~~TOP SECRET//SI/TK//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

(U) SEMI-ANNUAL REPORT TO CONGRESS
1 April to 30 September 2012

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20371031~~

~~TOP SECRET//SI/TK//NOFORN~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General 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 by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to ensure that Agency intelligence functions comply with federal law, Executive Orders, and DoD and NSA policies. The intelligence oversight mission is grounded in Executive Order 12333, which establishes broad principles under which Intelligence Community components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect 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/Central Security Service between 1 April and 30 September 2012. The report is mandated by the Inspector General Act of 1978.

(U) During the reporting period, the NSA OIG completed 17 audits, inspections, and special studies.

(U) The Audits Division completed seven audits spanning operations, finance, compliance with law and policy, and peer review.

(U) The Inspections Division completed reports on one joint inspection and three field inspections of NSA field sites.

(U) The Intelligence Oversight Division completed six special studies of information technology, operations, and compliance with law and policy.

(U) The Investigations Division fielded 556 contacts from the OIG Hotline. The team opened 45 investigations and closed 26 in the reporting period.

(U) Each report and special study contained recommendations on which the OIG and NSA management concurred, 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 257 recommendations issued in the reporting period, 113 have been closed.

(U) The Agency continues to recognize the independence of the OIG and has given this Office the resources it needs to fulfill its function.

(U) This semi-annual report, by concentrating on the findings of audits and other studies, points to areas in which the Agency can make and has made improvements. Senior management seems committed to making those improvements and is to be commended for its continued successful dedication to NSA's mission.

George Ellard

George Ellard
Inspector General

(U//~~FOUO~~) DISTRIBUTION:

DIR
DDIR
ExDIR
CoS
SID Dir
IAD Dir
TD Dir
LAO
OGC
ODOC
FAD
BMI
SAE
ODNI IG
DoD IG

(U) TABLE OF CONTENTS

(U) INDEX OF REPORTING REQUIREMENTS

(U)

IG Act	Reporting Requirement	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	1-2
§5(a)(2)	Recommendations for corrective action	1-2
§5(a)(3)	Previously reported significant recommendations not yet completed	4-6, 14-15
§5(a)(4)	Matters referred to prosecutorial authorities	17
§5(a)(5)	Information or assistance refused	N/A
§5(a)(6)	List of audit, inspection, and evaluation reports	19
§5(a)(7)	Summary of significant reports	1-2
§5(a)(8)	Audit reports with questioned costs	21
§5(a)(9)	Audit reports with funds that could be put to better use	23
§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) SIGNIFICANT PROBLEMS, ABUSES, AND DEFICIENCIES

(U) Recommendations for Corrective Action

(U) OIG studies during the reporting period did not reveal particularly serious or flagrant problems, abuses, or deficiencies related to the administration of Agency programs and requiring immediate reporting to the Director and Congress. The OIG did identify at least two significant problems that it has not yet resolved with management

I. (U//~~FOUO~~) **Audit of the Price Reasonableness of Agency-Awarded Contracts**

(U//~~FOUO~~) This audit was performed because Department of Defense audits had concluded that Contracting Officers (COs) were not performing or documenting price reasonableness determinations in accordance with the Federal Acquisition Regulation. The NSA OIG audit made the following recommendation:

- (U//~~FOUO~~) Develop a database of direct labor categories that includes rates and skill levels (work experience) that can act as a "yardstick" to assist COs in price reasonableness determinations. The database should take into consideration labor qualifications and competitively awarded contract rates to aid in performing cost comparisons.

II. (U//~~FOUO~~) **Special Study of the Retention of Domestic Communications Collected Under Foreign Intelligence Surveillance Act (FISA) Surveillances**

(U//~~FOUO~~) While conducting collection operations authorized under FISA, NSA incidentally collects domestic communications subject to retention limitations. The following significant recommendation has not been resolved:

- (U//~~FOUO~~) Per NSA/CSS Policy 1-12, baseline and document configurations of systems that process and store FISA data. Specifically, delineate data retention and standards and purging procedures in accordance with USSID SP0018 standards.

(U//~~FOUO~~) Although we directed responsibility for this recommendation to SID, no NSA element is addressing system configuration management standards in accordance with NSA/CSS Policy 1-12. Without system configuration management documentation, NSA leadership has limited assurance that the systems are configured to retain and purge FISA data as legally required.

(U) Significant Revised Management Decisions

(U) No management decisions have been significantly revised.

(U) AUDITS

(U) Audits Completed in the Reporting Period

(U) **Application Controls of the [redacted] Contracting System** (b)(3)-P.L. 86-36

(U//~~FOUO~~) NSA's Comptroller requested that the OIG review selected business support systems as part of the Agency's efforts to prepare for a financial statement audit. We found two control deficiencies in documentation and system monitoring of the Agency's automated contracting system. Business Management IT Support has updated system documentation and, along with Information and System Security Risk Management, has agreed to establish a monitoring capability with a process to review application logs. These findings do not constitute material weaknesses in regard to the Agency's financial statements.

(U) **External Quality Control Review of the National Geospatial-Intelligence Agency (NGA) Office of Inspector General Audit Staff**

(U//~~FOUO~~) We issued a "pass" opinion because we determined that the quality control system of the NGA OIG Audit Staff was adequately designed and functioning as prescribed. The concerns discovered during review of two audit projects and three non-audit projects were not significant enough to signify that material deficiencies existed in the NGA OIG process to comply with Government Auditing Standards. We provided suggestions to correct these deficiencies.

(U) **Oversight Review of the Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop**

(b) (6)

(U//~~FOUO~~) [redacted] a Certified Public Accountancy firm, issued unqualified opinions on the reliability of the financial statements of the Agency's Restaurant Fund and Civilian Welfare Fund. However, the firm raised concerns about high-speed Internet connectivity related to credit card transactions, prepaid expenses and inventory determination, anticipated oversight transition, and the Museum Gift Shop budget. The OIG's review concurred with these observations.

(U) **United Kingdom Tax Program for Defense Contractors**

(U//~~FOUO~~) The audit team reviewed the process for adding contractor employees to and removing them from the UK Tax Program and evaluated the program documentation that the Special United States Liaison Office London maintains. We found that contractor employees were working at [redacted] sites not listed in the original Memorandum of Understanding, and we found no official documentation that the United Kingdom had approved these sites for inclusion in the Tax Program. We also found seven problems with the program, including insufficient or lack of documentation and lax processes.

(U) **Price Reasonableness Determinations for Agency Contracts**

(U//~~FOUO~~) We reviewed 94 sole-source contracts to determine whether the Agency's Directorate of Acquisition is complying with Federal Acquisition Regulation requirements for

determining price reasonableness. In 68 of 94 contracts, Contracting Officers (COs) had performed minimal analysis and cost and price validation to justify their price reasonableness determinations. COs must improve these determinations to ensure that goods and services are obtained at fair and reasonable prices. We found three areas in which COs' price reasonableness determinations require improvement: Sole-source labor contracts, sole-source simplified acquisitions, and escalation rates. The OIG calculated that $3.56 million could have been saved had COs followed guidance on determining price reasonableness.

(U) **Government Purchase Card Program**

(U//~~FOUO~~) The objective of this audit was to determine whether the Agency's Government Purchase Card Program, which was established by the Department of Defense (DoD) to streamline acquisition processes for obtaining goods and services directly from vendors, complies with DoD and Agency policies and regulations. We found that seven of the 20 mandatory internal controls need strengthening to comply with those policies.

(U) **Agency's Compliance with the Federal Information Security Act (FISMA)**

(U//~~FOUO~~) FISMA requires that agencies measure the adequacy and effectiveness of their information security environment and the systems that operate within that environment. The FY2012 FISMA OIG audit details the Agency's efforts during the past year to improve information technology (IT) processes and track Agency and system weaknesses.

(U) Significant Recommendations Outstanding in Previous Semi-Annual Reports

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

(U) **Cross Domain Solutions (CDSs)**

(U//~~FOUO~~) The audit objective was to determine whether 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).

(~~C//REL TO USA, FVEY~~) **Finding** Agency CDSs

(U//~~FOUO~~) **Recommendation** Improve Agency CDS for all operational CDSs.

(U//~~FOUO~~) **UPDATE:** IT Policy plans to include in Agency Policy 6-8, *NSA/CSS Information Systems and Network Data and Software Transfers*, a requirement that all Agency CDSs has coordinated with Corporate Policy, Enterprise IT Implementation and Management, and the Unified Cross Domain Management Office to develop a draft policy and plans to have an Agency review by 31 October 2012. This action is due September 2013.

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

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

(U//~~FOUO~~) Active Security plans to deploy a risk assessment tool that allows Agency personnel to score their CDS against baseline configuration controls. also plans to deploy automated solutions to detect security baseline security control deficiencies. These actions are due by the end of FY2014.

(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, Agency organizations had been identified as responsible for performing essential tasks that support one or more of the 14 MEFs.

(~~C//REL TO USA, FVEY~~) **Finding** A small percentage of the organizations maintained complete, updated, and operationally tested Continuity of Operations (COOP) plans.

(U//~~FOUO~~) **Recommendation** Track organization compliance in developing complete COOP plans and performing annual updates and testing.

(U//~~FOUO~~) **UPDATE:** No progress noted since last report. This action was due June 2011.

(U) **Agency Controls for IT Hardware Purchases**

(~~C//REL TO USA, FVEY~~) The audit concluded that the Agency's Supply Chain Risk Management (SCRM) strategy

(~~C//REL TO USA, FVEY~~) **Finding** purchase controls

(~~C//REL TO USA, FVEY~~) **Recommendation**

(U//~~FOUO~~) **UPDATE:** TD has not produced the policy. This action was due November 2011.

(U//~~FOUO~~) **Recommendation**

(U//~~FOUO~~) **UPDATE:** No progress noted. This action was due November 2011.

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

(U//~~FOUO~~) **Finding** No central management of incidents

(U//~~FOUO~~) **Recommendation**

(U//~~FOUO~~) **UPDATE:** TD has not established the process. This action was due September 2011.

(U) **Nuclear Command and Control (NC2)**

(U//~~FOUO~~) The NC2 program Since 2003, approximately recommendations related to NC2 have been made by auditors and vulnerability assessment teams. The focus of the current audit was to ensure that actions taken satisfied previous recommendations. In addition, the audit reviewed new problems discovered since a 2006 OIG audit.

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

(U) **Finding** Problems with previously closed recommendations.

(~~S//NF~~) **Recommendation** Develop a [redacted] and establish a timeline for completion.

(U//~~FOUO~~) **UPDATE:** NC2's response to this recommendation is being coordinated with the Information Assurance Directorate. This action was due December 2011.

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

(U//~~FOUO~~) **Audit of NSA/CSS Wireless Networks and Devices**

(~~C//REL TO USA, FVEY~~) Wireless devices and networks pose significant security risks to wired and wireless networking infrastructures when not properly implemented. The audit concluded that the Agency has not defined and implemented an enterprise wireless Information Assurance program. As a result, [redacted]

(U) **Finding** No enterprise wireless Information Assurance program

(U//~~FOUO~~) **Recommendation** Develop an Agency wireless Information Assurance program, in accordance with CNSS Policy No. 17, that assigns the responsibility of oversight, coordination, and inventory management control of all authorized wireless networks and devices within the Agency.

(U//~~FOUO~~) Technology Directorate (TD) management agreed to implement this recommendation by 30 September 2012. **UPDATE:** Although TD has operational authority over the installation and deployment of IT infrastructure throughout the NSA/CSS enterprise, other NSA/CSS organizations are implementing wireless solutions independent of TD. TD is working to migrate each Directorate into the standard Change and Configuration processes that establish roles and responsibilities for critical stakeholders of wireless devices and maintain the Configuration Management Data Base that accounts for all wireless devices in the agency. TD is also working to provide monitoring, incident management, and problem management services. TD has revised its target completion date to 31 May 2013.

(U) Ongoing Audits

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

(U//~~FOUO~~) [redacted] **Program**

(U//~~FOUO~~) The audit objective is to determine whether system and security controls sufficiently protect the Agency's [redacted] program data and information, in accordance with Intelligence Community Directive 503, *Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation.*

(U) Export Controls

(U) The audit objective is to determine whether NSA's export control process complies with laws, regulations, and authorities.

(U) Cleared Defense Contractor Access to NSANet

(U) The audit objective is to determine whether cleared defense contractors' IT security controls protect Agency data and information in accordance with Intelligence Community Directive 503, *Intelligence Community Information Technology System Security Risk Management, Certification, and Accreditation.*

(U) **Human Resources Management System**

(U~~//FOUO~~) The NSA Comptroller has requested a review of application controls in the Agency's Human Resources Management System, as part of the Agency's quest to achieve financial auditability.

(U) **Civilian Pay and Benefits**

(U) The audit objective is to determine whether pay and benefits for civilian personnel were correctly paid and properly authorized for selected disbursals, such as overtime pay and administrative leave.

(U) **Key Management Infrastructure Program (KMI)**

(U) The audit objective is to determine the effectiveness of KMI in meeting program goals.

(U) **Conference Expenses**

(U) The audit objective is to determine the reasonableness of conference expenses.

(U) **NSA [redacted] Program**

(U~~//FOUO~~) The audit objective is to determine whether the Agency's [redacted] program complies with NSA/CSS and DoD policies and meets mission needs cost-efficiently.

(U) **Security System Testing of NSA/CSS Systems in Support of the Federal Information Security Management Act of 2002 (FISMA)**

(U~~//FOUO~~) The purpose of this testing is to assess system-specific security data for FISMA compliance.

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

(U) **Geospatial Tools**

(U) The audit objective is to determine whether the Agency's use of geospatial tools is cost-effective and meets customer requirements.

(U) This page intentionally left blank.

(U) INSPECTIONS

(U) Inspections Completed in the Reporting Period

(U//~~FOUO~~) **Inspection of Utah Regional Operations Center (UROC)**

(U//~~FOUO~~) This was the first IG inspection of UROC. The overall UROC command climate is positive. However, the Director and members of the workforce cited the Foreign Language Incentive Pay program as a concern because it provides greater rewards for analysts with proficiency in multiple languages than it does for analysts with deep expertise in a single, difficult language of high operational value. The UROC Director lacks staff who understand NSA's budget and contracting processes. Lack of centralized budget and financial planning for the site at higher headquarters is a related problem. The concerns noted during the inspection stem largely from the site's heavy reliance on enabling function support from inadequately trained or overburdened NSA civilians and Utah National Guard personnel unfamiliar with NSA standards.

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

(U//~~FOUO~~) **Short-Notice Limited-Scope Inspection of**

(U//~~FOUO~~) The inspection was limited to a review of IO program management, training, access to raw traffic databases, and dissemination of SIGINT. The OIG team found compliant with NSA policy for protecting and disseminating SIGINT information.

(U) **Inspection of NSA/CSS Pacific (NCPAC)**

(U//~~FOUO~~) NCPAC is well run and recognized by NSA/CSS organizations and external customers alike for its excellent support on regional issues. NCPAC Cryptologic Services Group Pacific (CSG PAC) analysts CSG PAC personnel provide liaison, coordination, advice, and assistance to USPACOM and its component commands and subordinate units and to NSA/CSS Hawaii on SIGINT support of USPACOM programs and operations.

(U//~~FOUO~~) The chief challenges at NCPAC arise from changes in civilian employee pay policies, which are expected to make attracting and retaining qualified personnel in Hawaii more difficult. NSA/CSS regional efficiency activities under way, such as the Information Assurance Directorate's construct and the creation of the Technology Regional Center Hawaii, will reduce the size of the NCPAC workforce. Functions performed at NCPAC will be consolidated elsewhere. NCPAC leadership is engaged in planning to ensure smooth transitions for the workforce as the role of the organization evolves.

(U//~~FOUO~~) **Joint Inspection of Aerospace Data Facility Colorado (ADF-C)**

(U//~~FOUO~~) ADF-C is recognized for its outstanding mission accomplishment, unwavering commitment and dedication of its workforce, and the joint construct of the site. The workforce has produced operational successes that would not have been possible without the outstanding collaborative work from the National Reconnaissance Office, NSA/CSS, National Geospatial-

Intelligence Agency, service members, and contractors. However, the site faces multiple challenges that could affect future operational successes: budget reductions, expanding mission, competing requirements, and changing personnel practices.

(U//~~FOUO~~) There were many repeat findings from the last Joint Inspection in October 2008 concerning communications and IT. Inspectors and senior IGs noted that the site-wide IT infrastructure hinders communication among the workforce, negatively affecting their ability to perform effectively and efficiently. [redacted] at the site present a roadblock to efficient operations.

(U//~~FOUO~~) Multiple training standards across the agencies and military services force site personnel to take the same training three or four times, particularly in Information Assurance and IO. Not having common IC training standards or reciprocal agreements to recognize common mandatory training requirements has been cited as a concern at other sites in several Joint IG reports since 2008.

(U) Significant Recommendations Outstanding in Previous Semi-Annual Reports

(U) All significant recommendations from previous reports have been implemented. (b)(3)-P.L. 86-36

(U) Ongoing Inspections

(U) **Field Inspection of NSA/CSS Representative to U.S. Southern Command (NCR SOUTH)**

(U//~~FOUO~~) The Inspections Division conducted a field inspection of NCR SOUTH from 23 April through 1 May 2012. The final report is in coordination.

(U) **Field Inspection of NSA/CSS Europe and Africa (NCEUR-AF)**

(U//~~FOUO~~) The Inspections Division conducted a field inspection of NCEUR-AF from 4 through 8 June 2012. The final report is in coordination.

(U) **Joint Inspection of Meade Operations Center (MOC)**

(U//~~FOUO~~) The Inspections Division conducted a joint inspection of MOC from 29 July through 2 August 2012. The final report is in coordination.

(U) **Field Inspection of NSA/CSS Representative to the Central Intelligence Agency (NCR-CIA)**

(U) The Inspections Division conducted a field inspection of NCR-CIA from 20 through 31 August 2012. The working draft is in process.

(U//~~FOUO~~) **Field Inspection of** [redacted]

(U//~~FOUO~~) The Inspections Division conducted a field inspection of [redacted] The working draft is in process.

~~(S//REL TO USA, FVEY)~~ **Field Inspection of** [redacted]

~~(S//REL TO USA, FVEY)~~ The Inspections Division conducted a field inspection of [redacted] The working draft is in process.

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

(U) This page intentionally left blank.

(U) SPECIAL STUDIES

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

(U) Special Studies Completed in the Reporting Period

~~(S//REL TO USA, FVEY)~~ **Computer Network Exploitation (CNE) Operations**

~~(TS//SI//REL TO USA, FVEY)~~ Computer Network Exploitation operations by the Signals Intelligence Directorate's present a high IO risk. To help mitigate the risk that could exceed its authorities, we recommended improvements in documentation for operations, employee understanding of IO requirements, and changing employee perception of their Senior Technical Writer as lawyer.

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

(U) **Mission Compliance and Inherently Governmental Functions**

~~(S//REL TO USA, FVEY)~~ The review of computer network exploitation operations revealed that the responsibilities of those performing mission compliance duties at NSA/CSS Washington (NSAW) are unclear. To resolve this, we recommended (1) defining mission compliance responsibilities and applying them consistently throughout NSAW, (2) determining which mission compliance responsibilities are inherently governmental and which are close to inherently governmental, and (3) establishing contract administration procedures when contractors perform mission compliance duties close to inherently governmental.

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~ The Three of the five recommendations made were closed before report publication.

~~(TS//SI//NF)~~ **NSA Controls for Foreign Intelligence Surveillance Court Order Regarding Business Records (BR) Collection**

~~(TS//SI//NF)~~ From December 2011 through March 2012, we performed testing and procedural reviews to assess the Agency's compliance. Other than one incident that NSA reported during our review, we found no instance of non-compliance with the Order for BR collection during calendar year 2011. Areas for improvement include accessibility of program material, keeping meeting notes, BR reconciliation, management oversight, and review of structure code test used in sampling. Two of the five recommendations made were closed before report publication.

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

(U//~~FOUO~~) **Review of [redacted] Intelligence Oversight Program**

~~(S//REL TO USA, FVEY)~~ We reviewed the [redacted] intelligence oversight program and determined that certain program activities were not in compliance with NSA/CSS policies and [redacted] instructions. [redacted] lacked centralized management and internal controls of IO activities, and there were weaknesses in [redacted] IO training. These weaknesses increase the risk of improper handling of SIGINT data and increase the potential for the organization to exceed its authorities. [redacted] management agreed to corrective actions that meet the intent of the recommendations.

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

(U//~~FOUO~~) The objective of this study was to assess the handling and protection of raw SIGINT data associated with [redacted] to ensure compliance with NSA authorities.

~~(S//SI/TK//REL TO USA, FVEY)~~ Our review of the processes associated with SIGINT data [redacted] revealed the following control weaknesses:

- (U//~~FOUO~~) Lack of proper authorization to have data at some sites,
- (U//~~FOUO~~) Lack of oversight of how [redacted]
- (U//~~FOUO~~) Lack of required IO training, and
- (U//~~FOUO~~) Insufficient [redacted]

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

(U//~~FOUO~~) [redacted] NSA have agreed with the recommendations in this report.

(U) Significant Recommendations Outstanding in Previous Semi-Annual Reports

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

(U) **Data Sharing with Third Party Partners**

(U//~~FOUO~~) 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 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]

(U//~~FOUO~~) **Finding** SID's dissemination of [redacted] to Third Party partners lacks adequate controls.

(U//~~FOUO~~) **Recommendation** Review and revise the 2007 oversight process for disseminating [redacted] to partners, including [redacted] procedures. Inform the workforce of the revised process.

(U) **UPDATE:** Although SID has revised the oversight process, it has not formally approved it or communicated it to the workforce. This action was due in November 2011.

(U) [redacted]

(U//~~FOUO~~) After the 11 September 2001 terrorist attacks on the United States, NSA established an [redacted]

(U//~~FOUO~~) **Finding** [redacted] lacks essential authorizing mission documentation and standards.

~~(C//REL TO USA, FVEY)~~ **Recommendation** Publish and publicize the missions and functions of [redacted] clearly defining the division of effort, prioritization, measures of success, and responsibilities of personnel.

(U//~~FOUO~~) **UPDATE:** [redacted] has drafted documentation. This action was due in September 2011.

(U//~~FOUO~~) **Finding** [redacted] lacks an IO program.

(U//~~FOUO~~) **Recommendation** Designate an [redacted] IOO focused on IO standards and practices to establish an [redacted] SOP that clearly delineates the standards for accepting, loading, processing, storing, reporting, and querying data associated with U.S. persons in accordance with DoD Regulation 5240.1-R and other regulations and instructions.

(U//~~FOUO~~) **UPDATE:** [redacted] has drafted documentation. This action was due in December 2011.

(U) Ongoing Special Studies

(U//~~FOUO~~) **Management Controls for NSA Compliance with Section 702 of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA §702)**

(U//~~FOUO~~) The study objective is to determine whether NSA controls are adequate to provide reasonable assurance that the Agency complies with the terms of FAA §702.

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

(U//~~FOUO~~) **SIGINT Threat Warning**

~~(S//REL TO USA, FVEY)~~ The study objective is to evaluate the efficiency and effectiveness of SIGINT threat warning support to [redacted] The study focuses on support to [redacted]

~~(TS//SI//REL TO USA, GBR)~~ **Management Controls for Implementation of FAA §702**

[redacted]

~~(C//REL TO USA, GBR)~~ The study objective is to determine whether controls established by the Agency, [redacted] are adequate to ensure compliance with [redacted]

(U) **Research Directorate's (RD) Intelligence Oversight and Compliance Program**

(U) The study objective is to review IO practices within RD to determine employee awareness of IO responsibilities and whether policies and procedures ensure compliance with IO authorities.

(U) [redacted] **Mission Compliance Program**

(U) The study objective is to ensure that management controls and IO practices have been and will continue to be incorporated into [redacted] while the product and service are being developed and to review IO practices to determine whether project managers are adequately considering IO policies and processes that ensure compliance with applicable authorities.

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

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

(U) This page intentionally left blank.

(U) INVESTIGATIONS

(U) Summary of Prosecutions

(U) As reported in the last Semi-Annual Report to Congress, three family members who ran the Bechdon Company, Inc., of Upper Marlboro, Maryland, were convicted of conspiring to commit and committing wire fraud arising from a fraudulent billing scheme on an NSA contract.

(U) On 3 May 2012, the United States Attorney's Office for the District of Maryland entered into a non-prosecution agreement with the Bechdon Company for all crimes arising out of the conspiracy. The government entered into the agreement in part because Bechdon cooperated in the investigation of the NSA overbilling scheme. As part of the agreement, Bechdon has agreed to pay a $1 million penalty to the government, sell all or substantially all its business operations, and accept the resignation of the company president no later than 31 December 2012. The monetary penalty schedule required an initial $600,000 payment to the United States Treasury within 14 days of the agreement, followed by $20,000 per month for 20 months or until Bechdon has paid the United States Treasury $1 million. These payments have been made as required.

(U) Referrals

(U//~~FOUO~~) The OIG Investigations Division has referred 48 matters to other organizations within the Agency.

(U) OIG Hotline Activity

(U//~~FOUO~~) The Investigations Division fielded 556 contacts through the OIG Hotline.

(U) Investigations

(U//~~FOUO~~) Forty-five investigations were opened and 26 were closed in the reporting period.

(U) This page intentionally left blank.

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

(U) Audits

(U) **Operations**

- (U) United Kingdom Tax Program for Defense Contractors
- (U) Price Reasonableness Determinations for Agency Contracts
- (U) Government Purchase Card Program

(U) **Finance**

- (U) Oversight Review of the Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop

(U) **Information Technology**

- (U) Application Controls of the [redacted] Contracting System
- (U) Agency's Compliance with the Federal Information Security Act

(U) **Peer Review**

- (U) External Quality Control Review of the National Geospatial-Intelligence Agency Office of Inspector General Audit Staff

(U) Inspections

(U) **Field Inspections**

- (U//~~FOUO~~) Utah Regional Operations Center
- (U//~~FOUO~~) [redacted]
- (U) NSA/CSS Pacific

(U) **Joint Inspections**

- (U//~~FOUO~~) Joint Inspection of Aerospace Data Facility Colorado

(U) Special Studies

(U) **Information Technology**

- (U//~~FOUO~~) Computer Network Exploitation by [redacted]

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

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

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

(U) **Operations**

- (U//~~FOUO~~) Mission Compliance and Inherently Governmental Functions
- ~~(TS//REL TO USA, FVEY)~~ [redacted]
- (U//~~FOUO~~) [redacted] Intelligence Oversight Program

(U) **Federal Compliance**

- ~~(TS//SI//NF)~~ NSA Controls for FISC Order Regarding Business Records (BR) Collection

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

(U) APPENDIX B
AUDIT REPORTS WITH QUESTIONED COSTS

(U//~~FOUO~~)

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	1	$3.56 million	$3.56 million
For which management decision was made during reporting period	1	$3.56 million	$3.56 million
Costs disallowed	1	0	0
Costs not disallowed	0	$3.56 million	$3.56 million
For which no management decision was made by end of reporting period	0	0	0
(U) Because OIG 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//~~FOUO~~)

(U) This page intentionally left blank.

(U) APPENDIX C
AUDIT REPORTS WITH FUNDS THAT COULD BE PUT TO BETTER USE

(U)

Report	Number of Reports	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) Because OIG 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)

(U) This page intentionally left blank.

(U) APPENDIX D
RECOMMENDATIONS SUMMARY

(U//~~FOUO~~) The OIG made 257 recommendations to NSA management in reports issued in the third and fourth quarters of FY2012: 64 in the third and 193 in the fourth. During the third and fourth quarters, the Agency implemented 105 and 50 recommendations, respectively.

(U) Managers fully implemented recommendations made in the following reports by the end of the second half of FY2012:

- (U) Audit of Foreign Intelligence Relationships (16 December 1999)
- (U) Status of McCreight Study Recommendations (14 September 2007)
- ~~(C//REL TO USA, FVEY)~~ Joint Inspection of NSA/CSS Europe/European Technical Center (18 December 2007)
- (U) Follow-up of Time Synchronization (23 January 2008)
- (U//~~FOUO~~) Field Inspection of the Office of China and Korea (26 September 2008)
- ~~(C//REL TO USA, FVEY)~~ Joint Inspection of [redacted]
- (U) Audit of Associate Directorate for Education and Training IT Infrastructure (28 July 2009)
- (U) Audit of Operational Test Authority (12 May 2010)
- ~~(C//REL TO USA, FVEY)~~ Audit of [redacted] (8 November 2011)

[redacted]
(b)(3)-P.L. 86-36

(U) This page intentionally left blank.