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

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

(U) SEMI-ANNUAL REPORT TO CONGRESS
1 April to 30 September 2011

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

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

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the 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 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 between 1 April and 30 September 2011. The report is mandated by the Intelligence Authorization Act of 2010.

(U) During the reporting period, the NSA OIG completed 59 audits, inspections, special studies, and investigations.

(U) The Audits Division completed five audits ranging from Information Technology to federal compliance to operations.

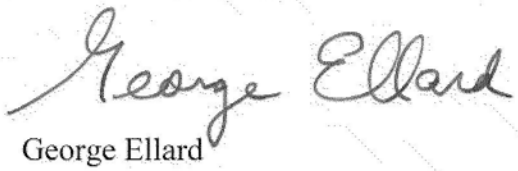
(U) The Inspections Division completed reports on two joint inspections of NSA field sites and one expeditionary operations review of [redacted] (b)(3)-P.L. 86-36

(U) The OIG completed five special studies of operations and intelligence oversight.

(U) The Investigations Division fielded 571 contacts from the OIG Hotline. The team opened 53 investigations and closed 46 in the reporting period.

(U) The office also completed internal quality assurance reviews of the Joint Inspection program and the follow-up process.

(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 213 recommendations issued in the reporting period, 36 have been closed.



George Ellard
Inspector General

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

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

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

(U) SIGNIFICANT PROBLEMS, ABUSES, AND DEFICIENCIES

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

(U//~~FOUO~~) OIG work during the reporting period did not reveal any particularly serious or flagrant problems, abuses, or deficiencies related to the administration of Agency programs and operations requiring immediate reporting to the Director and to Congress.

(U//~~FOUO~~) Completed reports did identify [redacted] significant problems related to Agency operations and made appropriate recommendations. Agency managers agreed with all recommendations; however, corrective action plans were not provided for one of the [redacted] significant recommendations.

(U) **Audit of Agency Controls for [redacted] IT Hardware Purchases** (29 April 2011)

(U//~~FOUO~~) The audit concluded that the Agency's Supply Chain Risk Management (SCRM) strategy [redacted]

(U) The audit included three significant recommendations: [redacted]

(U) **Audit of Nuclear Command and Control (NC2)** (23 September 2011)

(U//~~FOUO~~) The NC2 program [redacted] Since 2003, approximately [redacted] 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 the 2006 OIG audit.

(~~TS//NF~~) The audit revealed that all but [redacted] recommendations have been adequately closed. Key recommendations from 2005 dealing with [redacted] Appropriate corrective action has been taken for [redacted]

(U) The audit made two significant recommendations:

- (U//~~FOUO~~) Complete the testing and approval requirements for the accountability system to provide 100 percent assurance of the [redacted]
- (~~S//NF~~) [redacted] and establish a timeline for completion. (Management did not provide a corrective action plan for this recommendation.)

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

(U//~~FOUO~~) **Special Study of Non-Traditional Dissemination Methods: Dissemination Strategy Evaluation** (28 September 2011)

(U//~~FOUO~~) Since 2011, NSA has worked to address the challenges and opportunities presented by a Presidential call for increased information sharing. Various non-traditional dissemination methods have been implemented to facilitate that effort. The review, which focused on select processes and tools that analysts use for non-traditional dissemination, revealed that the Signals Intelligence Directorate (SID) does not have a comprehensive dissemination plan and that the Directorate's implementation of the IC-wide information-sharing system known as [redacted] resulted in confusion and overly restrictive limitations on its use.

(U//~~FOUO~~) The report made three significant recommendations:

- (U//~~FOUO~~) Conduct a strategic review of dissemination policy and create a comprehensive dissemination plan.
- (U//~~FOUO~~) Re-evaluate the internal controls used for [redacted] and the operating principles for NSA/CSS participation in the tool.
- (U//~~FOUO~~) Update the [redacted] and announce the new guide to the analytic workforce.

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

(U//~~FOUO~~) SID took immediate steps to implement the two recommendations related to [redacted] and they have been closed.

(U) AUDITS

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

(U) Audits Completed in the Reporting Period

(U) **Agency Controls for [redacted] IT Hardware Purchases** (29 April 2011)

(U//~~FOUO~~) Because of the growing reliance on globally sourced Information Technology (IT), Agency systems and networks [redacted]

(U) **NSA Police (NSAP) Operations** (9 May 2011)

(U//~~FOUO~~) Controls over NSAP equipment inventories must be tightened, and NSA needs a formal agreement with Fort Meade for Vehicle Cargo Inspection Facility (VCIF) services. NSAP management lacks a process to determine needs for operational equipment and supplies. As a result, Agency funds are not used economically and efficiently and inventory records are inaccurate. [redacted] The Agency spends more than [redacted] a year in salary expenditures [redacted] K-9 teams) for approximately [redacted] NSA and Fort Meade vehicle and cargo inspections. The Agency must formalize the VCIF operation agreement with Fort Meade to ensure a clear understanding of roles and responsibilities. We referred this matter to the Office of General Counsel for review.

(U) **NSA/CSS Compliance with the Federal Information Security Management Act (FISMA)** (13 September 2011)

(U//~~FOUO~~) FISMA requires measurements of the adequacy and effectiveness of the federal government's information security environment and systems that operate within that environment. The audit details the Agency's efforts during the past year to improve IT processes and track Agency and system weaknesses. More work must be done [redacted]

(U) **Nuclear Command and Control (NC2)** (23 September 2011)

(U//~~FOUO~~) The NC2 program [redacted] Since 2003, approximately [redacted] recommendations related to NC2 have been made. We concentrated on [redacted] previous recommendations that we determined to be the most relevant. 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.

(~~TS//NF~~) The audit revealed that all but [redacted] recommendations have been adequately closed. Key recommendations from 2005 dealing with [redacted] Management concurred with all [redacted] recommendations but did not provide corrective action plans for [redacted]

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

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

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

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

(U) **Audit of Cross Domain Solutions (CDSs)** (23 June 2010)

(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).

(~~S//REL TO USA, FVEY~~) **Finding** Agency CDSs [redacted]

(U//~~FOUO~~) **Recommendation** Improve [redacted] Agency CDS operations [redacted] for all operational CDSs. **UPDATE:** A solution is in development. This recommendation remains OPEN.

(U) **Audit of Mission Assurance Continuity of Operations Compliance and Testing** (17 August 2010)

(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** A small percentage of the [redacted] organizations maintained complete, updated, and operationally tested Continuity of Operations (COOP) plans. [redacted]

(U//~~FOUO~~) **Recommendation** Track organization compliance in developing complete COOP plans and performing annual updates and testing. **UPDATE:** Although only a small percentage of COOP plans have been updated and tracked, this action has been given high priority. This recommendation remains OPEN.

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

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

(U) Ongoing Audits

(U) **NSA/CSS Wireless Networks and Devices**

(U) The audit objective is to assess Agency controls for protecting against unauthorized operation of wireless networks and devices within NSA/CSS and to assess Agency wireless implementation initiatives.

(U) **High-Performance Computing**

(U) The audit objective is to evaluate the contracting process of the High Performance Computing – Special Program Office.

(U) **Information Sharing**

(U) The audit objective is to review Agency effectiveness in sharing cyber threat and vulnerability information with other IC agencies in accordance with the Comprehensive National Cyber Initiative.

(U) **Acquisition Security Process**

(U) The audit objective is to determine whether the acquisition security process effectively and efficiently mitigates the foreign ownership, control, or influence and counterintelligence risks of Agency IT purchases.

(U) **ARCANAPUP Modernization Effort**

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

(U) **General Application Controls for Agency Payroll, Human Resources, and Contracting Systems**

(U) The NSA Comptroller requested that we review the Defense Civilian Payroll System, the Human Resources Management System, and the Contracting Management Information System. The audit objective is to assess the general and application controls of these systems.

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

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

(U//~~FOUO~~) The audit objective is to determine whether the [redacted] user interface meets customer needs and whether its implementation is in compliance with Agency acquisition policies.

(U//~~FOUO~~) **NSA/CSS Compliance with the Federal Information Security Management Act (FISMA)**

(U) In accordance with Office of Management and Budget guidance, we will assess the overall effectiveness of Agency information security policies, procedures, and practices. Our report will be forwarded to the ODNI Inspector General for consolidation and reporting to legislative committees.

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

(U//~~FOUO~~) The audit objective is to determine whether the Directorate of Acquisition complies with Federal Acquisition Regulation requirements for determining price reasonableness and NSA/CSS Policy 8-4, *Competition in Contracting*.

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

(U//~~FOUO~~) The audit objective is to assess the privacy of data collected by [redacted] and validate that Personally Identifiable Information is adequately safeguarded from unauthorized access.

(U) **Export Controls**

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

(U) This page intentionally left blank.

(U) INSPECTIONS

(U) Inspections Completed in the Reporting Period

(U) **Joint Inspection of NSA/CSS Hawaii (NSAH)** (29 April 2011)

(U//~~FOUO~~) This inspection was conducted from 24 January to 4 February 2011. The site is led by a commander who emphasizes integration and collaboration with the Service Cryptologic Component commanders. The workforce is generally positive toward mission, but some are dissatisfied with the watch schedule, ineffective communications across the chain of command, and the overwhelming and conflicting nature of dual responsibilities (i.e., Joint and Service). Site leadership is heavily engaged in the simultaneous transitions of host responsibilities to NSA/CSS and mission to a new building, causing gaps in mission expertise. Lack of a comprehensive financial picture and centralized manpower-tracking tools inhibits efficient use of resources and affects numerous programs that require accurate manpower and resource data.

(U) **Joint Inspection of NSA/CSS**

(U//~~FOUO~~) This inspection was conducted from 2 to 13 May 2011. NSA/CSS and enabling organizations located at the are challenged with a Staffing is adequate to meet responsibilities, although competing priorities at times stretch the staff to their limits. Military/civilian relationships are good, and the enabling organizations are customer focused. The overall climate is positive.

(U//~~FOUO~~) is focused on mission success. However, there are a number of quality-of-life challenges, ranging from facilities conditions to limited work space to distant support services.

(U//~~FOUO~~) has strong leadership that has made positive improvements to morale. The command climate at is strong. There is a clear understanding of the mission, and military/civilian relationships are positive. The Director, although relatively new, has had a positive effect on the site and projects a clear vision of where must go in the future. He has been a catalyst for positive change.

(U) **Expeditionary Operations Review (EOR) of** (28 September 2011)

(U//~~FOUO~~) The EOR Team reviewed mission operations and IO at

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

(~~S//REL TO USA, FVEY~~) The CST and CSGs work closely with their customers and the extended enterprise to anticipate, identify, and satisfy support requirements. Knowledgeable customers understand the contribution of Signals Intelligence (SIGINT) to operations and point to individual and team behaviors when evaluating the success of CSGs or CSTs.

(U//~~FOUO~~) Site mission, functions, tasks, authorities, and differentiation from supported commands' organic SIGINT resources must be documented, and NSA/CSS Washington must provide reporting and sanitization Standard Operating Procedures. NSA/CSS should determine the feasibility of participating in supported element pre-deployment exercises and obtain supported commands' post-deployment feedback.

(U//~~FOUO~~) IO training and database access must be included on the deployment checklist. Officers in Charge need better guidance on how to perform O functions, and guides that detail processes and procedures must be developed.

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

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

(U) **Joint Inspection of** (17 November 2008)

(U) **FINDING: Fire Suppression System Lacking**

(U//~~FOUO~~) Lack of a fire suppression system in seriously degrades the ability to protect life and critical equipment. This deficiency was initially identified during a joint Inspector General inspection and was noted again in an NSA Occupational Health and Environmental Survey. Overall stewardship of facilities is the responsibility of Planning for fire suppression system installation however, no stakeholder agencies committed the needed funding. Although it remained a critical safety deficiency, no further progress was made until the Director, NSA emphasized the need to complete the action. contracted for system design, followed by a phased installation using consolidated cryptologic program funding. A projected completion date of remains tentative because of and possible delays in getting supplies needed to complete the installation. **UPDATE:** The projected completion date is still Disruption of supplies was minimal, and the contractor made changes to the work schedule to compensate for delays.

(U) **Multiple Joint Inspections from FY2005 to FY2010 Regarding USSID CR1200**

(~~C//REL TO USA, FVEY~~) USSID CR1200, *Concept of SIGINT Support to Military Commanders*, provides policy and guidance on SIGINT support to military commanders and operations. Published in 1998, this United States Signals Intelligence Directive (USSID) is severely outdated, contains obsolete functions and terminology not used in current military doctrine, provides no Higher Headquarters template for present-day Military Operations Integration, and does not establish standards for expeditionary SIGINT support for ongoing military operations. This significant deficiency was noted as a finding in inspection reports encompassing Global Cryptologic Enterprise Sites beginning in FY2005 and continuing to the present. An NSA/CSS action element is leading a working group with stakeholder participation to draft a new USSID as recommended in this inspection report. The action element determined that other supporting policy documents must first be updated; there is no estimated

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

completion date for this critical document. **UPDATE:** SID is developing a plan but intends to cancel this USSID. This recommendation remains OPEN.

(U) Ongoing Inspections

(U//~~FOUO~~) **Joint Inspection of**

(U//~~FOUO~~)

(U) **Joint Inspection of**

(U//~~FOUO~~) The NSA/CSS Office of Inspections conducted a Joint Inspection of The final report is in coordination.

(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

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

(~~TS//SI//NF~~) **NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Pen Register and Trap and Trace (PR/TT) Devices** (15 April 2011)

(~~TS//SI//NF~~) This review was conducted to determine whether the controls tested as part of a 2010 year-long review of NSA compliance with seven provisions of the Business Records (BR) Order were adequate to provide reasonable assurance of compliance with similar provisions of the PR/TT Order. Of the [redacted] queries made between [redacted] the date when the FISC signed PR/TT [redacted] and [redacted] no errors or instances of non-compliance were found with the five provisions of the PR/TT Order related to querying that were tested. These controls therefore were judged to be adequate to provide reasonable assurance of compliance with the Order. Although we intended to test NSA compliance with two additional provisions related to dissemination, we were not able to because NSA did not issue serialized SIGINT reports that contained PR/TT-derived [redacted] during the test period.

(~~TS//SI//NF~~) **NSA Controls to Comply with the FISC Order Regarding Business Records** (25 May 2011)

(~~TS//SI//NF~~) This report summarizes the results of our audit of NSA controls to comply with the FISC BR Order. From January through December 2010, we conducted monthly tests of NSA compliance with seven provisions of the BR Order to determine whether controls were in place and operating as intended. Querying controls were adequate to provide reasonable assurance of compliance with the five provisions of the Order we tested. Manual controls over the dissemination of serialized SIGINT reports and the compilation of the Weekly Dissemination Report were inherently risky but manageable. The manual dissemination controls will be increasingly difficult to manage if the amount of information disseminated outside NSA increases.

(U) **Review of Attrition of** [redacted] (26 May 2011)

(U//~~FOUO~~) The Director, NSA requested that the OIG review factors influencing recent attrition of [redacted] Between February and March 2011, the [redacted] resigned in lieu of termination on [redacted] The [redacted] were considered important to [redacted] mission because it takes [redacted] to train a replacement capable of performing at the level of those who have left. However, the overall mission impact of the departed [redacted] was considered minimal and under control. To mitigate future loss of these [redacted] the [redacted] with Human Resources assistance, is considering awarding retention bonuses to ensure that the Agency receives a return on its investment.

(b)(6)

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

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

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

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

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

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

(U//~~FOUO~~) **Non-Traditional Dissemination Methods: Dissemination Strategy Evaluation** (28 September 2011)

(U//~~FOUO~~) Various non-traditional dissemination methods have been implemented to address the challenges and opportunities presented by a Presidential call for increased information sharing. The review, which focused on select processes and tools that analysts use for non-traditional dissemination, revealed that SID does not have a comprehensive dissemination plan.

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

(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 with Third-Party partners.

(U//~~FOUO~~) **Finding** Documentation for disseminated to Third Party partners is not centrally maintained, retrievable, or current.

(U//~~FOUO~~) **Recommendation** The Foreign Affairs Directorate (FAD) should establish a repository for documentation of shared with Third-Party partners and add this as a Director of Foreign Affairs responsibility in NSA/CSS Policy 10-1. **UPDATE:** FAD has established a repository but has not updated documentation. FAD has been asked to update NSA/CSS Policy 1-10 with the statement that the Foreign Affairs Director shall maintain a central repository, on its database system for Third-Party information.

(~~C//REL TO USA, FVEY~~) **Finding** SID's dissemination of to Third-Party partners lacks adequate controls.

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

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

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

(~~S//NF~~) **Recommendation** Establish a standard process for handling all [redacted] **UPDATE:** SID has developed a process but has not formally approved or communicated it to the workforce.

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

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

(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] field sites, clearly defining the division of effort, prioritization, measures of success, and roles and responsibilities of personnel. **UPDATE:** [redacted] is making slow progress.

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

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

(U//~~FOUO~~) **Recommendation** Designate an [redacted] IO Officer 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. **UPDATE:** [redacted] is making slow progress.

(U) Ongoing Special Studies

(U//~~FOUO~~) **Management Controls to Implement the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008**

(U//~~FOUO~~) The objective of this study is to determine whether NSA controls are adequate to provide reasonable assurance that NSA complies with the terms of the FISA Amendments Act.

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

(U//~~FOUO~~) The objective of this study is to evaluate [redacted] FISA operations for compliance with national and NSA policies and procedures.

(~~TS//SI//NF~~) **NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Retention**

(~~TS//SI//NF~~) The objective of this study is to determine whether NSA controls are adequate to provide reasonable assurance that NSA complies with the terms of the FISC Order for BR retention.

(U) [redacted]

(~~S//SI//REL TO USA, FVEY~~) The objective of this study is to review recent [redacted]

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

(U) This page intentionally left blank.

(U) INVESTIGATIONS

(U) Summary of Prosecutions

(U) Indictment

(U) In May 2011, a federal grand jury indicted three family members for conspiracy to commit wire fraud arising from a fraudulent billing scheme on an NSA contract. The defendants, all former officials of an Agency contractor, are alleged to have instructed employees to inflate the number of hours spent working on NSA contracts and, in some cases, to claim time spent working on NSA contracts when in fact they had not been. The indictment seeks forfeiture of $1,455,174, believed to be the amount of payments fraudulently received from NSA.

(U) Sentencing

(U) In June 2011, a former Agency employee was sentenced to 18 months in prison followed by three years of supervised release for conspiring to obtain payments in return for taking actions as an NSA official and for making false statements to conceal the illegal payments from the Agency. The former employee was also ordered to serve six months of the supervised release in home detention with electronic monitoring and to perform 100 hours of community service and pay a $15,000 fine and $4,929.90 in restitution within 60 days. In the same case, two officials in a private company, who had made the improper payments, were also sentenced: one to one year and one day incarceration and three years of supervised release and the other to six months in prison followed by one year of supervised release. The company was also ordered to pay a fine of $130,000 and restitution of $104,989.84 (which has been paid in full).

(U) In September 2011, a former NSA contractor employee was sentenced to five years of probation, ten months of which is to be served in home detention with electronic monitoring, for making false statements in connection with labor hours claimed on an NSA contract. The former contractor employee was also required to pay restitution of $108,780.46, which represents payment for 836 labor hours not actually performed.

(U) Referrals

(U) The U.S. Attorney's Office in Baltimore, Maryland, is considering a contract labor mischarging case. The dollar amount is approximately $49,000, representing approximately 677 falsely claimed labor hours.

(U) OIG Hotline Activity

(U) The division fielded 571 contacts from the OIG Hotline. The team opened 53 investigations and closed 46 in the reporting period.

(U) This page intentionally left blank.

(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, 8-9, 12-13
§5(a)(4)	Matters referred to prosecutive authorities	15
§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) This page intentionally left blank.

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

(U) Audits

(U) **Information Technology**

- (U) Agency Controls for [redacted] IT Hardware Purchases
- (U) Nuclear Command and Control

(U) **Federal Compliance**

- NSA/CSS Compliance with the Federal Information Security Management Act (FISMA)

(U) **Operations**

- (U) NSA Police Operations

(U) Inspections

(U) **Joint Inspections**

- (U) NSA/CSS Hawaii
- (U) NSA/CSS Europe, [redacted]

(U) **Operations**

- (U) Expeditionary Operations Review of [redacted]

(U) Special Studies

(U) **Operations**

- (U) Review of Attrition of [redacted]
- (~~TS//SI//REL TO USA, FVEY~~) [redacted]
- (~~TS//SI//REL TO USA, FVEY~~) [redacted]

(U) **Intelligence Oversight**

- (~~TS//SI//NF~~) NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Pen Register and Trap and Trace Devices
- (~~TS//SI//NF~~) NSA Controls to Comply with the FISC Order Regarding Business Records

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

(U//~~FOUO~~)

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

(U) This page intentionally left blank.

(U) APPENDIX B:
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) 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)

(U) This page intentionally left blank.

(U) APPENDIX C: 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	1	$491,400 over 5-yr defense plan
For which management decision was made during reporting period	1	$491,400 over 5-yr defense plan
Value of recommendations agreed to by management	1	$466,602 over 5-yr defense plan
Value of recommendations not agreed to by management	1	$24,798 over 5-yr defense plan
For which no management decision was made by end of reporting period	0	0
(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.		

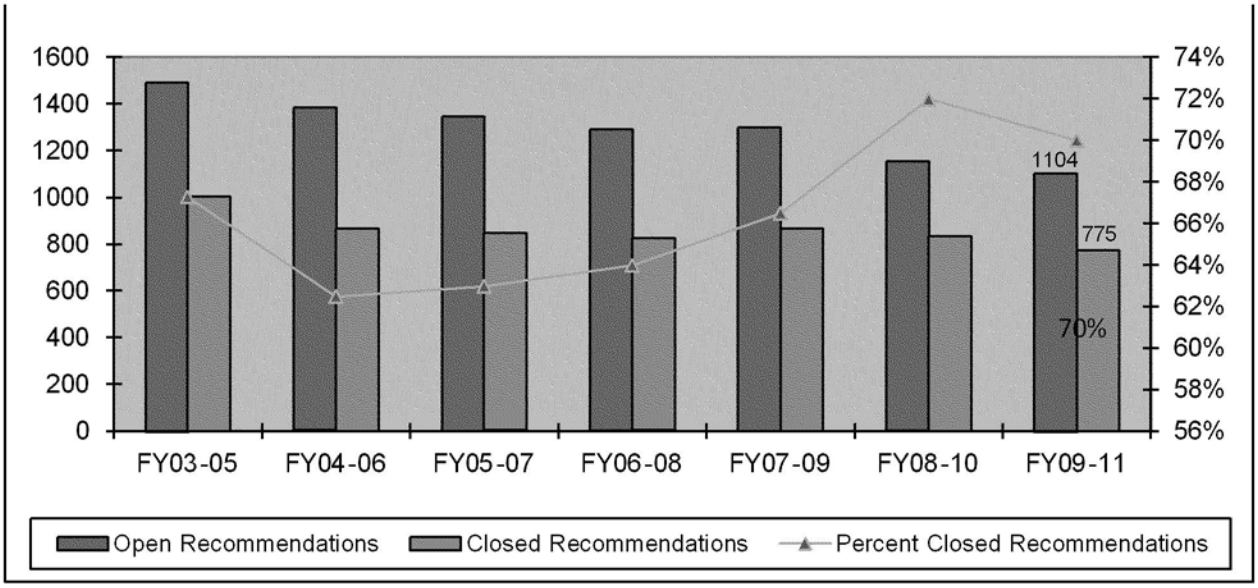
(U)

(U) This page intentionally left blank.

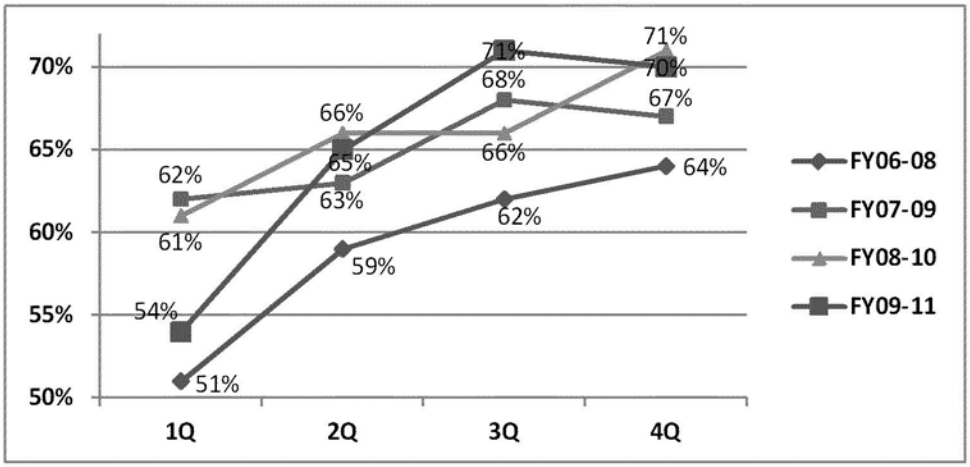
(U) APPENDIX D: RECOMMENDATIONS SUMMARY

(U//~~FOUO~~) The OIG made 213 new recommendations to NSA management in reports issued in the third and fourth quarters of FY2011: 99 in the third and 114 in the fourth. During the third and fourth quarters, the Agency implemented 84 and 71 recommendations, respectively. Figures 1 and 2 depict long-term progress in implementing OIG recommendations. We monitor recommendation completion on a rolling three-year average.

(U) Figure 1. Agency Implementation of OIG Recommendations



(U) Figure 2. Implementation Rate Comparison



(U) Percentages depict progress in implementing recommendations during a three-year period by quarter. Progress in the fourth quarter during the current three-year period is consistent with historical norms.

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

(U) Highlights

(U//~~FOUO~~) Managers fully implemented recommendations made in the following reports by the end of the fourth quarter:

- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) Package Screening for Chemical & Biological Agents (31 March 2006)
- (U//~~FOUO~~) NSA's Computer Security Incident Response Process (26 September 2006)
- (U) SPL Mask-Making and Wafer Fabrication Closeout (23 June 2008)
- (U) Agency System Security Plans (8 September 2008)
- (U) FMS FACTS (31 December 2008)
- (U) NSA/CSS Threat Operations Center (31 March 2009)
- (U) NSA/CSS Commercial Solutions Center (28 August 2009)
- (~~S//REL TO USA, FVEY~~) [redacted]
- (U) Foreign Language Incentive Program (13 May 2009)
- (~~TS//REL TO USA, FVEY~~) [redacted] (25 September 2009)
- (~~TS//REL TO USA, FVEY~~) [redacted] (25 September 2009)
- (U) Follow-up Audit of Contractor Space (30 September 2009)

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