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

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

(U) SEMI-ANNUAL REPORT TO CONGRESS
1 April to 30 September 2013

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

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: ~~20381121~~

~~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 conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

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

(U) INVESTIGATIONS

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

(U) INTELLIGENCE OVERSIGHT

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

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

(U) A MESSAGE FROM THE INSPECTOR GENERAL

(U) This report summarizes the more significant activities of the Office of the Inspector General (OIG) of the National Security Agency/Central Security Service between 1 April and 30 September 2013. The report is mandated by the Inspector General Act of 1978.

(U) During the reporting period, the NSA OIG completed 23 audits, inspections, and special studies.

(U) The Audits Division completed 13 audits spanning operations, finance, information technology, and compliance with federal law.

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

(U) The Intelligence Oversight Division completed four special studies of operations and compliance with federal law.

(U) The Investigations Division fielded 454 contacts from the OIG Hotline. The team opened 47 investigations and closed 59 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, except in one instance. The OIG tracks recommendations until they have been implemented and regularly reports to the NSA Director on the status of open recommendations. Of the 346 recommendations issued in the reporting period, 144 have been closed.

(U) In the reporting period, NSA contracted with an independent public accounting firm to audit the Agency's financial statements with OIG oversight. That contract is under protest.

DR. GEORGE ELLARD
Inspector General

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

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

(U) TABLE OF CONTENTS

(U) A MESSAGE FROM THE INSPECTOR GENERAL i

(U) SIGNIFICANT PROBLEMS, ABUSES, AND DEFICIENCIES 1

(U) RECOMMENDATIONS FOR CORRECTIVE ACTION 1
(U) SIGNIFICANT REVISED MANAGEMENT DECISIONS 2

(U) AUDITS 3

(U) AUDITS COMPLETED IN THE REPORTING PERIOD 3
(U) SIGNIFICANT RECOMMENDATIONS OUTSTANDING IN PREVIOUS SEMI-ANNUAL REPORTS 4
(U) ONGOING AUDITS 8

(U) INSPECTIONS 11

(U) INSPECTIONS COMPLETED IN THE REPORTING PERIOD 11
(U) SIGNIFICANT RECOMMENDATIONS OUTSTANDING IN PREVIOUS SEMI-ANNUAL REPORTS 12
(U) ONGOING INSPECTIONS 12

(U) SPECIAL STUDIES 15

(U) SPECIAL STUDIES COMPLETED IN THE REPORTING PERIOD 15
(U) SIGNIFICANT RECOMMENDATIONS OUTSTANDING IN PREVIOUS SEMI-ANNUAL REPORTS 15
(U) ONGOING SPECIAL STUDIES 16

(U) INVESTIGATIONS 19

(U) SUMMARY OF PROSECUTIONS 19
(U) REFERRALS 19
(U) OIG HOTLINE ACTIVITY 19
(U) INVESTIGATIONS 19

(U) APPENDIX A: AUDITS, INSPECTIONS, AND SPECIAL STUDIES COMPLETED IN THE REPORTING PERIOD 21

(U) APPENDIX B: AUDIT REPORTS WITH QUESTIONED COSTS 23

(U) APPENDIX C: AUDIT REPORTS WITH FUNDS THAT COULD BE PUT TO BETTER USE 25

(U) APPENDIX D: RECOMMENDATIONS SUMMARY 27

(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	6-8, 16
§5(a)(4)	Matters referred to prosecutorial authorities	19
§5(a)(5)	Information or assistance refused	N/A
§5(a)(6)	List of audit, inspection, and evaluation reports	21
§5(a)(7)	Summary of significant reports	1-2
§5(a)(8)	Audit reports with questioned costs	23
§5(a)(9)	Audit reports with funds that could be put to better use	25
§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	i

(U)

(U) SIGNIFICANT PROBLEMS, ABUSES, AND DEFICIENCIES

(U) Recommendations for Corrective Action

(U) OIG studies during the reporting period did not reveal particularly serious or flagrant problems, abuses, or deficiencies related to the administration of Agency programs and requiring immediate reporting to the Director and Congress, but the following three audits yielded significant recommendations.

I. (U) Cleared Defense Contractor (CDC) Access to NSANet

(U//~~FOUO~~) The overall objective of the audit was to determine whether CDC information technology (IT) security controls protect Agency data and information in accordance with Intelligence Community Directive 503, *Information Technology System Security Risk Management, Certification and Accreditation*, September 2008.

(U//~~FOUO~~) Our audit found classified and UNCLASSIFIED//FOR OFFICIAL USE ONLY information [redacted]. We also found that [redacted] were not in compliance with the [redacted] did not detect these system deficiencies. Furthermore, some Agency contracts with CDCs did not reference policies and directives assigning responsibility and accountability for IT security.

(U//~~FOUO~~) The OIG made the following recommendations: [redacted] and review Agency contract documentation to ensure that the standard set of IT security control requirements is included. Management agreed to the recommendations; however, the decision [redacted] did not change after management re-evaluated it.

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

II. (U) Custodial Property Officer Field Account (CPOFLD)

(U//~~FOUO~~) NSA created CPOFLD in the Defense Property Accountability System (DPAS) as a holding account to track Agency-owned accountable property at locations outside NSA Washington where NSA had not created a DPAS account. The original intent was to implement DPAS at all locations and move assets out of CPOFLD and into location accounts. However, at the time of our audit, the Agency had not created DPAS for some locations, and the CPOFLD account had grown to more than [redacted] assets with a reported value exceeding [redacted]

(U//~~FOUO~~) NSA controls were not adequate to ensure the accuracy of the CPOFLD account. As a result, the account was inaccurate and NSA [redacted] NSA most likely [redacted] and

incorrectly recorded these assets in CPOFLD. NSA did not maintain an audit trail to support ownership or location of assets recorded in CPOFLD. In addition, NSA [redacted] CPOFLD. As a result, the OIG could not locate [redacted] of [redacted] items during the inspection of property accountability. Finally, NSA did not value assets in DPAS in accordance with the Department of Defense (DoD) Financial Management Regulation because not all applicable costs were recorded.

(U//~~FOUO~~) The OIG recommended that NSA maintain a complete audit trail from the purchase of equipment through the receipt of goods, reconcile the CPOFLD account, including ownership determination, [redacted] and update the location of those that do, and ensure annual inventory of the CPOFLD account in accordance with DoD Financial Management Regulation. Management agreed to implement all recommendations.

III. (U) Audit of the Agency's [redacted] Program

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

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

(U//~~FOUO~~) Using [redacted] NSA/CSS aims to minimize risk to [redacted] and was the focus of the audit.

(~~S//NF~~) The audit found that the use of [redacted] at NSA/CSS is inconsistent because [redacted] responsibilities are spread across the Agency, few processes are in place to prevent individuals or mission organizations from circumventing the rules or to detect such circumvention, a [redacted] policy does not exist, and the [redacted] does not have enforcement authority over the [redacted] program. The audit also found that some [redacted] related [redacted] and some [redacted] have not been coordinated with the [redacted].

(U//~~FOUO~~) We recommended that the Chief of Staff and Senior Leadership Team develop a [redacted] program that promotes and enforces compliance with DoD regulations and implements internal controls that will prevent and detect non-compliance. Management agreed to implement our recommendations.

(U) Significant Revised Management Decisions

(U) No management decisions have been significantly revised.

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

(U) AUDITS

(U) Audits Completed in the Reporting Period

(U) Cleared Defense Contractor (CDC) Access to NSANet

(U//~~FOUO~~) NSA/CSS employs CDCs to perform unclassified and classified work in contractor SCIFs. By allowing CDCs to connect to and access NSA/CSS information systems, the Agency increases the risk of exposure to data exploitation and compromise by external and internal actors. The audit found classified and UNCLASSIFIED//FOR OFFICIAL USE ONLY information on some unclassified systems, information systems security controls not compliant with system security plans, and inconsistent IT security control requirements in contracts.

(U) The Agency's Small Business Program

(U//~~FOUO~~) We conducted seven tests to determine whether controls over the Agency's small business program protect the integrity of the program. We found that the controls are effective; however, improvements are needed in monitoring to ensure compliance with Federal Acquisition Regulation subcontracting performance thresholds. Proper monitoring will ensure that only eligible small businesses receive program benefits.

(U) Network Enclave Management

(U//~~FOUO~~) The objective of this audit was to determine whether Agency IT Efficiencies efforts will eliminate or reduce network enclaves and produce cost savings. Because of the extensive scope and varying maturity of the IT Efficiencies initiatives, the multi-year time frame for execution, and the lack of measurable goals for enclave elimination, we decided to close this audit. However, we are concerned that some of the challenges identified during our audit might affect the goals of enclave elimination and cost savings. We will monitor the status of these challenges and the IT Efficiencies and NSA-assigned Intelligence Community (IC) IT Enterprise efforts as they progress over the next several years, and we will evaluate the need for additional audits.

(U) The Agency's [redacted] Program

(S//~~REL TO USA, FVEY~~) NSA/CSS aims, through the use of [redacted] to minimize risk to its [redacted] This audit focused on [redacted] The audit revealed that the NSA/CSS [redacted] program lacks structure and a complete IT system, that training needs improvement, and that some [redacted] related contracts do not comply with DoD regulations.

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

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

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

(U) **Conference-Related Expenses**

(U//~~FOUO~~) Office of Management and Budget Memorandum 11-35 instructs all government agencies "to conduct a thorough review of the policies and controls associated with conference-related activities and expenses." We therefore reviewed 13 Agency-sponsored or co-sponsored conferences that cost in total at least [redacted]. The average cost to the Agency per conference was [redacted]. The average number of NSA attendees was approximately [redacted]. The audit revealed apparent ethical violations, inadequate oversight of funding for the [redacted] underreported conference costs, and questionable conference costs.

(U) **Custodial Property Officer Field Account (CPOFLD)**

(U//~~FOUO~~) The NSA Director is responsible for the accountability of all property under his command. NSA created CPOFLD in DPAS as a holding account to track Agency-owned accountable property at locations outside NSA Washington where NSA has not created a DPAS account.

(U//~~FOUO~~) The objective of the audit was to determine whether controls over the CPOFLD account are sufficient to ensure accuracy, including the number of assets and their dollar value as listed in NSA property records. We found that controls were not adequate to ensure the accuracy of the CPOFLD account. As a result, the account was inaccurate and NSA lost visibility over assets for which it might or might not be accountable.

(U) **Intelink Information Technology Security**

(U//~~FOUO~~) Intelink is a group of information services using commercial Internet technology, protocols, and applications on U.S. government and commercial telecommunications systems. The Office of the Director of National Intelligence Inspector General (IG) reported seven deficiencies in the FY2011 Independent Evaluation of ODNI Compliance with the Federal Information Security Management Act (FISMA) of 2002, when ODNI managed Intelink. In October 2011, a memorandum of understanding transferred Intelink services, resources, and personnel from ODNI to NSA/CSS. We sought to determine whether the Intelink security deficiencies identified in the FY2011 IC IG FISMA audit are still present now that NSA/CSS has assumed responsibility for supporting Intelink. Two of seven Intelink controls require improvement: Intelink access policy and contingency plan.

(U) **Compliance with the Reducing Overclassification Act**

(U//~~FOUO~~) This is the first of two reports required by the Reducing Over-Classification Act, which mandates that the Inspector General of each agency with an officer or employee authorized to make original classifications assess whether classification policies and rules have been adopted, followed, and effectively administered and identify policies and rules that might contribute to persistent misclassification. This audit found deficiencies in information security program management, original classification, derivative classification, information security self-inspection program, and information security training and education.

(U//~~FOUO~~) **The Agency's Denial and Deception Program**

(U//~~FOUO~~) NSA/CSS is a member of the Foreign Denial and Deception Committee (FDDC), which advises the Director of National Intelligence on foreign activities that thwart U.S. intelligence through denial and deception (D&D). The FDDC has issued strategies for guiding D&D efforts at IC agencies. The objective of the audit was to determine the progress the Agency has made toward implementing FDDC's 2011 strategy.

(U//~~FOUO~~) The organization responsible for managing D&D efforts was dissolved in 2009, preventing the Agency from monitoring progress. As a result, we were unable to determine the extent of the Agency's support for the IC strategy. Additional changes within the Signals Intelligence Directorate (SID) occurred since 2007, rendering the NSA/CSS policy for managing D&D efforts outdated.

~~(C//REL TO USA, FVEY)~~ NSA/CSS Policy 2-20, *Countering Adversarial Denial and Deception Activities*, 22 September 2005, assigns to SID responsibilities for understanding, identifying, and countering adversarial D&D activities focused on the signals intelligence system. Until the Agency updates NSA/CSS Policy 2-20 and reassigns D&D management responsibilities, NSA/CSS D&D efforts will lack central management.

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

(U//~~FOUO~~) NSA contracted with an independent public accounting firm to audit the financial statements of the NSA Restaurant Fund (RF) for the years ended 30 September 2012 and 2011 to provide a report on internal control over financial reporting and compliance with laws and regulations. The accounting firm found that the RF financial statements were fairly presented, in all material respects, in conformity with U.S. generally accepted accounting principles and that the RF had a deficiency in internal control over financial reporting considered to be a material weakness and another deficiency considered to be significant.

(U) **FY2013 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 five of the 11 areas: [redacted] (b)(3)-P.L. 86-36

(U) **The Agency's Personnel Accountability Program**

(U//~~FOUO~~) DoD Instruction 3001.02, *Personnel Accountability in Conjunction with Natural or Manmade Disasters*, 3 May 2010, requires that the Inspectors General of DoD components conduct bi-annual inspections of the personnel accountability programs of their components to ensure compliance with the instruction. Our review revealed that NSA/CSS does not monitor individual work center compliance and lacks a toll-free emergency call-in number.

(U) **The Agency's Suspension and Debarment Process**

(U//~~FOUO~~) The Federal Acquisition Regulation (FAR), subpart 9.4, permits agency officials to suspend and debar contractors from federal contracting. Suspensions and debarments are discretionary actions to protect the government from contractors who have engaged in misconduct, such as fraud or a criminal offense, or have violated the terms of their contracts.

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

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

The FAR directs agencies to establish appropriate suspension and debarment procedures. We found that the Agency has not actively used its suspension and debarment process.

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

(~~C//REL TO USA, FVEY~~) **on the Agency's Unclassified Network**

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

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

(U~~//FOUO~~) **Finding** Deficiencies with

(U~~//FOUO~~) **Recommendation** Before migrating to an complete and mitigate discovered vulnerabilities within an acceptable level of risk.

(~~S//SI//REL TO USA, FVEY~~) **UPDATE:** could not be updated to satisfy the Agency's requirement; therefore, an alternative that specializes in access was chosen. Additional requirements were associated with which caused delays; Originally due the revised target completion date is

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

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

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

(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).

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

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

(U~~//FOUO~~) **UPDATE:** The capability, which includes described in the OIG findings as risk factors in the risk scoring for each system, has been in development and testing since 2010

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

and has now achieved initial operational capability. Originally due 30 November 2011, these actions have a revised target completion date of December 2014.

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

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

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

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

(U//~~FOUO~~) **UPDATE:** Draft NSA/CSS Policy 6-32, *NSA/CSS Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)*, was sent out for formal Agency comment in early August, and critical comments are being adjudicated. Originally due November 2011, the revised target completion date is December 2013.

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

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

(U//~~FOUO~~) **UPDATE:** The incident response process that [redacted] requires will be satisfied with the draft NSA/CSS Policy 6-32. The policy was sent out for formal Agency comment in early August, and critical comments are being adjudicated. Originally due September 2011, the revised target completion date is December 2013.

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

(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 a 2006 OIG audit.

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

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

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

(U) **NSA Export Controls**

(U//~~FOUO~~) The objective of the audit was to determine whether NSA's export control process complies with laws and regulations and whether the Agency has adequate controls to ensure that transfers of export-controlled information are properly documented and authorized.

(U//~~FOUO~~) **Finding** Export control [redacted]

(U//~~FOUO~~) **Recommendation** For exports authorized through International Traffic in Arms Regulations exemption and Independent Export Authority letter, develop documentation

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

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

standards that require a detailed description of the item exported, defined scope of export, validated requirement, dollar value of export, and stakeholder approval.

(U//~~FOUO~~) **UPDATE** These standards have been added to updated NSA/CSS Policy 1-7, which is out for formal Agency comment. This action was due 1 June 2013.

(U) Ongoing Audits

(U) **Vulnerability Tracking System**

(U//~~FOUO~~) The audit objective is to determine whether [redacted] documentation while [redacted] from the NSA/CSS [redacted] Database to [redacted] (b)(3)-P.L. 86-36

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

(U//~~FOUO~~) The audit objective is to review the reports and related documentation of an independent public accounting firm's audit of the financial statements of the NSA Civilian Welfare Fund for the years ended 30 September 2012 and 2011.

(U) **Foreign Language Incentive Pay (FLIP)**

(U//~~FOUO~~) The audit objective is to determine the cost of paying multi-linguists FLIP for languages that are not an integral part of their mission.

(U) **Information Assurance Workforce Improvement Program (IAWIP)**

(U//~~FOUO~~) The audit objective is to determine whether the NSA IAWIP complies with DoD and NSA policy.

(U) **NSA/CSS Threat Operations Center (NTOC)**

(U//~~FOUO~~) The audit objective is to evaluate the effectiveness and efficiency of NTOC's 24/7 watch operations.

(U) **Information Assurance Directorate Mobility Program**

(U//~~FOUO~~) The audit objective is to examine allegations about the IAD Mobility Program, one of which was reported under the IC Whistle Blower Protection Act of 1998. Specifically, we will determine whether management oversight of the program complied with NSA/CSS policies and whether reported security risks were properly managed and communicated to the Defense Information Systems Agency.

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

(U//~~FOUO~~) The audit objective is to determine whether contractor enrollments in ADET training courses comply with policies, the effect of contractor enrollments on ADET's ability to train Agency personnel, and the costs of providing ADET training to contractors.

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

(U//~~FOUO~~) The audit objective is to determine whether the IDA contract is administered effectively and in compliance with contracting policies and whether the IDA has implemented controls to correct deficiencies noted in the past.

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

(U//~~FOUO~~) The audit objective is to determine whether collected signals intelligence (SIGINT) data is forwarded to the appropriate source systems of record through authorized data flows.

(U) **Vanpools**

(U//~~FOUO~~) The audit objective is to determine whether transit subsidy benefits for vanpool members are paid in accordance with regulations.

(U) **Contractor Qualifications**

(U//~~FOUO~~) The audit objective is to determine whether the Agency has adequate controls to ensure that contractor workforce qualifications meet the labor category requirements for their contracts and whether Agency personnel review monthly invoices to ensure that contractors charge their time to the appropriate labor category.

(U) **NSA/CSS Nuclear Weapons Personnel Reliability Program (NWPRP)**

(U//~~FOUO~~) The audit objective is to determine whether the NWPRP has complied with DoD and Agency guidance and implemented corrective actions to satisfy previous recommendations.

(U) This page intentionally left blank.

(U) INSPECTIONS

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

(U) Inspections Completed in the Reporting Period

(U) **Limited-Scope Field Inspection of Navy Information Operations Command Pensacola (NIOC-P), 22–26 October 2012**

(U//~~FOUO~~) The NSA/CSS OIG augmented the U.S. Fleet Cyber Command OIG inspection of NIOC-P, which [redacted] The inspection report, limited to [redacted] oversight activities not included in the Fleet Cyber Command IG report, recommended that proper documentation be put in place to authorize NIOC-P mission activity and [redacted]

(U) **Field Inspection of NSA/CSS Representative to U.S. Strategic Command (NCR STRATCOM), 5–9 November 2012**

~~(S//SI//REL TO USA, FVEY)~~ The broad mission of the NCR STRATCOM organization includes Cryptologic Services Group (CSG) SIGINT [redacted] in direct support of the USSTRATCOM Intelligence Directorate Joint Intelligence Operations Center. The organization also provides liaison officer support and cryptologic support services to command directorates, Joint Functional Component Command (JFCC)–Space, and JFCC–Integrated Missile Defense.

~~(S//SI//REL TO USA, FVEY)~~ The NSA contingent received very mixed reviews from senior USSTRATCOM customers. While personnel in liaison officer roles supporting the Joint-directorate level tended to be seen as providing great value, the services that the CSG provided were seen to be of lesser value. Customers also expressed concern that [redacted]

(U) **Joint Inspection of NSA/CSS Texas Cryptologic Center (NSAT), 4–15 February 2013**

(U//~~FOUO~~) NSA/CSS, Army Intelligence and Security Command, and Air Force Intelligence, Surveillance and Reconnaissance Agency OIGs inspected NSAT, which provides SIGINT support that responds to customer information needs.

(U//~~FOUO~~) NSAT faces challenges posed by information technology infrastructure and analytic modernization transition. Most of NSAT's workforce [redacted] however, a strong training program enables the organization to produce SIGINT reports that receive positive feedback from customers.

(U//~~FOUO~~) Although the NSAT workforce enjoys the site facilities, to which the workforce moved in 2012, the location outside a military base has created some special challenges. NSAT [redacted] Of particular concern to service leaders were [redacted] who

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

arrived at NSAT [redacted] Each service is left to make arrangements for these individuals [redacted]

(U) **Field Inspection of NSA/CSS Representative to the Federal Bureau of Investigation (NCR FBI), 11–22 March 2013**

(U//~~FOUO~~) This was the first inspection of the NCR FBI organization whose employees are embedded in FBI organizations to facilitate information sharing and collaboration. Although successful in accomplishing their mission, NCR FBI personnel are challenged by the need to provide timely SIGINT support for the wide-ranging and geographically dispersed FBI mission. The dissemination process for [redacted] is time consuming. Although technical impediments to the timely sharing of SIGINT information are being addressed, NSA analysts are frustrated by the lack of clear and readily accessible sharing guidance for NSA analysts interacting with the FBI.

(U) **Field Inspection of NSA/CSS Representative to the National Geospatial-Intelligence Agency (NCR NGA), 22 April–3 May 2013**

(U//~~FOUO~~) This was the first inspection of the NCR NGA. Although successful in accomplishing their mission, NCR NGA personnel are challenged by the need to provide timely SIGINT support for the wide-ranging NGA mission. The dissemination process for [redacted] is time consuming. The technical impediments to the timely sharing of SIGINT information with NGA are being addressed. Individuals expressed frustration, however, with the lack of clear and readily accessible sharing guidance for NSA analysts interacting with NGA.

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

(U//~~FOUO~~) Despite the isolation at this remote location in [redacted] which creates quality-of-life challenges, the NSA/CSS and FCC joint inspection team found a positive command climate.

(U//~~FOUO~~) The cryptologic workforce was shouldering an increasing number of collateral duties [redacted] NSA enabler functions were not in place to support [redacted] As a result, the military workforce in particular was sacrificing family time and working outside their primary skill sets to perform functions typically performed by full-time NSA/CSS enablers.

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

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

(U) Ongoing Inspections

(U) **Inspection of the** [redacted]

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

(U) **Joint Inspection of the**

(U//~~FOUO~~) The Inspections Division conducted a joint inspection of The working draft report is in coordination.

(U) **Inspection of the**

(U//~~FOUO~~) The Inspections Division conducted a field inspection of The working draft report is in coordination.

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

(U//~~FOUO~~) The Inspections Division conducted a joint inspection of The working draft report is in coordination.

(U//~~FOUO~~) **Joint Follow-Up Inspection of the**

(U//~~FOUO~~) NSA/CSS and the U.S. Army Intelligence and Security Command OIGs conducted a joint follow-up inspection of the The working draft report is in coordination.

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

(U) This page intentionally left blank.

(U) SPECIAL STUDIES

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

(U) Special Studies Completed in the Reporting Period

(U) **External Service Provider**

(U//~~FOUO~~) The IC IG requested that NSA/CSS's OIG assist with a study of the IC's practices for FY2011. This report addresses the NSA/CSS OIG study related to the Agency's external service provider,

(U//~~FOUO~~) The NSA/CSS OIG found one control deficiency involving had not forwarded at least information system security incidents to the NSA/CSS Information Systems Incident Response Team (NISIRT), as the contract requires. As a consequence, the Agency

(U//~~FOUO~~) **Personnel Tracking and Accountability in the Extended Enterprise**

(U//~~FOUO~~) A review of personnel tracking tools at three large enterprise sites showed duplication of effort in funds and manpower expended at each site to accomplish the same functions. In addition, the study found a lack of a centralized NSA budget process to capture field requirements.

(U) **System**

(U//~~FOUO~~) is NSA/CSS's corporate compliance tool for automating the process for access to NSA/CSS-hosted data. The OIG testing and procedural reviews to determine whether properly manages access to NSA/CSS-hosted data affirmed that, with few exceptions, access controls are effective. Nonetheless, lacks corporate governance and policy, some users have access to data and oversight and compliance verification efforts within are inconsistent.

(U//~~FOUO~~) **Auditing Control Framework for Analyst Queries of SIGINT System Databases**

(U//~~FOUO~~) We studied auditing control framework for analyst queries of SIGINT system databases. We found that the data the Agency uses to monitor auditing compliance of SIGINT queries is inaccurate and that additional controls are needed to improve auditing control framework.

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

(U) **Technology Directorate Mission Compliance Program**

(U) The TD Office of Compliance, a directorate compliance component, is tasked with providing the Technology Director with reasonable assurance that TD personnel and affiliates within TD-sponsored projects and programs are reliably and verifiably following the legal authorities and

policies affecting U.S. person privacy and mission compliance. Compliance leads assigned to each TD deputy directorate oversee compliance standards implementation within their assigned deputy directorate.

(U//~~FOUO~~) Some TD compliance activities are not meeting NSA/CSS policies and standards:

- (U//~~FOUO~~) TD lacks centralized management of intelligence oversight (IO) and compliance activities.
- (U//~~FOUO~~) Internal control on data access is lacking.
- (U//~~FOUO~~) Weaknesses exist in IO training.

(U//~~FOUO~~) These deficiencies increase the risk for improper handling of NSA mission data. Recent compliance incidents highlight our concerns.

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

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

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

(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** Per 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] will become the baseline for documenting configuration of the systems known to process and store FISA data. The teams continue to integrate systems and system information and are updating their interface to include [redacted] to make the process more user-friendly. Policy 1-12 is being updated to require the system owners of all systems with FISA data to register their systems in both [redacted] and [redacted] Policy 1-12 is expected to be published by the end of January 2014.

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

(U) Ongoing Special Studies

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

[redacted]

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

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

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

(U) **Information Assurance Directorate (IAD) Office of Oversight and Compliance (IV) Mission Compliance Program**

(U) The objective of this study is to evaluate the effectiveness of IAD IV policies and procedures in ensuring that information assurance (IA) activities comply with U.S. law and other directives.

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

~~(S//REL TO USA, FVEY)~~ The objectives of this study are to (1) evaluate compliance with policies and procedures that support the use of integrated SIGINT and IA authorities for the [redacted] and (2) determine whether personnel working under integrated SIGINT and IA authorities for the cybersecurity mission understand the boundaries of and comply with the requirements of those authorities.

(U//~~FOUO~~) **Intelligence Oversight of the Federally Funded Research and Development Center – Institute for Defense Analyses**

(U//~~FOUO~~) The objective of this review is to determine whether controls established by the Agency, in conjunction with the IDAs, are adequate to ensure compliance with E.O. 12333 and all laws and policies for [redacted]

(U//~~FOUO~~) **Testing of Management Controls for FAA §702**

(U//~~FOUO~~) The objective of this study is to determine whether the controls are effective to ensure compliance with FAA §702 Targeting and Minimization Procedures.

~~(TS//REL TO USA, FVEY)~~ [redacted]

(U//~~FOUO~~) The objectives of this study are to determine whether planned and existing policies and internal controls ensure that the organizations under review can accomplish their missions and provide reasonable assurance that [redacted] activities are carried out with due regard for legal, operational, and other factors.

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

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

(U) This page intentionally left blank.

(U) INVESTIGATIONS

(U) Summary of Prosecutions

(U) No cases were prosecuted during the reporting period.

(U) Agency Referrals

(U) Two contract labor mischarging cases involving a loss to the government of more than $396,000 were referred to an office of the United States Attorney and accepted for prosecution during the reporting period.

(U//~~FOUO~~) The Division referred 20 investigations and five contacts involving Agency personnel to Employee Relations (ER) for disciplinary action. One employee was dismissed from the Agency, three employees received suspensions, seven employees received written reprimands, two received letters of counseling, disciplinary action is pending against ten employees, and no action was taken in two cases. Sixteen investigations substantiating contractor misconduct were referred to the Maryland Procurement Office for action.

(U) OIG Hotline Activity

(U//~~FOUO~~) The Investigations Division fielded 454 contacts through the OIG Hotline.

(U) Investigations

(U//~~FOUO~~) Forty-seven investigations were opened and 59 were closed in the reporting period.

(U) Contractor labor mischarging

(U//~~FOUO~~) During the reporting period, the OIG opened nine contractor labor mischarging investigations while substantiating 11 cases. The 11 closed cases resulted in the proposed recoupment of more than $493,000. Ten investigations remain open.

(U) Government travel card abuse

(U//~~FOUO~~) During the reporting period, the OIG opened two investigations into government travel card abuse. The OIG substantiated five cases, which resulted in one employee's resignation from the Agency and one employee receiving a reprimand. Action against the remaining three employees is pending. One investigation remains open.

(U) Time and attendance fraud

(U//~~FOUO~~) During the reporting period, the OIG opened six investigations into employee time and attendance fraud. The OIG substantiated five cases, which resulted in one employee's dismissal from the Agency, one suspension, and no action taken in one case. Action against the remaining two employees is pending. Eight time and attendance investigations remain open.

(U) **Computer misuse**

(U//~~FOUO~~) The OIG opened 12 investigations involving allegations of computer misuse by five employees and seven contractors. During the reporting period, the OIG substantiated two cases of employee misuse of IT systems and substantiated six cases of contractor misuse. The cases substantiated against the government employees were referred to ER for administrative action, and the cases substantiated against the contractors were referred to the Maryland Procurement Office.

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

(U) Audits

(U) **Operations and Support**

- (U) Conference-Related Expenses
- (U) The Agency's Small Business Program
- (U) The Agency's Personnel Accountability Program
- (U) The Agency's [redacted] Program
- (U) The Agency's Suspension and Debarment Process
- (U//~~FOUO~~) The Agency's Denial and Deception Program

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

(U) **Finance**

- (U) Custodial Property Officer Field Account
- (U) Oversight Review of the Restaurant Fund

(U) **Information Technology**

- (U) Audit of Cleared Defense Contractor Access to NSANet
- (U) Audit of Network Enclave Management
- (U) Intelink Information Technology Security

(U) **Federal Compliance**

- (U) NSA's Compliance with the Reducing Overclassification Act
- (U) FY2013 Compliance with the Federal Information Security Management Act

(U) Inspections

(U) **Field Inspections**

- (U) Navy Information Operations Command Pensacola
- (U) NSA/CSS Representative to U.S. Strategic Command
- (U) NSA/CSS Representative to the Federal Bureau of Investigation
- (U) NSA/CSS Representative to the National Geospatial-Intelligence Agency

(U) **Joint Inspections**

- (U) NSA/CSS Texas Cryptologic Center
- (U//~~FOUO~~) [redacted]

(U) Special Studies

(U) **Operations**

- (U//~~FOUO~~) Personnel Tracking and Accountability in the Extended Enterprise
- (U) [redacted] System
- (U//~~FOUO~~) [redacted] Auditing Control Framework for Analyst Queries of SIGINT System Databases
- (U) Technology Directorate Mission Compliance Program

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

(U) **Federal Compliance**

- (U) External Service Provider [redacted]

(U) APPENDIX B
AUDIT REPORTS WITH QUESTIONED COSTS

(U~~//FOUO~~)

Report	Number	Questioned Costs	Unsupported Costs
For which no management decision had been made by start of reporting period	0 0		0
Issued during reporting period	1	$159,000	$159,000
For which management decision was made during reporting period	1 $159,000		$159,000
Costs disallowed	1	$159,000	$159,000
Costs not disallowed	0	0	0
For which no management decision was made by end of reporting period	0 0		0
(U) Because OIG recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.			

(U~~//FOUO~~)

(U) This page intentionally left blank.

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

(U)

Report	Number of Reports	Amount
For which no management decision had been made by start of reporting period	0	0
Issued during reporting period	0	0
For which management decision was made during reporting period	0	0
Value of recommendations agreed to by management	0	0
Value of recommendations not agreed to by management	0	0
For which no management decision was made by end of reporting period	0	0
(U) Because OIG recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.		

(U)

(U) This page intentionally left blank.

(U) APPENDIX D
RECOMMENDATIONS SUMMARY

(U//~~FOUO~~) The OIG made 346 recommendations to NSA management in reports issued in the third and fourth quarters of FY2013: 77 in the first and 269 in the second. During the third and fourth quarters, the Agency implemented 117 and 160 recommendations, respectively.

(U) Managers fully implemented recommendations made in the following reports by the end of the second half of FY2013:

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

- (U) Inspection of the Directorate of Engineering (6 November 2006)
- (U//~~FOUO~~) Joint Inspection of [redacted]
- (U) Inspection of the [redacted]
- (U) Audit Report on Federally Funded Research and Development Center – Institute for Defense Analyses (16 September 2009)
- (U) Audit Report on Accounts Payable (22 March 2010)
- (U) Joint Inspection of NSA/CSS Georgia (30 June 2010)
- (U//~~FOUO~~) Special Study of the [redacted]
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records—Control Weaknesses (29 September 2010)
- (U//~~FOUO~~) Special Study of Non-Traditional Dissemination Methods: Dissemination Strategy Evaluation (28 September 2011)
- ~~(TS//SI//NF)~~ Special Study of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Collection (1 August 2012)
- (U) Special Study of the Research Directorate's Compliance Program (16 October 2012)

(U) This page intentionally left blank.