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

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

(U) SEMI-ANNUAL REPORT TO CONGRESS
1 October 2010 to 31 March 2011

Derived from: NSA/CSSM 1-52
Dated: 20070108
Declassify on: ~~20320108~~

~~TOP 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 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 at management's request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with assessments 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 October 2010 and 31 March 2011. The report is mandated by the Intelligence Authorization Act of 2010.

(U) During the reporting period, the NSA OIG completed 28 audits, inspections, special studies, and investigations.

(U) The Audits Division completed nine audits ranging from federal compliance to Information Technology to financial management and operations. The OIG rarely issues reports without a management decision and on only a few occasions does the OIG encounter non-concurrence with its recommendations. In this reporting period, however, the Audit Report of NSA/CSS Enterprise Solution and Baseline Exception Request Processes contained one non-concurrence. The Director has resolved this situation.

(U) The Inspections Division completed reports on a field inspection of Cryptologic Services Group –Marine Corps Intelligence Agency and joint inspections of Menwith Hill Station and NSA activities at the U.S. Central Command.

(U//~~FOUO~~) The OIG completed special studies on SIGINT Support [redacted] and Foreign Intelligence Surveillance Court Rule 13(a) and 13(b) filings.

(U) The Investigations Division fielded 477 contacts from the OIG Hotline. The team opened 20 investigations and closed 11 in the reporting period.

(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 274 recommendations issued in the reporting period, 70 have been closed.

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

George Ellard
Inspector General

(U) 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) This page intentionally left blank.

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

(U) AUDITS

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

(U) Completed Audits

(U//~~FOUO~~) **Audit of Data Sharing with Third-Party Partners** (20 September 2010) (published in previous quarter but not listed in the quarterly report, which was submitted early)

(~~TS//SI//NF~~) In 2009, NSA sent more than [redacted] messages to Third Party partners [redacted] Completion of recommended actions will reduce the risk associated with disseminating [redacted] to Third Parties.

(U) **Audit of Educational Assistance and Recruitment Programs** (18 November 2010)

(U//~~FOUO~~) NSA/CSS spends approximately [redacted] a year on incentives to meet its skill needs, including scholarship awards to students majoring in critical fields, tuition assistance to employees taking college courses, bonus compensation to employees relocating to field sites, and recruitment bonuses to employees who staff hard-to-fill positions. The audit found that standard processes for overseeing scholarship programs are lacking. The Agency has initiated action to recoup approximately $1 million in tuition payments from employees whose grades did not meet eligibility requirements for tuition assistance.

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

(U) **Audit of the FISA Amendments Act §702 Detasking Requirements** (24 November 2010)

(~~S//REL TO USA, FVEY~~) Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (FAA) has strengthened SIGINT collection, particularly against terrorist targets. From September 2008 to March 2010, the number of SIGINT reports that incorporated FAA §702 sourced collection grew from fewer than [redacted] to more than [redacted] and the percentage of counterterrorism reporting with a contribution from FAA §702 collection rose steadily from [redacted] to [redacted] percent.

(~~TS//SI//NF~~) However, collection under FAA §702 must cease under certain circumstances to remain lawful, potentially resulting in gaps in coverage. To regain coverage, NSA must transition to another authority, [redacted] for continued collection. [redacted]

(U//~~FOUO~~) **Audit of the Nuclear Weapons Personnel Reliability Program** (28 December 2010)

(U//~~FOUO~~) The purpose of the Nuclear Weapons Personnel Reliability Program (NWPRP) is to ensure that all NSA/CSS personnel who perform nuclear weapons-related duties meet the highest standards of reliability, including physical, psychological, and technical competence. The audit concluded that NWPRP provides reasonable assurance that only the most reliable individuals perform duties associated with nuclear weapons. The audit did identify a problem in drug-testing methodology. Agency managers agreed to fix the problem.

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

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

(~~TS//SI//NF~~) **Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – December 2010** (monthly test reports from August through December 2010)

(~~TS//SI//NF~~) This report summarizes results of tests of controls for December to ensure NSA's compliance with seven requirements of the Foreign Intelligence Surveillance Court Order Regarding Business Records (BR). The monthly tests were conducted throughout 2010 as part of the continuous auditing methodology and to meet OIG oversight requirements of the BR Order. The report found that NSA controls over querying were adequate to provide reasonable assurance of compliance with the five provisions of the Order that were tested. The report also found that although manual controls over the dissemination of serialized Signals Intelligence reports and the compilation of the Weekly Dissemination Reports are inherently risky, they are acceptable given the amount of information disseminated [ ] reports during 2010).

(U) **Audit of Firewall Management for CES and** [ ] (28 January 2011)

(~~C//REL TO USA, FVEY~~) We reviewed [ ] organizations that operate and maintain firewalls that protect the Cryptanalysis and Exploitation Service (CES) and [ ] and found [ ]

Technology Directorate and Signals Intelligence Directorate have concurred with our recommendations to improve the management of CES and [ ] firewalls.

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

(U) **Audit of Market Research and Competition** (31 January 2011)

(U//~~FOUO~~) Market research and competition are essential to fair pricing. The objective of this audit was to determine whether the Agency is adequately seeking competition in contracting and whether adequate market research is being conducted and documented. The audit found that the Acquisition Resource Center is an effective tool, but staffing levels need review; competition statistics are inaccurate because of coding errors; definition of competition needs revision; and market research documentation needs improvement. Management is addressing the recommendations.

(U) **Oversight Review of the Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop** (18 March 2011)

(U) This report summarizes the results of our oversight review of the audit of the Restaurant Fund (RF), the Civilian Welfare Fund (CWF), and the Cryptologic Museum Gift Shop for FY2010 by a Certified Public Accountant firm. The objective was to ensure that the audit of the RF, CWF, and Cryptologic Museum Shop was consistent with Government Auditing Standards. We concluded that it was, and the CPA firm did not identify management concerns.

(U) **Audit of the Power, Space, and Cooling Triage Process for the Extended Enterprise** (25 March 2011)

(U//~~FOUO~~) The Power, Space, and Cooling Triage process is operating as intended. The [ ] extended enterprise sites that participate in the process have improved management of their power requirements. However, one significant problem is the inability of participating sites to measure power usage consistently because of a lack of standardized capability to monitor power.

(U) **Audit of NSA/CSS Enterprise Solution and Baseline Exception Request Processes** (31 March 2011)

(U~~//FOUO~~) The Technology Directorate established the National Security Agency/Central Security Service Enterprise Solution (NES) and Baseline Exception Request (BER) processes to reduce Information Technology (IT) complexity, improve interoperability and security, and manage IT costs. Our review found that Agency organizations and contractors [redacted] Without functioning controls to ensure compliance, the Agency and its Chief Information Officer (CIO) will be unable to manage effectively IT items purchased and installed by Agency organizations and its contractors. Management concurred with all but one recommendation.

(U) Audits of Particular Significance

(U) **Audit Report of NSA/CSS Enterprise Solution and Baseline Exception Request Processes** (31 March 2011)

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

(U) **QUESTIONED COSTS**

(U~~//FOUO~~) This audit uncovered [redacted] worth of IT purchases that Agency organizations and contractors acquired under a fictitious BER approval number. Management will review a representative sample of these requisitions to determine whether the questioned costs were in compliance with the NES Baseline and take the appropriate action if the item purchased was not compliant. If the sample shows significant rates of non-compliance, the review will be extended to all requisitions under the fictitious number. In the meantime, new control processes have been implemented to prohibit future use of fictitious approval numbers. The processes involve Enterprise Information Technology, Directorate of Resources Management, and Directorate of Acquisition. This review will also provide insight on how to strengthen the controls being designed in response to other OIG recommendations made in this report.

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

(U) **Audit of Operational Test Authority** (12 May 2010)

(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 1** The OIG recommended establishing an independent OTA with direct reporting authority to the NSA Director. **UPDATE:** This recommendation is now CLOSED.

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

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

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

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

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

(U//~~FOUO~~) **Recommendation 1** The OIG recommended improving [redacted] Agency CDS [redacted] for all operational CDSs.

(~~S//NF~~) **Finding** The Agency [redacted]

(U//~~FOUO~~) **Recommendation 5** The OIG recommended developing a standard operating procedure (SOP) to document approved [redacted] This SOP should require that changes be logged and controlled in an approved central repository. **UPDATE:** This recommendation is now CLOSED.

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

(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** [redacted]

(U//~~FOUO~~) **Recommendation 1** The OIG recommended that the Agency track organization compliance in developing complete COOP plans and performing annual updates and testing.

(U) Ongoing Audits

(U) **Audit of NSA Police Operations**

(U//~~FOUO~~) The audit objective is to evaluate the effectiveness and efficiency of the National Security Agency Police (NSAP) at NSA/CSS Washington (NSAW), specifically to determine whether NSAP is adequately equipped, staffed, and trained to protect and defend NSAW personnel and property.

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

(U//~~FOUO~~) The audit objective is to determine whether the Agency's internal controls effectively reduce the risk for [redacted] Technology purchases.

(U) **Audit of NSA/CSS's 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 spaces and to assess Agency wireless implementation initiatives.

(U) **Audit of High-Performance Computing**

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

(U) **Audit of Information Sharing**

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

(U) **Audit of the 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 risk of the Agency's information technology purchases.

(U) **Audit of the ARCANAPUP Modernization Effort**

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

(U) **Audit of Nuclear Command and Control (NC2) Program**

(U) The audit objective is to determine whether NSA implemented corrective actions to satisfy recommendations made in previous audits and reviews of the NC2 process.

(U) **Audit of NSA's Compliance with National Security Directive 42 to Support Non-DoD Agencies for Network Intrusions**

(U) The audit objective is to determine whether the Information Assurance Directorate is effectively fulfilling the Agency's responsibilities for network intrusion support to non-DoD agencies in accordance with National Security Directive 42, *National Policy for the Security of National Security Telecommunication and Information Systems*, 5 July 1990.

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

(U) The audit objective is to assess the general and application controls of the Agency's payroll, human resources, and contractor systems. Specifically, the NSA Comptroller has requested that we review the Defense Civilian Payroll System, the Human Resources Management System, and the Contracting Management Information System.

(U) This page intentionally left blank.

(U) INSPECTIONS

(U) Completed Inspections

(U) **Joint Inspection of Alaska Mission Operations Center** (8 October 2010)

(U//~~FOUO~~) The Alaska Mission Operations Center (AMOC) has made significant progress since its first Joint IG inspection in 2006. Site leadership is actively engaged in mission and working diligently to shift the culture from an Air Force-focused site to an NSA/CSS site. Site leadership is trying to balance mission needs and resources based on inadequate guidance and documentation from NSA/CSS. The site uses mission personnel to supplement necessary enabling functions resulting from increased mission growth and an increase in NSA/CSS civilian personnel. An appropriate skill mix is hard to determine because much of the mission is not formally documented. The future for AMOC includes new mission sets, more customer engagement, and aggressive partnership development, all of which could place additional burdens on an already stretched workforce.

(U) **Field Inspection of Cryptologic Services Group–Marine Corps Intelligence Agency** (1 December 2010)

(U//~~FOUO~~) The field inspection of the Cryptologic Services Group (CSG)–Marine Corps Intelligence Agency (MCIA) found a number of serious problems with the organization's readiness to accomplish its assigned mission. Although manning numbers are sufficient, the majority of personnel CSG training, intelligence oversight, and mission guidance to junior personnel were not sufficient. We also found that Recommendations have been formally tasked for action.

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

(U) **Joint Inspection of Menwith Hill Station** (14 December 2010)

(~~C//REL TO USA, FVEY~~) Mission accomplishment at Menwith Hill Station is successful. However, NSA/CSS and other agency mission sponsors must provide guidance to the site on mission prioritization. The lack of agreement on cost-sharing Memoranda of Understanding and remains of significant concern; however, significant progress has been made toward resolving both findings since the inspection. Continued and repeated delays in military construction funding for family housing projects affect quality of life for assigned personnel. Recommendations have been formally tasked for action.

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

(U) **Joint Inspection of NSA Activities at U.S. Central Command** (4 March 2011)

(U//~~FOUO~~) Leadership has built a positive, mission-oriented workforce. In almost every area, however, inspectors found processes that were successful yet undocumented. Lack of formal guidance makes it difficult at times for NSA/CSS Representative to Central Command (NCRCENT) personnel to support NSA interests effectively. Implementation of field governance is applied inconsistently across the [redacted] Furthermore, NSA Headquarters' over-reliance on Staff Processing Forms makes it difficult to operate in a fast-paced operational environment. [redacted] Lack of promotion opportunities, as a result of civilian promotion caps, [redacted] Recommendations have been formally tasked for action.

(U) Inspections of Particular Significance

(U) **Joint Inspection of Menwith Hill Station** (14 December 2010) (b)(3)-P.L. 86-36

(U) **REFERRAL: Problems with DoDEA School Administration**

(U//~~FOUO~~) Although not within the scope of an Intelligence Community inspection, the Menwith Hill Station (MHS) Joint Inspection Team identified, documented, and addressed widespread, longstanding discontent with perceived lack of professionalism by the on-base Department of Defense Education Activity (DoDEA) School administrators and teachers. The situation adversely affects the station's quality of life and mission operations. A Joint Inspector General (IG) town hall meeting was conducted to gain a better understanding of the scope of school-related issues. The meeting was attended by approximately [redacted] parents, many of whom were extremely frustrated by their inability to resolve issues despite numerous visits and telephone calls to the school. The IG's concern about degradation of mission operations and MHS quality of life drove our decision to include this in our report. The 2007 MHS Joint IG Inspection also documented concerns with effective administration, management, and discipline in the MHS DoDEA School. The Joint Inspection Team findings were formally referred to the DoD IG as a matter under its purview. Updates from the site indicate that the referral resulted in increased scrutiny from the DoDEA regional administration and that the local school administration has begun to make positive changes.

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

(U) **Joint Inspection of** [redacted] (17 November 2008)

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

(U//~~FOUO~~) Lack of a fire suppression system in [redacted] seriously degrades the ability to protect life and critical equipment. This deficiency was initially identified during a 1997 Joint Inspector General inspection and was again noted in an NSA Occupational Health and Environmental Survey conducted in 2000. Overall stewardship of [redacted] facilities is the responsibility of [redacted] Planning for fire suppression system installation began in May 2001; however, no stakeholder agencies committed the needed funding. Although it remained a critical safety deficiency, no further progress was made until September 2009, when the Director, NSA emphasized the need to complete the action. [redacted] contracted for system

design, followed by a phased installation in 2010 using consolidated cryptologic program funding. The installation is now 37% complete. A projected completion date of November 2011 remains tentative because of [redacted] and possible delays in getting supplies needed to complete the installation.

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

(~~C//REL TO USA, FVEY~~) *Concept of SIGINT Support to Military Commanders* provides policy and guidance on Signals Intelligence (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 [redacted] Global Cryptologic Enterprise Sites beginning in FY2005 (Reference Findings: [redacted] 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 completion date for this critical document.

(U) **Joint Inspection of NSA/CSS Georgia** (30 June 2010)

(U//~~FOUO~~) **Finding** Substantial growth in NSA/CSS Georgia's (NSAG) 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 FG-10-2036** NSA Headquarters and NSAG should define, program for, and provide the minimum mission enabler personnel and funds needed to operate the Center effectively. **UPDATE:** This recommendation is now CLOSED.

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

[redacted]

(U//~~FOUO~~) **Recommendation FG-10-2001** 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. **UPDATE**: This recommendation is now CLOSED.

(U) Ongoing Inspections

(U) Joint Inspection of NSA/CSS Hawaii

(U//~~FOUO~~) The NSA/CSS Office of Inspections conducted a Joint Inspection of NSA/CSS Hawaii between 24 January and 4 February 2011. The final report is in coordination.

(U) Expeditionary Operations Review of

(U//~~FOUO~~) The Inspections Team conducted a review of NSA activities from The draft report is in coordination.

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

(U) SPECIAL STUDIES

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

(U) Completed Special Studies

(U) **Special Study of SIGINT Support to** (10 February 2011)

~~(TS//SI//NF)~~ The objective of this special study was to assess procedures and controls used to provide Signals Intelligence (SIGINT) support The study focused on support to We reviewed mission management, analytic techniques, and SIGINT dissemination. With few exceptions, NSA/CSS support was effective, and SIGINT reporting complied with Agency directives. However, NSA/CSS has not established a common definition, qualification or proficiency standards, or formal training for operational support policy should be improved, CT operational security should be reviewed, and the role of the CT Mission Management Center should be clearly delineated; and reporting guidance is ambiguous, does not effectively address and has inconsistent reporting standards. The corrective actions planned by management meet the intent of the recommendations.

(U//~~FOUO~~) **Review of Foreign Intelligence Surveillance Court (FISC) Rule 13(a) and 13(b) Filings** (22 March 2011)

(U//~~FOUO~~) FISC Rule 13(a) requires the government to immediately correct misstatements or omissions of material facts in submissions to the FISC. Rule 13(b) requires the government to immediately inform the FISC of incidents outside the scope of the Court's authorization. The NSA Office of General Counsel (OGC) coordinates the filing of notices with the US Department of Justice, the final author of 13(a) and 13(b) notices. The OIG reviewed 13(a) and 13(b) filings from September 2009 through November 2010 for timeliness and accuracy. In that period, no FISC notices were amended because of material misstatements within the initial FISC incident reports. However, we observed that OGC does not maintain a central repository or tracking system for 13(a) and 13(b) filings. During our review, the Signals Intelligence Directorate and OGC adopted a process to address timeliness concerns. We will consider conducting another review when that process matures.

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

(U) Special Studies of Particular Significance

(U) **Special Study of SIGINT Support to** 10 February 2011)

~~(TS//SI//NF)~~ NSA/CSS in support of counter-terrorism (CT) missions, This information can be combined with However, NSA CT organizations do not share a common definition of what constitutes contributing to inconsistent practices and affecting mission performance.

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

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

(U) Review of 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 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]

(U//~~FOUO~~) **Finding** 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.

(U//~~FOUO~~) **Recommendation 1a** FAD should establish a repository for documenting [redacted] shared with third-party partners, and it should update existing documentation. **UPDATE:** FAD has established a repository but has not updated documentation.

~~(C//REL TO USA, FVEY)~~ **Finding** Although SID's Analysis and Production Directorate (S2) developed a process in February 2007 to sample [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 sample [redacted] disseminated to partners is unclear, and, as a result, [redacted] is inconsistent.

(U//~~FOUO~~) **Recommendation 2a** SID should revise its oversight process for disseminating [redacted] to partners, including sampling 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.

(U//~~FOUO~~) **Finding** SID lacks a standard process for [redacted]

(U//~~FOUO~~) **Recommendation 2b and 2c** SID should establish a standard process [redacted]

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

(U//~~FOUO~~) **Special Study of** [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 mission documentation and standards for NSA Headquarters and the Extended Enterprise.

~~(C//REL TO USA, FVEY)~~ **Recommendation 1b** [redacted] should develop a Mission and Functions Statement, Strategic Plan, and implementing instructions, reflecting the evolving mission of [redacted]

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

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

[redacted] external agencies. The documents should clearly define internal management controls in standard operating procedures, system configuration management, and budget documentation.

(U//~~FOUO~~) **Finding** [redacted] has no Intelligence Oversight program.

(U//~~FOUO~~) **Recommendation 9a.** The [redacted] should establish an Intelligence Oversight program in accordance with Department of Defense regulations and NSA policies.

(U) Ongoing Special Studies

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

(~~TS//SI//NF~~) The objective of this study is to determine whether controls to ensure NSA compliance with the key terms of the Foreign Intelligence Surveillance Court Order regarding business records are operating as intended.

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

(U//~~FOUO~~) **Special Study on Non-traditional Dissemination Methods**

(U//~~FOUO~~) The objective of this study is to evaluate the use of non-traditional dissemination methods for compliance with policies and procedures.

(~~TS//SI//NF~~) **Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Pen Register and Trap and Trace Devices**

(~~TS//SI//NF~~) The audit objective is to determine whether the controls tested as part of a 2010 yearlong review of NSA compliance with seven provisions of the Business Records Order were adequate to provide reasonable assurance of compliance with similar provisions of the Pen Register and Trap and Trace Order.

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

(U//~~FOUO~~) **Special Study of Computer Network Exploitation** [redacted]

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

(~~TS//SI//NF~~) **Audit of 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 Foreign Intelligence Surveillance Court Order for business records retention.

(U) This page intentionally left blank.

(U) INVESTIGATIONS

(U) Summary of Prosecutions

(U) **Convictions**

- (U) An Agency employee pled guilty in December 2010 to accepting more than $110,000 in bribes from a contractor as part of a scheme to defraud NSA. Sentencing is scheduled for June 2011 in the U.S. District Court in Baltimore, MD.

- (U) A contractor pled guilty in December 2010 to making unlawful payments to a government official as part of a scheme to defraud NSA. On 12 April 2011, the contractor was sentenced in the U.S. District Court in Baltimore, MD, to one year and one day incarceration and three years of supervised release, the first six months of which will be served in home detention.

- (U) A contractor pled guilty in December 2010 to making unlawful payments to a government official as part of a scheme to defraud NSA. Sentencing is scheduled for June 2011 in the U.S. District Court in Baltimore, MD.

(U) Referrals

(U) Three contract labor mischarging investigations are being considered for prosecution. The potential dollar loss exceeds $90,000.

(U) OIG Hotline Action

(U//~~FOUO~~) As the result of an OIG hotline complaint from a member of the public (via unclassified Internet website), an Internet service provider was asked to remove the NSA logo from the profile of a blogger, who was not affiliated with NSA. The Internet service provider complied in March 2011.

(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	3, 8, 11
§5(a)(2)	Recommendations for corrective action	3, 8, 11
§5(a)(3)	Previously reported significant recommendations not yet completed	3-4, 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	19-20
§5(a)(7)	Summary of significant reports	3, 8, 11
§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

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

(U) Audits

(U) **Financial Management**

- (U) Audit of Educational Assistance and Recruitment Programs

(U) **Federal Compliance**

- (U) Audit on the FISA Amendments Act §702 Detasking Requirements
- (~~TS//SI//NF~~) Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – December 2010

(U) **Information Technology**

- (U) Audit of Firewall Management for CES and [redacted] (b)(3)-P.L. 86-36
- (U) Audit Report of NSA/CSS Enterprise Solution and Baseline Exception Request Processes

(U) **Operations**

- (U//~~FOUO~~) Audit of the Nuclear Weapons Personnel Reliability Program

(U) **Business Practices**

- (U) Audit of Market Research and Competition
- (U) Audit of the Power, Space, and Cooling Triage Process for the Extended Enterprise

(U) Inspections

(U) **Joint Inspections**

- (U) Joint Inspection of Alaska Mission Operations Center
- (U) Joint Inspection of Menwith Hill Station
- (U//~~FOUO~~) Joint Inspection of U.S. Central Command

(U) **Field Inspections**

- (U) Field Inspection of Cryptologic Services Group–Marine Corps Intelligence Agency

(U) Special Studies

(U) **Operations**

- (U//~~FOUO~~) Special Study of SIGINT Support to [redacted] (b)(3)-P.L. 86-36

(U) **Federal Compliance**

- (U//~~FOUO~~) Review of Foreign Intelligence Surveillance Court (FISC) Rule 13(a) and 13(b) Filings

(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	2	$49,820,000	$920,000
For which management decision was made during reporting period	2	$49,820,000	$920,000
Costs disallowed	1	$920,000	$920,000
Costs not disallowed	0	0	0
For which no management decision was made by end of reporting period	1	$48,900,000	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

(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) 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.