

~~SECRET//REL TO USA, FVEY~~



OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

October 2, 2009

IG-11084-09

(U) MEMORANDUM FOR COMMANDER, NSA/CSS GEORGIA,
Fort Gordon, GA

(U//~~FOUO~~) OFFICER IN CHARGE (OIC), [REDACTED] NSA/CSS
GEORGIA, Fort Gordon, GA

SUBJECT: (U//~~FOUO~~) Intelligence Oversight of the [REDACTED]
Program at NSA/CSS Georgia (ST-09-0020) - ACTION MEMORANDUM

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

(U//~~FOUO~~) During the investigation of alleged improprieties at NSA Georgia (NSAG) in 2004 and 2005 and reported by a former NSA assignee in 2008, we identified some practices in [REDACTED] that are inconsistent with established NSA/CSS policies and procedures. For details concerning the investigation, see *Report of Investigation Regarding Alleged Improprieties at NSA Georgia* (Report of Investigation), IV-09-0003, August 14, 2009. These practices may increase the risk of mishandling U.S. persons information and, therefore, require your attention.

A. (U) Improper Dissemination of Raw SIGINT

~~(S//REL TO USA, FVEY)~~ We discovered that as of 20 August 2009,

[REDACTED] Daily Summaries could be accessed in [REDACTED] archives on NSAnet.¹ For a listing of the summaries, see pp. 30 - 34 in the Report of Investigation. The [REDACTED] Daily Summaries were also saved in the Extended Shared Enterprise Corporate Server (ESECS).² These summaries or gists are not minimized for dissemination and are, therefore, considered raw traffic. They can be viewed by anyone with an NSAnet account, including personnel outside the SIGINT production chain, thus constituting

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

~~(S//REL TO USA, FVEY)~~ [REDACTED] Daily Summaries are created from data pulled by analysts [REDACTED]

² (U//~~FOUO~~) ESECS is a web-based collaboration suite or content management system hosted on NSAnet that provides workflow automation, document management, content search, and subscription/notification services. It provides communities of interest in which organizations can store information and share it among their analysts and with their customers. Most content within ESECS is viewable by the entire user population; however, access policies can be applied to any object to restrict access.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20340401

~~SECRET//REL TO USA, FVEY~~

dissemination. Such access to raw traffic is inconsistent with USSID SP0018, § 6.2, which requires that access to raw traffic storage systems containing identities of U.S. persons be limited to SIGINT production personnel. As a result, [] should develop: 1) written procedures for properly reviewing materials so that only evaluated and minimized traffic is posted on [] NSAnet website; and 2) access controls to ensure that only authorized personnel within the SIGINT production chain gain access to unminimized SIGINT, []

(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)

B. (U) Retention Period of U.S. Persons Information

(U//~~FOUO~~) In accordance with USSID SP0018, § 6.1.a, NSAG should assess the need to retain the summaries containing U.S. person information addressed in the Report of Investigation. []

[]

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

(U//~~FOUO~~) []

[]

C. (U) Noncompliance with Quarterly Reporting Requirements

(U//~~FOUO~~) Although [] currently provides informal input (by email, with no [] OIC review) for the NSAG Quarterly Report on Compliance with E.O. 12333 and Related Directives, this reporting does not meet the standard in USSID SE5120, which states:

3.6. (C//REL) [] will submit a quarterly report via NSA/CSS Georgia to the Office of Inspector General (OIG) of activity covered by Executive Order 12333 (*emphasis added*).³

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

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

(U//~~FOUO~~) The informal process used by NSAG to obtain [] input for the Quarterly Report does not ensure complete reporting and gives both [] and NSAG only limited visibility into [] compliance. In accordance with USSID SE5120 and NSA guidance, [] should prepare a complete and formal report, signed by the [] OIC, thereby certifying appropriate

³ The USSID mirrors standards in Paragraph 8.4 in USSID SP0018 and Paragraph 7.g. in NSA/CSS Policy 1-23.

~~SECRET//REL TO USA, FVEY~~

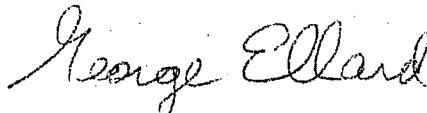
oversight of intelligence activities. The OIC is responsible for ensuring that [] SIGINT activities are lawful and not contrary to SIGINT authorities and that employees are aware of the authorities as they relate to the [] mission. NSAG should maintain copies of [] reports for review by oversight officials upon request.

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

(U//~~FOUO~~) We also noted that, in 2004 and 2005, [] IO training was not uniform for all personnel performing the [] mission and did not adhere to the standards set in NSA/CSS policies.⁴ In 2006, NSAG changed its IO training standards so that all personnel receiving an NSAG badge must complete NSAG IO training upon initial assignment and annually thereafter. Additionally, [] now uses Job Qualification Standards for linguists and analysts that all newly-assigned personnel must successfully complete. These procedures were not reviewed during the investigation, but will be evaluated during the upcoming Joint Inspection of NSAG scheduled for February 2010.

(U//~~FOUO~~) We request that NSAG, with the assistance of the [] provide us with a status of actions taken to resolve the aforementioned inconsistencies. We appreciate the courtesy and cooperation extended to the investigators throughout the investigation. If you need clarification or additional information, please contact [] on 963-2979 (s) or by e-mail at []@nsa.

(b) (6)



GEORGE ELLARD
Inspector General

⁴ Paragraph 7.b. in NSA/CSS Policy 1-23, and Paragraph 7.4 in USSID 5762(P).

~~SECRET//REL TO USA, FVEY~~