~~SECRET//COMINT//NOFORN~~

Attached to this letter is the Semiannual Report to Congress by the Inspector General of the National Security Agency for the period 1 April to 30 September 2010.

I adopt the statistics and other information contained in that report.

Sincerely,

GEN Keith B. Alexander
USA

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20351001~~

~~SECRET//COMINT//NOFORN~~

~~SECRET//COMINT//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

Further dissemination of this report outside NSA is ***PROHIBITED*** without the approval of the Inspector General.

(U) SEMIANNUAL REPORT TO CONGRESS
1 April to 30 September 2010

George Ellard
Inspector General

Derived from: NSA/CSSM 1-52
Dated: 20101031
Declassify on: ~~20351031~~

~~SECRET//COMINT//NOFORN~~

(U) NSA OFFICE OF THE INSPECTOR GENERAL

(U) The NSA Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA activities are conducted in compliance with the law. The OIG also serves as an ombudsman, assisting Agency employees, civilian and military, with complaints and questions.

(U) Intelligence Oversight

(U) The OIG Office of Intelligence Oversight reviews NSA's most sensitive and high-risk programs for compliance with the law.

(U) Audits

(U) The OIG Office of Audits within the OIG provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether NSA operations comply with federal policies. Information Technology audits determine whether IT solutions meet customer requirements, while conforming to information assurance standards. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) Investigations and Special Inquiries

(U) The OIG Office of Investigations administers a system for receiving and acting on requests for assistance and complaints about fraud, waste, and mismanagement. Investigations and special inquiries may be undertaken as a result of such requests and complaints (including anonymous tips), at the request of management, as the result of questions that surface during inspections and audits, or at the initiative of the Inspector General.

(U) Field Inspections

(U) The Office of Field Inspections conducts site reviews as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with an assessment of compliance with federal policy. The Office partners with Inspectors General of Service Cryptologic Components and other Intelligence Community Agencies to conduct joint inspections of consolidated cryptologic facilities.

(U) A MESSAGE FROM THE INSPECTOR GENERAL

(U) This report summarizes the more significant activities of the Office of the Inspector General (OIG) of the National Security Agency between 1 April and 30 September 2010. The report is mandated by the Intelligence Authorization Act of 2010.

(U) The most significant activity in the OIG during the reporting period was the continuing increase in the breadth and depth of the Office's expertise in information technology (IT), cyber, and intelligence oversight (IO). The NSA Director enabled this expansion of our capacities by supporting our efforts to hire superbly qualified recruits from the private sector and personnel steeped in NSA's mission from within the Agency.

(U) During the reporting period, the NSA OIG completed 60 audits, inspections, special studies, and investigations. The audits were almost evenly distributed across IO, IT, and mission programs.

(~~S//REL TO USA, FVEY~~) Completed IO reports included an advisory report on an OIG pilot test of NSA controls designed to ensure compliance with an Order of the Foreign Intelligence Surveillance Court (FISC) and monthly reports on OIG tests of FISC Order controls for January through July 2010. Reports related to mission programs included an audit of the Agency's Operational Test Authority, an audit of the Information Assurance Directorate's encryption interoperability, an audit of mission-assurance and continuity-of-operations compliance and testing, and a cyber research project. IT and cyber reports included an audit of [redacted] classified networks, an audit of the Agency's compliance with the Federal Information Security Management Act, and an audit of the Agency's Cross Domain Solutions.

(U) We also completed an external peer review of the investigative and audit offices within the OIG of the National Reconnaissance Office.

(U) The inspection staff completed reports on a joint inspection of the NSA/CSS Georgia Cryptologic Center and a headquarters inspection of the Agency's signals intelligence development strategy and governance.

(U) Special studies were completed on the [redacted] two SIGINT sites, data sharing with third-party partners, and the Selective Employment of Retirees/Standby Active Reserve Programs.

(U) The investigations staff opened 31 investigations and closed 44. (b)(3)-P.L. 86-36

(U) Each report and special study contained recommendations on which the OIG and NSA management concurred, recommendations designed to improve the efficiency and effectiveness of the programs under review. The OIG tracks recommendations until they have been implemented and regularly reports to the NSA Director on the status of open recommendations. Of the 210 recommendations issued in the reporting period, 68 have been closed.

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

George Ellard

George Ellard
Inspector General

DISTRIBUTION:

Dir
DDir
ExDir
CoS
D/C CSS
SID Dir
IAD Dir
CTO
RD
BMI
ODNI IG
DoD IG
CYBERCOM IG

cc:

LAO
OGC

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

(U) INDEX OF REPORTING REQUIREMENTS

(U)

I.G. Act	Reporting Requirement	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	3-8
§5(a)(2)	Recommendations for corrective action	3-8
§5(a)(3)	Previously reported significant recommendations not yet completed	N/A
§5(a)(4)	Matters referred to prosecutive authorities	9
§5(a)(5)	Information or assistance refused	N/A
§5(a)(6)	List of audit, inspection, and evaluation reports	13
§5(a)(7)	Summary of significant reports	3-8
§5(a)(8)	Audit reports with questioned costs	17
§5(a)(9)	Audit reports with funds that could be put to better use	21
§5(a)(10)	Summary of reports for which no management decision was made	N/A
§5(a)(11)	Significant revised management decisions	N/A
§5(a)(12)	Management decision disagreements	N/A

(U)

(U) This page intentionally left blank.

(U) AUDITS OF PARTICULAR SIGNIFICANCE

(U) The Operational Test Authority

(U) The audit objective was to evaluate the effectiveness of the Agency's Operational Test Authority (OTA) as NSA's independent testing authority.

(U//~~FOUO~~) **Finding** The OTA is not independent because of its 2007 realignment under the Technology Directorate (TD), which is responsible for developing technology for major systems. TD can influence OTA because it controls OTA's budget and reviews OTA's suggested changes to Agency policies and guidance.

(U//~~FOUO~~) **Recommendation** The OIG recommended establishing an independent OTA with direct reporting authority to the NSA Director.

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

(U) Cross Domain Solutions

(U//~~FOUO~~) The audit objective was to determine whether Cross Domain Solutions (CDSs) effectively and efficiently protect Agency networks. A CDS is a controlled interface that allows the secure transfer of data between domains with different security levels (e.g., Top Secret to Unclassified).

(~~S//NF~~) **Finding 1** Agency CDSs

(~~C//REL TO USA, FVEY~~) **Recommendation 1** The OIG recommended improving Agency CDS

(~~S//NF~~) **Finding 2** The Agency

(U//~~FOUO~~) **Recommendation 2** The OIG recommended developing a standard operating procedure (SOP) to document approved and allow system administrators to configure Agency CDSs. This SOP should require that changes be logged and controlled in an approved central repository.

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

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

(U) Mission-Assurance Continuity-of-Operations Compliance and Testing

(U//~~FOUO~~) In August 2008, NSA identified 14 Mission Essential Functions (MEFs) that must be performed in all circumstances. As of August 2009, [redacted] Agency organizations had been identified as being responsible for performing essential tasks that support one or more of the 14 MEFs.

(~~C//REL TO USA, FVEY~~) **Finding** [redacted]

(U//~~FOUO~~) **Recommendation** The OIG recommended that the Agency track organization compliance in developing complete COOP plans and performing annual updates and testing.

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

(U) INSPECTIONS OF PARTICULAR SIGNIFICANCE

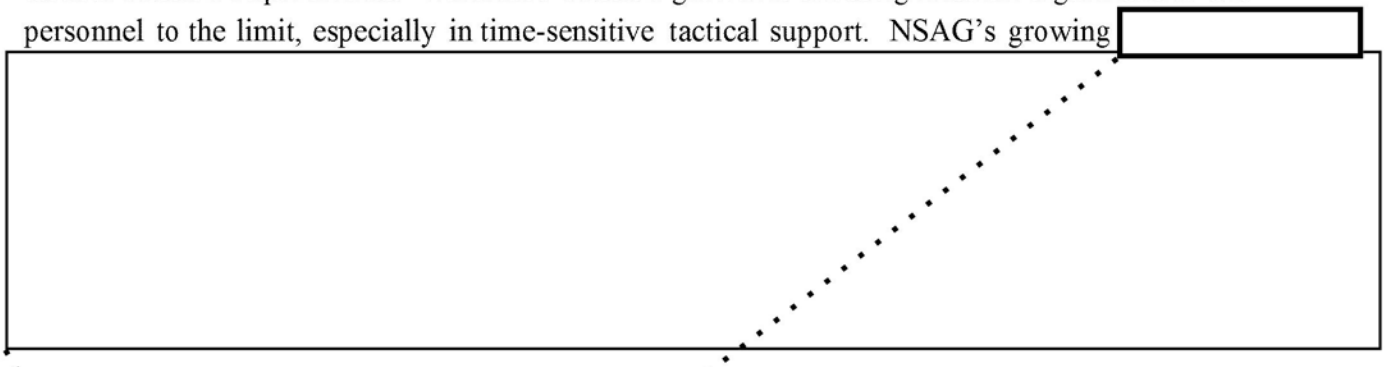
(U) NSA Georgia Cryptologic Center

(~~U//FOUO~~) During the reporting period the NSA Office of Inspections completed a Joint Inspection of the NSA Georgia (NSAG) Cryptologic Center at Fort Gordon, Georgia.

(U//~~FOUO~~) **Finding 1** Substantial growth in NSAG's Signals Intelligence, Information Assurance, and Computer Network Operations (CNO) missions and its information technology infrastructure has strained mission support resources. During the past five years, NSAG has experienced a large influx of joint and tactical personnel, who arrive without enabling support. They rely instead on NSA's heavily burdened support infrastructure. A root cause of this deficiency is the lack of clear manpower and budget requirements necessary to operate the cryptologic center.

(~~U//FOUO~~) **Recommendation 1** NSA Headquarters and NSAG should define, program for, and provide the minimum mission enabler personnel and funds needed to operate the Center effectively.

(~~C//REL TO USA, FVEY~~) **Finding 2** There are not enough joint operations personnel at NSAG to meet tactical mission requirements. Continued mission growth is stressing mission organizations and personnel to the limit, especially in time-sensitive tactical support. NSAG's growing



(~~U//FOUO~~) **Recommendation 2** The NSA Signals Intelligence Director should develop a business plan for the prioritization and appropriate distribution of tactical missions and associated resources at NSAG, taking into consideration the demands that additional mission will put on the site.

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

(U) This page intentionally left blank.

(U) SPECIAL STUDIES OF PARTICULAR SIGNIFICANCE

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

(U) Data Sharing with Third-Party Partners

(~~S//REL TO USA, FVEY~~) NSA's third-party partners are nations other than Australia, Canada, New Zealand, and the United Kingdom with which the U.S. government has national Signals Intelligence (SIGINT) arrangements. The purpose of the review was to determine whether policies and procedures are in place to ensure compliance with authorities for sharing [redacted] with third-party partners.

[redacted]

(~~S//NF~~) **Finding 1** Updated policies and process improvements are needed. Documentation for [redacted] disseminated to third-party partners is not centrally maintained. Limited documentation is scattered across many locations throughout the SIGINT Directorate (SID) and the Foreign Affairs Directorate (FAD). Documentation in FAD's Foreign Affairs Knowledge System is not current or easily retrievable.

(~~S//REL TO USA, FVEY~~) **Recommendation 1** FAD should establish a repository for documenting [redacted] shared with third-party partners, and it should update existing documentation.

(~~S//REL TO USA, FVEY~~) **Finding 2** Although SID's Analysis and Production Directorate (S2) developed a process in February 2007 to [redacted] disseminated to third-party partners, the process is not well understood, and it has never been reviewed. Quarterly guidance to the S2 workforce on how to [redacted] disseminated to partners is unclear, and, as a result, [redacted] is inconsistent.

(~~S//SI//REL TO USA, FVEY~~) **Recommendation 2** SID should revise its oversight process for disseminating [redacted] to partners, including [redacted] procedures, and inform the workforce of the revised process. SID should also publish an approval authority matrix for third-party activity and formal training on third-party partnerships and provide it to NSA personnel.

(~~S//SI//REL TO USA, FVEY~~) **Finding 3** SID lacks a standard process for [redacted]

(~~S//REL TO USA, FVEY~~) **Recommendation 3** SID should establish a standard process [redacted]

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

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

(U//~~FOUO~~) The

(U//~~FOUO~~) After the 11 September 2001 terrorist attacks on the United States, NSA established a Since then, has undergone several reorganizations; most recently, became an element of the SIGINT Development Strategy and Governance organization.

(U//~~FOUO~~) **Finding 1** lacks essential mission documentation and standards for NSA Headquarters and the Extended Enterprise.

(~~C//REL TO USA, FVEY~~) **Recommendation 1** should develop a Mission and Functions Statement, Strategic Plan, and implementing instructions, reflecting the evolving mission of external agencies. The documents should clearly define internal management controls in standard operating procedures, system configuration management, and budget documentation.

(U//~~FOUO~~) **Finding 2** has no Intelligence Oversight program.

(U//~~FOUO~~) **Recommendation 2** The should establish an Intelligence Oversight program in accordance with Department of Defense regulations and NSA policies.

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

(U) INVESTIGATIONS OF PARTICULAR SIGNIFICANCE

(U) Summary of Prosecutions

(U) Indictment

(U) An Agency employee was indicted in June 2010 for accepting more than $110,000 in bribes from a contractor as part of a scheme to defraud NSA. The trial is scheduled for January 2011 in the United States District Court in Baltimore, MD.

(U) Conviction

(U) A former Agency contractor pled guilty in July 2010 to submitting false labor charges for approximately $82,000. Sentencing occurred in October 2010 in the United States District Court in Baltimore, MD.

(U) Referrals

- (U) An Agency employee and timekeeper submitted 531.75 hours of false labor charges for a loss to the government of approximately $22,000. The case was presented to the Office of the United States Attorney for the District of Maryland in August 2010 and was accepted for prosecution.
- (U) A former Agency subcontractor submitted 34 false travel vouchers from 2007 to 2009 with claims of approximately $21,000. In May 2010, the case was presented to the Office of the United States Attorney for the District of Maryland. A decision on prosecution is pending.
- (U) An Agency contractor violated 18 U.S.C. §208 because he returned to NSA as a contractor within one year of his retirement as an NSA senior employee. The Office of the United States Attorney for the District of Maryland declined prosecution in July 2010.
- (U) Nine cases of contractor labor mischarging were referred to the Office of the United States Attorney for the District of Hawaii. Five cases have been declined for prosecution; decisions are pending on four. The amount of possible labor mischarging in these cases is approximately $180,000.
- (U) Ten cases of contractor labor mischarging were referred to the Office of the United States Attorney for the District of Maryland and were declined for prosecution. The possible mischarging in these cases was approximately $424,000.

(U) This page intentionally left blank.

(U) APPENDIX A

(U) AUDITS, INSPECTIONS, AND SPECIAL STUDIES COMPLETED IN THE REPORTING PERIOD

This page intentionally left blank.

(U) APPENDIX A

(U) AUDITS, INSPECTIONS, AND SPECIAL STUDIES COMPLETED IN THE REPORTING PERIOD

(U) Audits

- (U) The Cryptographic Interoperability Strategy/Suite B
- (U) Mission-Assurance Continuity-of-Operations Compliance and Testing
- (U) Compliance with the Federal Information Security Management Act
- (U) The Operational Test Authority
- (~~S//REL TO USA, FVEY~~) Cyber Security: NSA Response to [redacted] Classified Networks
- (U) Cross Domain Solutions
- (U) External Peer Review of NRO

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

(U) Inspections

- (U~~//FOUO~~) SIGINT Development Strategy and Governance
- (U) NSA Georgia Cryptologic Center

(U) Special Studies

- (U~~//FOUO~~) NSA Controls for a Classified Program (and monthly test reports from March through August 2010)
- (U~~//FOUO~~) [redacted]
- (U) Selective Employment of Retirees and Standby Active Reserve Programs
- (U) [redacted]
- (U) Cyber Research
- (U) Data Sharing with Third-Party Partners

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

(U) This page intentionally left blank.

(U) APPENDIX B

(U) AUDIT REPORTS WITH QUESTIONED COSTS

(U) This page intentionally left blank.

(U) APPENDIX B

(U) AUDIT REPORTS WITH QUESTIONED COSTS

(U)

Report	Number	Questioned Costs	Unsupported Costs
For which no management decision had been made by start of reporting period	0	0	0
Issued during reporting period	0	0	0
For which management decision was made during reporting period	0	0	0
Costs disallowed	0	0	0
Costs not disallowed	0	0	0
For which no management decision was made by end of reporting period	0	0	0

(U)

(U) Because our recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.

(U) This page intentionally left blank.

(U) APPENDIX C

(U) AUDIT REPORTS OF FUNDS THAT COULD BE PUT TO BETTER USE

(U) This page intentionally left blank.

(U) APPENDIX C

(U) AUDIT REPORTS OF FUNDS THAT COULD BE PUT TO BETTER USE

(U)

Report	Number	Amount
For which no management decision had been made by start of reporting period	0	0
Issued during reporting period	0	0
For which management decision was made during reporting period	0	0
Value of recommendations agreed to by management	0	0
Value of recommendations not agreed to by management	0	0
For which no management decision was made by end of reporting period	0	0

(U)

(U) Because our recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.