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

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

(U) SEMI-ANNUAL REPORT TO CONGRESS
1 April to 30 September 2014

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

Classified By:
Derived From:
NSA/CSSM 1-52 dtd 20130930,
CNCI SCG dtd 20140515,
INRO CG dtd 20120227,
Declassify On: ~~20391031~~

(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 Intelligence Community 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 2014. The report is mandated by the Inspector General Act of 1978.

(U) During the reporting period, the NSA OIG completed 18 audits, inspections, and special studies.

(U) The Audits Division completed 12 audits spanning operations, information technology, and finance.

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

(U) The Intelligence Oversight Division completed three special studies of operations and information technology.

(U) The Investigations Division fielded 557 contacts from the OIG Hotline. The team opened 56 investigations and closed 60 in the reporting period.

(U) Each report and special study contained recommendations designed to improve the efficiency and effectiveness of the programs under review. Management agreed with these recommendations. The OIG tracks recommendations until they have been implemented and regularly reports to the NSA Director on the status of open recommendations. Of the 282 recommendations issued in the reporting period, 97 have been closed.

George Ellard

DR. GEORGE ELLARD
Inspector General

(U) DISTRIBUTION:

DIR
DDIR
ExDIR
CoS
SID DIR
DL SIDIGLIAISON
IAD DIR
TD DIR
LAO DIR
OGC DIR
ODOC DIR
FAD DIR
BMI DIR
SAE
IC 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)	Significant outstanding recommendations	6-9, 13-14
§5(a)(4)	Matters referred to prosecutorial authorities	15
§5(a)(5)	Information or assistance refused	N/A
§5(a)(6)	List of audit, inspection, and evaluation reports	17-18
§5(a)(7)	Summary of significant reports	N/A
§5(a)(8)	Audit reports with questioned costs	20
§5(a)(9)	Audit reports with funds that could be put to better use	21
§5(a)(10)	Summary of reports for which no management decision was made	N/A
§5(a)(11)	Significant revised management decisions	2
§5(a)(12)	Management decision disagreements	N/A

(U)

(U) SIGNIFICANT PROBLEMS, ABUSES, AND DEFICIENCIES

(U) Recommendations for Corrective Action

(U) Office of the Inspector General (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, but the following two audits yielded significant recommendations.

I. (U) Contractor Qualifications

(U//~~FOUO~~) The audit focused on whether the qualifications of contractor personnel met labor category requirements and whether companies billed correct labor categories and rates.

(U//~~FOUO~~) We determined that contracting officer representatives (CORs) were not consistent in their review of contractor qualifications. CORs did not always review résumés to validate that personnel met qualifications outlined in contracts. Of the 84 CORs who had responsibility for validating résumés, 35 percent did not review them and, therefore, had no assurance that the Agency was getting what it paid for. As a result, 30 contractors who were not qualified for their assigned labor categories charged $420,000 to contracts in May 2013.

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

(U//~~FOUO~~) We also determined that the Agency must change its invoicing review process to ensure that contractors correctly charge their time to appropriate labor categories. Some contractors failed to provide the information required for NSA to pay invoices, and, therefore, CORs should have rejected the invoices. Because of insufficient billing information, the audit team questioned labor charges of more than [redacted] in one month. The audit found that 41 CORs used documents other than invoices when authorizing payments. Forms such as the Funds and Man-Hour Expenditure Report, also known as a burn-rate analysis, were commonly used to approve payments. Fourteen contractors exceeded the negotiated loaded labor rate by 20 percent without required approvals, which resulted in questionable costs of more than $24,000 in the month reviewed.

(U//~~FOUO~~) We concluded that NSA qualification and invoice review standards and guidance must be strengthened to provide effective contract oversight. We made six recommendations that the Agency agreed to implement to improve oversight of NSA contractors.

II. (U) Information Assurance Workforce Improvement Program (IAWIP)

(U//~~FOUO~~) The audit objective was to determine whether NSA/CSS complies with the IAWIP in accordance with Department of Defense (DoD) Directive (DoDD) 8570.01 and NSA/CSS Policy 6-34.

(U//~~FOUO~~) The audit found that the NSA/CSS IAWIP should improve the designation and tracking of IAWIP positions within the Agency. The Agency must designate specific positions

that meet the IAWIP criteria and determine whether personnel working in IAWIP designated positions have the required certifications. We found that NSA has large groups of personnel performing IA duties, but their positions have not been properly designated as IAWIP positions. Of the [redacted] IA personnel tracked by the IAWIP office, 71 percent were certified. The Agency IAWIP must be strengthened to ensure that personnel performing IA duties have been properly certified.

(U//~~FOUO~~) The Agency agreed to implement our seven recommendations to improve the designation and tracking of IAWIP positions.

(U) Significant Revised Management Decisions

(U) No management decisions were significantly revised.

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

(U) AUDITS

(U) Audits Completed in the Reporting Period

(U) NSA FY2013 Compliance with the Improper Payments Elimination and Recovery Act (IPERA)

(U//~~FOUO~~) Each fiscal year, the NSA/CSS IG is required to determine whether the Agency is in compliance with IPERA and submit a report on that determination. Our audit concluded that the Agency is fully compliant with IPERA; it was non-compliant in the two previous audits.

(U) Information Assurance Workforce Improvement Program

(U) DoD Directive 8570.01, *Information Assurance Training, Certification, and Workforce Management*, requires implementation of an Information Assurance (IA) Workforce Improvement Program (IAWIP) to build an expert DoD IA workforce. DoDD 8570.01-M requires that personnel who perform IA duties maintain certification corresponding to the highest functions their positions require. The audit found that NSA/CSS's IAWIP needs improvement in designating and tracking IAWIP positions within the Agency and that certifications are not reviewed periodically to ensure that they are current.

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

(U) Nuclear Weapons Personnel Reliability Program (NWPRP)

(U//~~FOUO~~) One of the Agency's most important missions is [redacted] The purpose of the NWPRP is to ensure that all NSA/CSS personnel who perform duties associated with nuclear weapons meet "the highest possible standards of individual reliability." The audit found that NWPRP designated positions are not well defined. As a result, individuals performing critical NC2 duties might not be NWPRP certified and subject to DoD reliability standards. The audit also found that documentation for appointments to key NWPRP positions lacks fundamental details, such as names of individuals appointed, effective date of appointments, and responsibilities delegated by appointments, and does not always reflect current assignments, resulting in lack of accountability.

(U) Vanpools

(U//~~FOUO~~) Executive Order 13150, *Federal Workforce Transportation*, requires that federal agencies establish transportation fringe benefit programs that offer a non-taxable transit subsidy to qualified federal employees who use mass transit or vanpools for their daily commutes. Our review concluded that the Agency's vanpool transit benefit program did not comply with all DoD requirements. Some vanpool applications were incomplete, ineligible participants received benefits, and important internal controls did not exist. As a result, NSA paid $51,176 in transit benefits to ineligible participants from 1 October 2012 to 30 June 2013. We also estimated that NSA paid $9,722 in transit subsidies for employees who rode in a vanpool on less than

50 percent of their scheduled workdays. In addition, the Agency did not maintain accurate and complete vanpool records.

(U) Information Assurance Directorate Mobility Program

(U//~~FOUO~~) The NSA/CSS OIG examined two hotline complaints, one of which was reported under the Intelligence Community Whistle Blower Protection Act of 1998, concerning the Information Assurance Directorate (IAD) Mobility Program. We determined that, initially, the IAD Mobility Program lacked oversight and documentation. However, IAD mission managers and program leadership now provide program oversight and comply with NSA policies.

(~~S//NF~~) We substantiated alleged risks to [redacted] During the audit, DoD Instruction 8500.01 was issued, [redacted] The Defense Information Systems Agency, NSA's partner in this program, also communicated the potential risks of the [redacted] A mitigating [redacted] addressing the [redacted] is being implemented but is approximately four months behind schedule.

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

(U) Federally Funded Research and Development Center–Institute for Defense Analyses (IDA)

(U//~~FOUO~~) In 1958, NSA established a long-term contractual relationship with IDA to create a Federally Funded Research and Development Center (FFRDC) in Princeton, New Jersey, to fulfill the need for a dedicated group of world-class mathematicians. IDA has since added centers in Bowie, Maryland, and La Jolla, California. [redacted] Our review found that the IDA contract is not administered efficiently and that property accountability is fragmented and does not meet standards.

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

(U) Oversight Review of the Restaurant Fund (RF)

(U//~~FOUO~~) NSA contracted with an independent certified public accounting firm to audit the comparative financial statements of the NSA RF for the years ended 30 September 2013 and 2012 and to report on internal controls on financial reporting and compliance with laws and regulations. The accounting firm found that the RF financial statements had been fairly presented, in all material respects, in conformity with U.S. generally accepted accounting principles, and that the RF had four deficiencies in internal controls on financial reporting considered to be material weaknesses and two deficiencies in compliance considered to be significant, one of which was a repeat finding.

(U) Oversight Review of the Civilian Welfare Fund (CWF)

(U//~~FOUO~~) NSA contracted with an independent certified public accounting firm to audit the comparative financial statements of the NSA CWF for the years ended 30 September 2013 and 2012 and to report on internal controls on financial reporting and compliance with laws and regulations. The accounting firm found that the CWF financial statements had been fairly presented, in all material respects, in accordance with U.S. generally accepted accounting

principles, and that the CWF had two deficiencies in internal control on financial reporting that are considered to be material and two deficiencies in internal control over compliance that are considered to be significant, one of which was a repeat finding.

(U) Signals Intelligence (SIGINT) Directorate Data Flow Management

(U//~~FOUO~~) To improve data flow governance, the Mission Governance Team in the Office of Targeting Strategy & Mission Integration (TSMI) was created to track and document movement of SIGINT data and verify system compliance with all data authorities. Some SIGINT data flows are being forwarded without sufficient TSMI oversight because of a deficient data flow governance process and limited enforcement of United States Signals Intelligence Directive DA3511, *Targeting and Data Flow Management*. As a result, there is an increased risk of non-compliance with laws, directives, and policies that govern U.S. person and second-party person privacy. TSMI's data flow governance process and oversight of data flows have helped the Agency manage compliance and operational risks. However, problems affecting risk and mitigation remain. There is no complete and accurate picture of the data.

(U) Contractor Qualifications

(U//~~FOUO~~) Contractor companies and their personnel are critical to NSA/CSS. Oversight to ensure that these companies meet contract requirements and efficiently use the Agency's limited resources is also critical. Our review revealed that qualification and invoice review standards must be strengthened to provide effective contract oversight. Some CORs, who are responsible for contract oversight, did not perform detailed reviews of monthly invoices or review qualifications of contractor personnel.

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

(U) FY2014 Report of NSA/CSS Compliance with the Federal Information Security Management Act (FISMA)

(U//~~FOUO~~) We reported on the Agency's compliance with 11 IT security programs or processes. The Agency must improve in [redacted] of the 11 areas: [redacted]

(U) Contractor Participation in Associate Directorate for Education and Training (ADET) Courses

(U//~~FOUO~~) ADET's *Contractor Training Policy and Procedures* outlines the limited conditions under which government training of contractor personnel might be proper. ADET expressed concern to the OIG about increased contractor training; therefore, we conducted this audit to determine whether contractor training complies with Agency policies. We concluded that contracting officer course approval documentation was not maintained and that courses provided to contractor employees did not relate to the statement of work or were basic or introductory and, therefore, might not have been necessary. Our testing of the Agency's electronic education systems, the [redacted] revealed that accurate permanent records are not maintained and system controls can be circumvented.

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

(U) Significant Outstanding Recommendations

(U) The Communications Security (COMSEC) Accountability Program

(U//~~FOUO~~) Agency policy does not require an independent investigation to determine why COMSEC material was lost, although that is key to preventing recurrences. The Information Assurance Insecurities Branch (now Audits and Insecurities) performs a limited trend analysis of COMSEC incidents only on request, and it does not follow up to determine whether corrective action has been taken. In FY2005,

(U//~~FOUO~~) **Finding** COMSEC incidents need independent investigation.

(U//~~FOUO~~) **Recommendation** Revise NSTISSI 4003 and NSA/CSS Policy Manual 3-16 to require an independent investigation of insecurities involving missing COMSEC material, with the major reason for the loss summarized in the final report for COMSEC incidents; record the results in the insecurity database.

(U//~~FOUO~~) **UPDATE:** The IAD Director signed CNSSI No. 4003 on 27 May 2014, and it is available through the CNSS.gov web site. NSA/CSS Policy 3-16 was published on 4 June 2014. IAD is updating NSA/CSS Policy Manual 3-16, which is expected to be issued in November 2014. The recommendation was originally scheduled to be closed in September 2007.

(U//~~FOUO~~) **Recommendation** Perform trend analysis to identify measures needed to prevent COMSEC insecurities at all levels.

(U//~~FOUO~~) **UPDATE:** IAD insecurities analysts began trend analysis of U.S. insecurity information in June 2014 using the IAD database; however, the database continues to be developed to meet the requirements of analysis to be performed. The recommendation was originally scheduled to be closed in September 2007.

(U//~~FOUO~~) **Recommendation** Revise NSA/CSS Policy Manual 3-16 to establish criteria and procedures for requesting an investigation from the appropriate ADS&CI office involving loss of classified COMSEC material from NSA COR accounts and COMSEC material

(U//~~FOUO~~) **UPDATE:** NSA/CSS Policy 3-16 was published on 4 June 2014. IAD is updating NSA/CSS Policy Manual 3-16, which is expected to be issued in November 2014. The recommendation was originally scheduled to be closed in May 2007.

(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 manages the secure transfer of data between domains with different security levels (e.g., Top Secret to Unclassified).

(~~TS//SI//NF~~) **Finding** NSA organizations as DCID 6/3 and DoD guidance require, because The Technology Directorate (TD) must monitor compliance with this guidance when it has been issued.

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

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

(U//~~FOUO~~) **Recommendation** validate compliance with the security configuration policy.

(U//~~FOUO~~) **UPDATE:** The estimated to be completed in January 2015, includes four CDS configuration control areas that will validate compliance with the security configuration policy. The original recommendation was scheduled to be closed in December 2010.

(U) Agency Controls for Information Technology (IT) Hardware Purchases

(~~C//REL TO USA, FVEY~~) The audit concluded that the Agency's supply chain risk management (SCRM) strategy

(U//~~FOUO~~) **Finding** purchase controls

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

(U//~~FOUO~~) **UPDATE:** TD has addressed the process but not the entire Agency The original recommendation was scheduled to be closed in November 2011.

(U) Nuclear Command and Control (NC2)

(U//~~FOUO~~) The NC2 program Since 2003, approximately 350 recommendations related to NC2 have been made by auditors and vulnerability assessment teams. The focus of the 2013 OIG audit was to ensure that actions taken satisfied previous recommendations. In addition, the audit reviewed new problems discovered since a 2006 OIG audit.

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

(~~S//NF~~) **Recommendation** and establish a timeline for completion.

(U//~~FOUO~~) **UPDATE:** A high-level requirements document and a plan of action and milestones document have been created, and discussions were held to identify possible mission assurance sites. A cost estimate of has been assessed. Analysis of alternatives and a schedule and strategy to engage in the FY2016 budget cycle must be completed. This recommendation was originally scheduled to be closed in December 2011.

(~~C//REL TO USA, FVEY~~) **Recommendation** Conduct an annual exercise of primary and back-up systems and services

(U//~~FOUO~~) **UPDATE:** IAD reported that the remaining systems to be tested require replacement parts before testing. The purchase of the replacement parts was delayed due to the acquisition process, and at this time there is no estimated delivery date. will re-test once the parts arrive. This recommendation was originally scheduled to be closed in December 2011.

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

(U) NSA/CSS Enterprise Solution (NES) and Baseline Exception Request Processes (BER)

(U//~~FOUO~~) TD established the NES/BER processes to reduce IT complexity, improve interoperability and security, and manage IT costs. The audit concluded that Agency organizations and contractors [redacted]

(U) **Finding** Agency organizations and contractors [redacted]

(U//~~FOUO~~) The Chief Information Officer (CIO) chose to terminate the current NES and BER processes, (recommendation 1) using a phased approach between October 2011 and September 2013.

(U//~~FOUO~~) **Recommendation :** If NES and BER processes are terminated, implement a new process that will [redacted] including automated compliance verification and performance monitoring, as required by the Clinger-Cohen Act.

(U//~~FOUO~~) **Recommendation :** The new or existing process should implement Recommendations 2 through 5 to strengthen compliance among Agency organizations and contractors.

(U//~~FOUO~~) **Recommendation :** Upon completion of Recommendation 1, implement automated compliance controls that ensure that organizations [redacted]

(U//~~FOUO~~) **UPDATE:** TD has developed new processes for [redacted] but has not addressed [redacted] These recommendation s were originally due to be resolved by 30 September 2013.

(U//~~FOUO~~) **Recommendation :** Upon completion of Recommendation 1, develop contract provisions to require contractors to comply with NES and BER processes, as NSA/CSS Policy 6-1 requires.

(U//~~FOUO~~) **UPDATE:** TD has not completed the necessary contract provisions to require contractors to comply with NSA/CSS Policy 6-1. This recommendation was originally scheduled to be closed in April 2011.

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

(U) Ongoing Audits

(U) Security Controls for the NSA/CSS Data Cloud

(U//~~FOUO~~) The objective is to determine whether Agency data is being properly tagged to ensure its confidentiality, integrity, and availability.

(U) NSANet Server Security

(U//~~FOUO~~) The objective is to determine whether physical and logical access security controls of Agency-operated servers connected to NSANet are effective in securing the Agency's data.

(U) [redacted]

(U//~~FOUO~~) The objectives of this joint NSA/CSS-National Reconnaissance Office audit are to determine whether the [redacted] system meets NSA/CSS requirements to support the

Intelligence Community and to assess the acquisition oversight practices used to manage [redacted] development and operations life cycle.

(U) Operational Test Authority (OTA)

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

(U//~~FOUO~~) The objective is to determine whether OTA is independent.

(U) Use of [redacted] Cell Phones and Mobile Computing Devices

(U//~~FOUO~~) The objective is to determine whether cell phones and mobile computing devices issued to NSA employees are accounted for and used in accordance with laws, regulations, and policies.

(U) Systems Engineering and Technical Assistance (SETA) Contractors Non-Disclosure Agreements

(U//~~FOUO~~) The objective is to determine whether Agency SETA contractors have access to proprietary information without non-disclosure agreements.

(U) Technology Transfers

(U//~~FOUO~~) The objective is to determine whether NSA/CSS has an effective and repeatable process for transferring technologies and capabilities developed by the Research Directorate to NSA/CSS operations.

(U) Virtual Desktop Infrastructure

(U//~~FOUO~~) The objective is to evaluate the effectiveness and efficiency of the implementation of the virtual desktop infrastructure.

(U) Purchasing Cyber Exploits

(U//~~FOUO~~) The objective is to determine whether the Agency has controls for managing cyber vulnerability and exploit purchases.

(U) FY2014 Financial Statement Audit

(U) The FY2014 Intelligence Authorization Act requires that NSA ensure that a full financial audit is conducted beginning with Fiscal Year 2014 and that, as early as practicable, but no later than the FY2016 audit, the NSA Director take all reasonable steps necessary to ensure that the audit contains an unmodified opinion on the Agency's financial statements.

(U) The audits are the responsibility of NSA's IG, who is given the discretion to contract with an independent public accounting firm to conduct them. The IG contracted with [redacted] to audit NSA's FY 2014 financial statements. The OIG is overseeing the firm's work.

(U) The objective of the audit is to provide an opinion as to whether the Agency's financial statements are presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles. In addition, federal financial statement audit requirements mandate that the auditor assess the Agency's internal controls and the Agency's compliance with applicable laws and regulations.

(U) INSPECTIONS

(U) Inspections Completed in the Reporting Period

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

(U//~~FOUO~~) NSA/CSS and Army Intelligence and Security Command Offices of the Inspector General conducted a joint inspection of . Inspectors found that an aging IT infrastructure poses challenges to the workforce. The time needed to get an NSANet account is excessive—six weeks on average—and some account requests take as long as three months, effectively reducing a one-year tour to nine months.

(U//~~FOUO~~) Inadequate manpower was widely cited as a problem by the workforce. Further review revealed that assigned billets were adequate to perform mission but that frequent redirection of personnel was creating shortages in several areas. Requirements to provide manning to support often bring operations manning to minimum levels, increasing stress on junior personnel.

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

(U) Field Inspection of NSA/CSS Representative to the United States Special Operations Command (NCR SOCOM), 28 October–19 November 2013

(U//~~FOUO~~) The NSA/CSS inspection team found an overall positive command climate at the NCR SOCOM and Cryptologic Support Group SOCOM organization (F1T) on MacDill Air Force Base in Florida. Recent personnel turnovers, however, created stress on the staff to perform routine functions. Although successful in accomplishing its mission, F1T will face increased complexities in supporting

(U//~~FOUO~~) Limited-Scope Field Inspection of

(U//~~FOUO~~) An inspection team conducted a limited-scope inspection of facilitates travel of NSA/CSS personnel to and from

(U//~~FOUO~~) Inspectors witnessed an efficient process that quickly and professionally handles travelers arriving in and departing from Storage of hazardous materials in the warehouse and management and accountability of property throughout the area of responsibility were the most serious problems found during the inspection.

(U) Significant Outstanding Recommendations

(U) All significant recommendations from previous inspection reports have been implemented.

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

(U) Ongoing Inspections

(U) Joint Inspection of NSA/CSS Georgia Cryptologic Center (NSAG)

(U//~~FOUO~~) The NSA/CSS, INSCOM, Fleet Cyber Command (FCC), and Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA) OIGs conducted a joint inspection of NSAG from 3 to 14 March 2014. The final report is in progress.

(U) Joint Inspection of the

(~~S//TK//REL TO USA, FVEY~~) The NSA/CSS, AFISRA, FCC, CIA, and National Reconnaissance Office OIGs conducted a joint inspection of A draft report is in progress.

(U) Field Inspection of the Center for the Advanced Study of Language (CASL)

(U//~~FOUO~~) The NSA/CSS OIG conducted a field inspection of CASL from 21 to 25 July 2014. A working draft report is in progress.

(U) Joint Inspection of the Alaska Mission Operations Center (AMOC)

(U//~~FOUO~~) The NSA/CSS, AFISRA, and FCC OIGs conducted a joint inspection of AMOC from 22 July to 2 August 2014. The final report is in progress.

(U) Field Inspection of NSA/CSS Representative and Cryptologic Services Group U.S. Transportation Command (NCR TRANSCOM)

(U//~~FOUO~~) The NSA/CSS OIG conducted a field inspection of NCR TRANSCOM from 12 to 15 August 2014. The working draft report is in progress.

(U) Field Inspection of National Laboratories

(U//~~FOUO~~) The NSA/CSS OIG conducted a field inspection of NSA programs at Lawrence Livermore and Sandia National Laboratories from 18 to 22 August 2014. A working draft report is in progress.

(U) Field Inspection of

(~~TS//SI//NF~~) The NSA/CSS OIG conducted a field inspection of A working draft report is in progress.

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

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

(U) SPECIAL STUDIES

(U) Special Studies Completed in the Reporting Period

(U//~~FOUO~~) Cybersecurity: Integrating SIGINT and Information Assurance (IA) Authorities to Protect and Defend U.S. Networks

(U//~~FOUO~~) IAD's and the NSA/CSS Threat Operations Center's (NTOC) execution of the cybersecurity mission to protect and defend U.S. networks requires the compliant integration of SIGINT and IA authorities. Although IAD and NTOC analysts understand the boundaries of these authorities, management oversight and internal controls for integrating SIGINT and IA need improvement.

(U) Intelligence Oversight of the Federally Funded Research and Development Center–Institute for Defense Analyses (IDA)

(U//~~FOUO~~) NSA [redacted] with the IDA. The OIG's review of the controls to ensure compliance with Executive Order 12333 and other laws and policies for [redacted] found that, although most responsibilities were being fulfilled, some areas need improvement. (b)(3)-P.L. 86-36

(U//~~FOUO~~) USSOCOM Program Compliance with Signals Intelligence Policies and Procedures

~~(S//NF)~~ A special Department of Defense mission unit executes a range of military operations [redacted] that support the requirements of the Commander, United States Special Operations Command (USSOCOM), the geographic combatant commanders, and other government agencies. A 2005 memorandum of agreement describes the special cryptologic partnership between NSA/CSS and USSOCOM and establishes the framework from which to derive the joint responsibilities in producing and sharing intelligence information and technology in support of NSA/CSS cryptologic requirements and USSOCOM tactical operations.

~~(S//NF)~~ The NSA/CSS Liaison Office is responsible for coordinating [redacted] Liaison personnel understand SIGINT policies and procedures and have established procedures for interacting with the U.S. Cryptologic System. However, internal controls need improvement.

(U) Significant Outstanding Recommendations

(U//~~FOUO~~) Retention of Domestic Communications Collected Under Foreign Intelligence Surveillance Act (FISA) Surveillances

(U//~~FOUO~~) While conducting collection operations authorized under FISA, NSA sometimes incidentally collects domestic communications subject to retention limitations.

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

(U//~~FOUO~~) **Finding** Although NSA collection systems and raw traffic databases can be programmed to facilitate compliance with retention procedures, some processing and retention procedures are not so programmed.

(U//~~FOUO~~) **Recommendation** In accordance with NSA/CSS Policy 1-12, develop a plan containing timelines to baseline and document configuration of systems that process and store FISA data. Provide the OIG with a list of those systems. The OIG will assess the implementation of this plan in a future audit.

(U//~~FOUO~~) **UPDATE:** [redacted] and [redacted] are the baseline for documenting configuration of systems that process and store FISA data. NSA/CSS Policy 1-12 is being updated to require the system owners of all systems with FISA data to register their systems in [redacted] and [redacted]. This recommendation was originally scheduled to be closed in September 2008.

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

(U) Ongoing Special Studies

(U//~~FOUO~~) Implementation of §215 of the USA PATRIOT Act and §702 of the FISA Amendments Act (FAA)

(U//~~FOUO~~) The objective of this study, requested by eight members of the Senate Committee on the Judiciary, is to describe how data is collected, stored, analyzed, disseminated, and retained under §215 and §702 authorities in effect in 2013, steps taken to protect U.S. person information, restrictions on using the data and how the restrictions are implemented, causes of non-compliance, the steps NSA has taken to minimize recurrence, analyst use of the data to support intelligence missions, and the oversight and compliance activities performed by internal and external organizations in support of the FAA §702 minimization procedures and Business Records FISA Orders.

(U) Nepotism in the Associate Directorate for Security and Counterintelligence (ADS&CI)

(U//~~FOUO~~) This special study focuses on whether ADS&CI violated nepotism policies or laws governing appointment, employment, promotion, and reward of its personnel.

(U) Signals Intelligence Directorate Office of Oversight and Compliance (SV) Mission Compliance Program

(U//~~FOUO~~) The objective of this study is to evaluate the effectiveness of the SV compliance program, including its support to the global SIGINT enterprise.

(U) INVESTIGATIONS

(U) Summary of Prosecutions

(U) In May 2014, a former Agency contractor pled guilty in federal court to making false claims to the government in connection with work at NSA. In September 2014, the former contractor was sentenced to six months home detention, three years probation, and a $100 special assessment. The individual was also ordered to pay restitution of $65,264.55, which has been paid in full. The Assistant U.S. Attorney is coordinating with suspension and debarment authorities to preclude the former contractor's participation in government contracts.

(U) Agency Referrals

(U//~~FOUO~~) The Investigations Division referred one investigation to the U.S. Attorney's Office for the District of Maryland for prosecution. The case involves an Agency employee who represented his privately owned corporation to another government agency to obtain a government decision in favor of his company. The investigation substantiated violations of the U.S. Code and Code of Federal Regulations. The employee resigned from the Agency before the investigation was completed, and the U.S. Attorney declined prosecution.

(U//~~FOUO~~) The Investigations Division referred 17 investigations involving Agency personnel to Employee Relations for disciplinary action. Two employees resigned from the Agency in lieu of disciplinary action, one employee received a written reprimand, two employees received no punishment, and disciplinary action is pending against 12 employees.

(U//~~FOUO~~) We referred 18 investigations substantiating contractor misconduct to the Maryland Procurement Office for action, resulting in the proposed recoupment of more than $315,000.

(U) OIG Hotline Activity

(U//~~FOUO~~) The Investigations Division fielded 557 contacts through the OIG hotline.

(U) Significant Investigations

(U) FISA violation

(U//~~FOUO~~) An OIG investigation substantiated an allegation that an Agency employee failed to report a violation FISA. As a result of a software error, approximately [redacted] files containing FISA data were retained beyond the allowable retention date. When the error was discovered, the files were deleted in accordance with established procedures, but an OIG investigation substantiated that the responsible branch chief failed to notify the oversight and compliance authorities of the data retention violation in violation of United States Signals Intelligence Directive SP0019, *NSA/CSS Signals Intelligence Directorate—Oversight and Compliance Policy*, and SID

Oversight and Compliance Memorandum *FISA-Related Responsibilities*. The case was referred to ER, which decided that no disciplinary action against the employee was warranted.

(U) Misuse of a Communications Intelligence (COMINT) system

~~(TS//SI//REL TO USA, FVEY)~~ An OIG investigation substantiated an allegation that an Agency employee intentionally misused a COMINT system. During an unauthorized test of the system, the Agency employee used an overly broad search term, which resulted in the retrieval of U.S. person communications. The employee reported the violation to the appropriate oversight and compliance authorities, and an OIG investigation substantiated that the employee intentionally used a selection term that was reasonably likely to result in the interception of communications to or from U.S. persons, in violation of E.O. 12333, *United States Intelligence Activities*; DoD Directive 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*; and USSID SP0018, *Legal Compliance and U.S. Person Minimization Procedures*. ER issued the employee a written letter of reprimand.

(U) Contract violation

(U//~~FOUO~~) An OIG investigation substantiated allegations that an Agency senior executive tasked a contractor to perform work exceeding the scope of the contract, creating the potential for an unauthorized commitment, as defined by the Federal Acquisition Regulations (FAR). In addition, the evidence supported the conclusion that the employee tasked the contractor to perform inherently governmental functions, in violation of the FAR and NSA/CSS Policy 1-39, *Inherently Governmental Functions*. The case was referred to ER, which decided that no disciplinary action against the employee was warranted.

(U) Abuse of power

(U//~~FOUO~~) An OIG investigation determined that an Agency senior executive provided preferential treatment to a junior employee by advocating for the promotion of the employee but not for other, similarly situated employees. The evidence substantiated violations of *Standards of Conduct for Employees of the Executive Branch* and the NSA/CSS Personnel Management Manual. The OIG also determined that the subject used public office for the private gain of a friend, in violation of law. The case has been referred to ER for potential disciplinary action.

(U) Investigations

(U//~~FOUO~~) Fifty-six investigations were opened and 60 were closed in the reporting period.

(U) Contractor labor mischarging

(U//~~FOUO~~) During the reporting period, the OIG opened 18 contractor labor mischarging investigations and substantiated seven cases, which resulted in the proposed recoupment of more than $154,000. Twenty-three investigations remain open.

(U) Time and attendance fraud

(U//~~FOUO~~) During the reporting period, the OIG opened six investigations into employee time and attendance fraud and substantiated seven cases, which resulted in one employee's resignation from the Agency and a proposed recoupment of $51,000. Action against the remaining six employees is pending. Seven investigations remain open.

(U) Computer misuse

(U//~~FOUO~~) During the reporting period, the OIG opened 11 investigations involving allegations of computer misuse by two employees and nine contractors. The OIG substantiated six cases of contractor misuse of government information systems, which were referred to the Maryland Procurement Office. One case involving an Agency employee was not substantiated. Investigations involving one employee and three contractors remain open.

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

(U) Audits

(U) Operations and Support

- (U) NSA/CSS Nuclear Weapons Personnel Reliability Program
- (U) Vanpools
- (U) Federally Funded Research and Development Center–Institute for Defense Analyses
- (U) Contractor Qualifications
- (U) Contractor Participation in Associate Directorate for Education and Training Courses

(U) Information Technology

- (U) Information Assurance Workforce Improvement Program
- (U) Information Assurance Directorate Mobility Program
- (U) Signals Intelligence Directorate Data Flow Management
- (U) FY2014 Report of NSA/CSS Compliance with the Federal Security Management Act

(U) Financial

- (U) NSA FY2013 Compliance with the Improper Payments Elimination and Recovery Act
- (U) Oversight Review of the Restaurant Fund
- (U) Oversight of the Civilian Welfare Fund

(U) Inspections

(U) Field Inspections

- (U) Field Inspection of NSA/CSS Representative to the United States Special Operations Command
- (U) Limited-Scope Field Inspection of [redacted]

(U) Joint Inspections

- (U//~~FOUO~~) Joint Inspection of [redacted]

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

(U) Special Studies

(U) Operations

- (U) Intelligence Oversight of the Federally Funded Research and Development Center–Institute for Defense Analyses
- (U//~~FOUO~~) USSOCOM Program Compliance with Signals Intelligence Policies and Procedures

(U) Information Technology

- (U//~~FOUO~~) Cybersecurity: Integrating Dual Signals Intelligence and Information Assurance Authorities to Protect and Defend U.S. Networks

(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	1	$5.32 million	$5.32 million
For which management decision was made during reporting period	1	$5.32 million	$5.32 million
Costs disallowed	0	0	0
Costs not disallowed	1	$5.32 million	$5.32 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)

(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	1	$60,898
For which management decision was made during reporting period	1	$60,898
Value of recommendations agreed to by management	1	$60,898
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) APPENDIX D
RECOMMENDATIONS SUMMARY

(U//~~FOUO~~) The OIG made 282 recommendations to NSA management in reports issued in the second half of FY2014. The Agency implemented 324 recommendations in the reporting period.

(U) Managers fully implemented recommendations made in the following reports by the end of the second half of FY2014:

- (U) Joint Inspection of NSA/CSS Colorado (18 June 2008)
- (U) Field Inspection of the Cryptologic Services Group–Marine Corps Intelligence Activity (1 December 2010)
- (U) Audit of the Power, Space, and Cooling Triage Process for the Extended Enterprise (25 March 2011)
- (U) Joint Inspection of NSA/CSS Hawaii (29 April 2011)
- ~~(TS//SI//NF)~~ Special Study of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (25 May 2011)
- (U//~~FOUO~~) Joint Inspection of NSA/CSS Europe, [redacted]
- (U) Expeditionary Operations Review (28 September 2011) (b)(3)-P.L. 86-36
- (U//~~FOUO~~) Advisory Report on [redacted]
- (U//~~FOUO~~) Joint Inspection of [redacted]
- (U) Audit of NSA/CSS FY2011 Compliance with the Improper Payments Elimination and Recovery Act (16 March 2012)
- (U//~~FOUO~~) Field Inspection of NSA/CSS Europe and Africa (13 November 2012)
- (U) Joint Inspection of Meade Operations Center (21 December 2012)
- (U) Audit of NSA/CSS FY2012 Compliance with the Improper Payments Elimination and Recovery Act (15 March 2013)
- (U//~~FOUO~~) Study of NSA/CSS Personnel Tracking and Accountability in the Extended Enterprise (3 July 2013)
- (U) Audit of the NSA's Denial and Deception Program (15 August 2013)
- (U//~~FOUO~~) Field Inspection of NSA/CSS Representative to the National Geospatial-Intelligence Agency (18 September 2013)
- (U//~~FOUO~~) Field Inspection of NSA/CSS Representative to the U.S. Special Operations Command (12 March 2014)

(U) This page intentionally left blank.