~(S//SI//REL TO USA, FVEY)~~ On [ ] occasions, [redacted] the United States. Another target [redacted] to the United States.

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

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

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

[redacted] (b)(1)
(b)(3)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(S//SI//REL TO USA, FVEY)~~ Action Taken. The selectors for the affected collection were detasked from selection management systems used to manage and task selectors on collection systems [redacted] Unintentionally intercepted electronic mail and voice communications were deleted. Data was removed from data storage systems. Corrective actions were taken to lessen the risk of recurrence included additional training and education and changes to internal controls and software. (b)(1) (b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ **Unintentional dissemination of U.S. identities.** During this quarter, [redacted] 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. Additionally, [redacted] U.S. identities were released without proper authority as a result of tips, analysis of events, or being included in a briefing slide. The data for the [redacted] violations was recalled, cleared from computer hard drives, and destroyed.

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

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

~~(S//SI//NF)~~ **The Protect America Act of 2007 (PAA).** To ensure the "foreignness" of a target as required by the PAA [redacted] This risk reduction measure identified [redacted] incidents [redacted] in the United States. In [redacted] instances, as required by the PAA, collection was suspended immediately until the target left the United States. In one instance, analysts noted the target's presence in the United States, [redacted] resulting in detasking delays and in unauthorized collection. Corrective actions have been taken to lessen the risk of recurrence, including changes to internal control procedures. In [redacted] instances, unauthorized collection occurred when the targets were later found to be in the United States.

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

~~(TS//SI//NF)~~ **Foreign Intelligence Surveillance Act (FISA) collection.** There were [redacted] FISA collection incidents in calendar year 2007. Causes for the inadvertent collection include: [redacted] queries were deleted, cell phone numbers were removed from the tasking database, and intercepts were destroyed.

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

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

~~(TS//SI//NF)~~ **FISA dissemination.** [redacted] published reports were cancelled because they contained the identities of U.S. persons, organizations, or entities. Additionally, there were [redacted] instances of improper dissemination of unevaluated, unminimized SIGINT derived from court-approved collection. In the first instance, an analyst sent unminimized NSA FISA-derived communications to [redacted] analysts without proper authorization. The same day, [redacted] analysts were instructed to delete the communications. In the second incident, unevaluated, unminimized SIGINT derived from court-approved collection was improperly disseminated to a [redacted] The same day [redacted] shared the information with [redacted] and [redacted] subsequently destroyed the improperly disseminated material, which contained the identifications of [redacted] U.S. entities. In the third instance, an analyst forwarded FISA data to a [redacted] site, which was not authorized to receive such data. [redacted] personnel discovered the mistake and destroyed all the data.

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

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

(U) **Counterintelligence Activities**

(U) Nothing to report.

(U) **Intelligence-related Activities**

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

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

[redacted] A request to target the communicant overseas was submitted to the Office of the Attorney General.

(b)(7)(E)
OGA

~~(TS//SI//REL TO USA, FVEY)~~ NSA Texas inappropriately targeted a U.S. person based on an [redacted] Upon recognition of the mistake, the telephone numbers were detasked. The next day, analysts determined that detasking had not taken place and took measures to detask the numbers.

(U//~~TOUO~~) On [redacted] occasions, SIGINT analysts accessed SIGINT in databases to which they improperly retained access from previous assignments. Their accounts

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

were disabled and they received remedial training concerning the proper use of databases.

(U) **Misuse of the U.S. SIGINT System**

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

~~(S//SI//NF)~~ While teaching a class on analyzing communication networks, the instructor purposely entered the phone number of his friend, who was neither a U.S. person nor living in the United States. [redacted] The instructor was counseled on the restrictions on NSA authorities and was mandated to attend training on USSID SP0018, which he completed in July 2007.

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

~~(S//SI//NF)~~ A SIGINT analyst conducted database queries at the request and with the permission of a [redacted] The analyst targeted the [redacted] in a SIGINT database. No information was developed and no reports were issued.

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

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] intercepted the communications of an unidentified individual calling a targeted telephone. Based on the content of the call, NSA analysts [redacted] do not believe this is a random telephone call, but rather a misuse of government information by a witting individual [redacted] This matter was reported to the Department of Defense General Counsel for an investigative determination. The incident has not violated U.S. person privacy rights but is reported because of the misuse of the U.S. SIGINT System.

2. (U//~~FOUO~~) Intelligence Oversight Inspections

(U//~~FOUO~~) During 2007, 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, Attorney General procedures, and Department of Defense and internal directives. With few exceptions, the issues presented from the five inspections were routine and indicated that the operating elements understand the restrictions on NSA/CSS activities. The NSA/CSS OIG will track inspection corrective actions.

(U//~~FOUO~~) **NSA/CSS Georgia.** NSA/CSS Georgia has made significant improvements in its intelligence oversight program. The program management function was transferred to the operations staff from the security directorate. NSA/CSS Georgia has implemented a process to track intelligence oversight training for newly arrived employees by using computer account creation information. Advanced intelligence oversight training on United States Signals Intelligence Directive SIGINT Policy 0018 (USSID SP0018) and the FISA was created for operations watch officers to provide more in-depth information and training on application of the authorities. Personnel within operational areas, especially high-risk mission areas, are well versed in the intelligence oversight authorities.

(U//~~FOUO~~) [redacted]. The [redacted] (b)(3)-P.L. 86-36 intelligence oversight training program suffered from a lack of oversight. Only a small number of [redacted] employees had completed the required intelligence oversight training in the last 2 years. Employees are aware of their reporting responsibilities, and incidents are reported in a timely manner.

(U//~~FOUO~~) [redacted] (b)(1) (b)(3)-P.L. 86-36 is diligently working to improve its Intelligence Oversight program, but procedures fall short of the minimum required to ensure that all employees receive required intelligence oversight training. Training is not managed effectively or efficiently, and there are no internal controls ensure training compliance. Although the understanding of NSA authorities in relation to collection, minimization, and dissemination was noted as poor, no intelligence oversight-related concerns were noted within operations.

(U//~~FOUO~~) [redacted]. Intelligence Oversight Program Management is degraded by weaknesses in the [redacted] personnel database and the process used to ensure that all personnel with [redacted] receive intelligence oversight training before they are exposed to operational or classified information. Additionally, although training is conducted as required by the DoD Regulation 5240.1-R and NSA/CSS Policy 1-23, more emphasis is needed on USSID SP0018 and National Telecommunications and Information Systems Security Directive 600 standards. There were no intelligence oversight concerns noted within mission operations. (b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)

~~(S//SI//REL TO USA, FVEY)~~ [redacted] Intelligence Oversight is hampered by the absence of clearly delineated roles and responsibilities for the [redacted] Intelligence Oversight Program Manager and organizational points of (b)(1) (b)(3)-P.L. 86-36

contact. The organization lacks documented processes and procedures for timely reporting intelligence oversight incidents and violations, and there are no documented procedures for tracking intelligence oversight training; therefore, accounting for personnel who require the training is incomplete. Additionally, [redacted] is not complying with intelligence oversight measures detailed in a [redacted] agreement with the SIGINT Director regarding [redacted]

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

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

~~(S//SI//NF)~~ Practicing due diligence, NSA has improved internal controls to reduce the risk of unauthorized collection. [redacted]

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

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) **Intelligence Oversight Special Studies**

(U//~~FOUO~~) [redacted] The NSA OIG conducted a study on [redacted] that receive raw SIGINT. The objectives of the review were to determine whether selected [redacted] have the proper authorization to access raw SIGINT, have been provided guidance on its proper handling and use, and have adhered to applicable intelligence oversight authorities.

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

(U//~~FOUO~~) Signals Intelligence Directorate (SID) documentation, guidance, and intelligence oversight related to the sharing of raw SIGINT with the [redacted]

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

visited is inadequate. The internal controls within SID to oversee SIGINT enabling work performed at the visited were not effective, efficient, or measurable. Many SID and employees were not cognizant of required intelligence oversight training and related oversight procedures. The NSA OIG will track the deficiencies and oversee corrective action.

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

~~(TS//SI//NF)~~ A review was completed to determine whether NSA The review did not find a pattern of errors, exaggeration of facts, or any intentional misstatements by NSA

~~(TS//SI//REL TO USA, FVEY)~~

86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(U//FOUO)~~

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

~~(C//NF)~~ **Retention of Domestic Communications Collected Under FISA Surveillances.** While conducting collection operations authorized under the FISA of 1978, as amended, NSA incidentally collects domestic communications, subject to retention limitations. Although NSA information systems can be programmed to facilitate compliance with retention limitations, the SID is not fully using information system capabilities to do so. The OIG did not detect major instances of domestic communications in conflict with minimization procedures; however, we determined that the risk is high for noncompliance. The OIG found that appropriate training on how data repository system capabilities can aid analysts to comply with retention rules The

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

OIG also found that developing an FBI-Compatible Dissemination System could lower NSA's risk of noncompliance.

(U) **Intelligence Oversight Investigation**

(U//~~FOUO~~) The NSA OIG Chief of Intelligence Oversight and the OIG Ombudsman completed an inquiry into a complaint of improper intelligence collection at a field site. The allegations were not substantiated.