Doc ID: 6676414

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

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE


# (U) SEMI-ANNUAL REPORT TO CONGRESS
## 1 October 2012 to 31 March 2013

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

Approved for Release by NSA on 07-31-2019,
FOIA Case # 79825 (litigation)

Classified By:
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20380430~~

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

Release: 2019-07
NSA:09287

# (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.



Release: 2019-07
NSA:09288

# (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 October 2012 and 31 March 2013. 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.

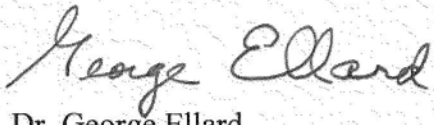
(U) The Audits Division completed eight audits spanning operations, finance, and information technology.

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

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

(U) The Investigations Division fielded 406 contacts from the OIG Hotline. The team opened 48 investigations and closed 49 in the reporting period.

(U) Each report and special study contained recommendations on which the OIG and NSA management agreed, 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 422 recommendations issued in the reporting period, 164 have been closed.



Dr. George Ellard
Inspector General



Release: 2019-07
NSA:09289

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

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

Doc ID: 6676414



# (U) TABLE OF CONTENTS





Release: 2019-07
NSA:09291

# (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 | 5-6, 14 |
| §5(a)(4) | Matters referred to prosecutorial authorities | 17 |
| §5(a)(5) | Information or assistance refused | N/A |
| §5(a)(6) | List of audit, inspection, and evaluation reports | 19 |
| §5(a)(7) | Summary of significant reports | 1-2 |
| §5(a)(8) | Audit reports with questioned costs | 21 |
| §5(a)(9) | Audit reports with funds that could be put to better use | 23 |
| §5(a)(10) | Summary of reports for which no management decision was made | N/A |
| §5(a)(11) | Significant revised management decisions | N/A |
| §5(a)(12) | Management decision disagreements | N/A |

(U)

# (U) SIGNIFICANT PROBLEMS, ABUSES, AND DEFICIENCIES

## (U) Recommendations for Corrective Action

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

### I. (U) NSA Export Controls

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

(U//~~FOUO~~) The audit found that the Agency's control of [redacted] and NSA might not be meeting its obligation to notify Congress of certain high-dollar-value exports.

(U//~~FOUO~~) The Agency also lacks a segregated structure for export control; thus, final approval for exporting [redacted] has been taken from mission directors. Without oversight from accountable managers, [redacted]

(U) The OIG made the following recommendations:

- (U//~~FOUO~~) For exports authorized through International Traffic in Arms Regulations (ITAR) exemptions and Independent Expert Authority (IEA) letters, develop documentation standards that require detailed descriptions of the items exported, defined scopes of export, validated requirements, dollar value of exports, and stakeholder approvals.
- (U//~~FOUO~~) Request that the Office of General Counsel (OGC) clarify the Agency's requirement to notify Congress about transfers of [redacted]
- (U//~~FOUO~~) Amend [redacted] to:
  - (U//~~FOUO~~) Establish that [redacted] are accountable for ITAR-controlled [redacted] and hold final approval authority for ITAR exports of [redacted] and
  - (U//~~FOUO~~) Formally delegate approval authority for ITAR exports [redacted] to specific management levels [redacted]

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



Release: 2019-07
NSA:09293

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

## II. (U) Fair Labor Standards Act (FLSA) Overtime Overpayments

(U//~~FOUO~~) Under the Code of Federal Regulations Foreign Exemption Criteria, non-exempt employees working at foreign locations are limited to the overtime rates paid to exempt employees. From January 2001 through May 2012, NSA/CSS overpaid [redacted] employees $642,691 for overtime in foreign locations. In July 2012, NSA/CSS notified Congress that it had corrected the problems and had implemented manual controls as early as March 2011. The NSA/CSS Chief of Staff requested that the OIG determine whether appropriate steps had been taken to prevent a recurrence of these errors. We found that these procedures were ineffective in preventing incorrect payments because they are manually intensive and rely on Human Resources personnel to continuously monitor changing employee travel plans.

(U) The OIG made the following recommendation:

> (U//~~FOUO~~) Implement a process for non-exempt employees to change their FLSA overtime statuses when deployed or on temporary duty to foreign locations. Require that certifying officials approve employee FLSA status changes.

(U//~~FOUO~~) Management provided an alternative solution that meets the intent of the recommendation.

## (U) Significant Revised Management Decisions

(U) No management decisions have been significantly revised.



Release: 2019-07
NSA:09294

# (U) AUDITS

## (U) Audits Completed in the Reporting Period

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

(U) The audit objective was to determine the effectiveness of KMI in meeting program goals. The audit did not reveal any reportable findings; however, the KMI Project Management Office should ensure that the KMI web site contains current information.

### (U) Human Resources Management System

(U//~~FOUO~~) The NSA Comptroller requested a review of application controls in the Agency's Human Resources Management System, as part of the Agency's quest to achieve financial auditability. We found three control deficiencies involving user accounts, segregation of duties, and system monitoring. Human Resources Information Systems has updated the account deletion process and removed formerly undeleted user accounts. Records and Technology management has documented roles with conflicting capabilities.

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

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

(U//~~FOUO~~) Fundamental system security controls have not been consistently implemented or appropriately maintained for [redacted] These controls include system component authorization, access, and account management controls; training administration and compliance controls; and operational controls maintained and reviewed consistently as part of an effective continuous monitoring program. Management agreed with all recommendations and has initiated corrective action plans to improve [redacted] system security controls and provide additional assurance that data is protected.

### (U) Export Controls

(U//~~FOUO~~) This audit focused on two key areas of technology security at NSA: (1) defense-related exports by contractors supporting [redacted] and (2) certification of data protection and authorization of data release for exports of [redacted]

(U//~~FOUO~~) Our audit found ineffective processes in controlling defense-related exports. [redacted]



Release: 2019-07
NSA:09295

(U) **Civilian Pay and Benefits**

(U//~~FOUO~~) The objective of the audit was to determine whether pay and benefits for civilian personnel were correctly paid and properly authorized for selected entitlements, such as overtime pay and administrative leave. The audit revealed that improvements could be made in controls over payroll transactions, accurate and timely certification of timesheets, and reconciliation of cash awards.

(U) **Fair Labor Standards Act (FLSA) Overtime Overpayments**

(U//~~FOUO~~) NSA/CSS recently implemented procedures to change FLSA exemption status for non-exempt employees traveling outside the United States. However, we found that these procedures are ineffective in preventing incorrect payments because they are manually intensive and rely on Human Resources personnel to continuously monitor changing employee travel plans.

(U) **NSA/CSS FY2012 Compliance with 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 not fully compliant with IPERA for the second consecutive year.

(U) **Geospatial Analysis Tools**

(U//~~FOUO~~) The audit focused on determining which software applications NSA analysts use for geospatial analysis, how the applications are managed, and whether they meet customer requirements. The audit did not reveal reportable problems; however, [redacted] who responded to an OIG survey of analysts' satisfaction with NSA's geospatial tools. In addition, the [redacted] whose mission is to acquire, support, and maintain geospatial tools, does not manage and support two tools that NSA analysts use.

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

(U//~~FOUO~~) We tested security configuration controls for selected Agency servers for compliance with selected FISMA metrics. We found security vulnerabilities in the [redacted] The Agency is developing a Risk Management Framework through which it should formally assess and continuously monitor servers for the vulnerabilities identified.

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



Release: 2019-07
NSA:09296

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

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

### (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).

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

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

(U//~~FOUO~~) **UPDATE:** IT Policy has coordinated with Corporate Policy, Enterprise IT Implementation and Management, and the Unified Cross Domain Management Office (UCDMO) to develop draft Policy 6-8, *NSA/CSS Information Systems and Network Data and Software Transfers*. Originally due 30 November 2011, this action has a revised target completion date of March 2014.

(U//~~FOUO~~) In addition to

. Originally due 30 November 2011, these actions have a revised target completion date of December 2014.

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

### (U) Mission Assurance Continuity of Operations Compliance and Testing

(U//~~FOUO~~) In August 2008, NSA identified 14 mission-essential functions (MEFs) that must be performed in all circumstances. As of August 2009, Agency organizations had been identified as responsible for performing essential tasks that support one of more of the 14 MEFs.

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

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

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

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

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

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



Release: 2019-07
NSA:09297

(~~C//REL TO USA, FVEY~~) **Finding** [redacted] purchase 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)*, is under review by OGC. Once OGC comments have been received and adjudicated, the Technology Directorate (TD) plans to direct an Agency policy review. [redacted] anticipates publication of this policy by the end of second quarter FY2014. This action was due November 2011.

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

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

(U//~~FOUO~~) **UPDATE:** Draft NSA/CSS Policy 6-32 addresses incident response requirements for [redacted] purchases. [redacted] anticipates publication of this policy by the end of second quarter FY2014. This action was due September 2011.

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

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

(U//~~FOUO~~) The NC2 program [redacted] Since 2003, approximately 350 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 last report. This action was due December 2011.

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

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

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

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

(U//~~FOUO~~) TD management agreed to implement this recommendation by 30 September 2012. **UPDATE:** The Agency has made progress. By publishing NSA Policy 6-27, *Wireless Information Technology Systems*, 14 March 2013, the Agency has established the requisite controls, oversight, and policy to develop an Information Assurance wireless program.

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



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

Release: 2019-07
NSA:09298

## (U) Ongoing Audits

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

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

### (U) Conference Expenses

(U) The audit objective is to determine the extent of conference expenses and whether the Agency followed policies and regulations.

### (U) [redacted] Program

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

### (U) Small Business Program

(U//~~FOUO~~) The audit objective is to evaluate the controls over the Agency's small business program.

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

### (U) Network Enclave Management

(U) The audit objective is to determine whether Agency IT efficiency efforts will eliminate or reduce network enclaves and produce cost savings.

### (U) Intelink IT Security

(U) The audit objective is to determine whether the seven security deficiencies identified in the FY2011 Intelligence Community OIG FISMA audit are still present, now that NSA supports Intelink.

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

(U) The audit objective is to determine whether controls over the CPOFLD property accountability account ensure accuracy of the account.

### (U) Compliance with Public Law 111-258, "Reducing Overclassification Act"

(U) The audit objectives are to assess whether classification policies and procedures have been adopted and effectively administered and to identify policies and procedures that contribute to misclassification of material.

### (U) Vulnerability Tracking System

(U//~~FOUO~~) The audit objective is to determine whether Information Security (TS) retained system vulnerability documentation [redacted]

### (U//~~FOUO~~) Countering Denial and Deception

(U//~~FOUO~~) The audit objective is to determine the progress the Agency has made in implementing the Intelligence Community's strategy for countering denial and deception activities.

### (U) Suspension and Debarment Process

(U) The audit objective is to determine whether the Agency has effective procedures for referring cases of contractor misconduct for suspension and debarment.

### (U) FY2013 Compliance with FISMA

(U) The audit objective is to evaluate the Agency's information security program and practices in accordance with Office of Management and Budget guidance.

# (U) INSPECTIONS

## (U) Inspections Completed in the Reporting Period

**(U//~~FOUO~~) Inspection of NSA/CSS Representative to U.S. Southern Command (NCR SOUTHCOM)**

(U//~~FOUO~~) NCR SOUTHCOM is geographically separated: NCR SOUTHCOM and Cryptologic Services Group (CSG) SOUTHCOM are in Miami, and CSG Key West is in Key West. Lack of documentation at both locations creates concern about mission delegation and implementation of programs. NCR and CSG leadership in Miami and Key West have been innovative and creative in their approaches to mission and support to SOUTHCOM/Joint Inter-Agency Task Force-SOUTH but must follow up informal agreements on mission delegation and processes with documentation to ensure clear division of effort and compliance with authorities.

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

(~~C//REL TO USA, FVEY~~) NCEUR-AF has problems with aging facilities. Chief among these is insufficient air conditioning, which resulted in open windows and doors in the sensitive compartmented information facility (SCIF) for the physical comfort of the workforce. While cooling problems are being addressed incrementally as the NCEUR building in Stuttgart, Germany, is renovated, an interim solution was put in place as a result of the inspection to ensure that the SCIF is not vulnerable to electronic penetration.

(~~U//FOUO~~) Inspectors also found that [redacted] of the [redacted] vehicles in the NCEUR-AF Motor Pool at [redacted] did not meet the Department of Defense (DoD) utilization goals. Inspectors concluded that new efficiencies might be realized in vehicle fleet management. The OIG issued an advisory memorandum to all field sites instructing site chiefs to regularly review mileage utilization for all vehicles in their motor pools, in accordance with DoD Regulation 4500.36-R, *Management, Acquisition, and Use of Motor Vehicles*. [redacted] (b)(3)-P.L. 86-36

[redacted] (b)(1) (b)(3)-P.L. 86-36

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

(U//~~FOUO~~) The MOC is recognized by NSA/CSS organizations and external customers for providing excellent expeditionary SIGINT support through pre-deployment training, recruitment and deployment of analysts, and responsiveness to the information needs of tactical customers.

(~~S//REL TO USA, FVEY~~) However, the MOC faces challenges posed by [redacted] A timely corporate decision about [redacted] would enable more efficient staffing and space utilization for the MOC and NSA/CSS Washington.

(U//~~FOUO~~) The MOC inspection resulted in an OIG advisory memorandum on potential cost savings from stricter management of NSA tools in the field. Inspectors noted an excessive number and the wrong types of hand and power tools for the maintenance performed by site technicians.



Release: 2019-07
NSA:09301

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

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

(~~S//REL TO USA, FVEY~~) Although successful in accomplishing its mission of facilitating collaboration and providing SIGINT assistance to CIA components, the NCR CIA organization faces challenges to information sharing posed by IT problems and

(U//~~FOUO~~) Although the technical impediments to processing and sharing SIGINT information are being addressed, analysts expressed frustration with the lack of clear and readily accessible dissemination guidance from the Deputy Directorate for Customer Relations. Interviewees noted that decisions to share or disseminate information seem to be made case by case. Analysts are repeatedly required to seek answers to what they believe must be fairly common information-sharing questions. As a result, determining what and how to share seems subjective.

(U//~~FOUO~~) **Inspection of** (b)(3)-P.L. 86-36

(~~S//REL TO USA, FVEY~~) mission is to facilitate cryptologic relationships with the support U.S. military elements and national SIGINT customers and provide technical expertise and mission-enabling engineering support to

(~~S//REL TO USA, FVEY~~) Although employees expressed enthusiasm for working with they also expressed frustration with a perceived lack of clear vision to deepen collaboration with

(U//~~FOUO~~) faces challenges posed by insufficient enabler support, particularly in installations and logistics.

(~~S//REL TO USA, FVEY~~) **Inspection of**

(~~S//SI//REL TO USA, FVEY~~) mission is to provide and *ad hoc* support to U.S. military operations employees expressed frustration with

(~~S//SI//REL TO USA, FVEY~~) At the time of the inspection, was exploring other possibilities to occupy the workforce, including

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

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



Release: 2019-07
NSA:09302

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

(~~S//SI//REL TO USA, FVEY~~) Inspectors noted that the future mission and staffing for [redacted] should be determined as quickly as possible. In addition to the opportunity costs posed by the seemingly under-utilized personnel, the actual personnel costs are not insignificant.

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

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

## (U) Ongoing Inspections

(U) **Limited-Scope Joint Inspection Report, Navy Information Operations Command, Pensacola (NIOC-P)**

(U) The Inspections Division augmented the U.S. Fleet Cyber Command OIG from 22 to 26 October 2012 during an inspection of NIOC-P. A draft report is in progress.

(U) **Inspection of the NSA/CSS Representative to U.S. Strategic Command (NCR STRATCOM)**

(U) The Inspections Division conducted a field inspection of NCR STRATCOM from 5 through 9 November 2012. The final report is in coordination.

(U) **Joint Inspection of NSA/CSS Texas Cryptologic Center (NSAT)**

(U) The Inspections Division conducted a joint inspection of NSAT from 4 through 15 February 2013. A draft report is in coordination.

(U) **Inspection of the NSA/CSS Representative to the Federal Bureau of Investigation (NCR FBI)**

(U) The Inspections Division conducted a field inspection of NCR FBI from 11 through 22 March 2013. A draft report is in progress.



Release: 2019-07
NSA:09303

(U) This page intentionally left blank.



Release: 2019-07
NSA:09304

# (U) SPECIAL STUDIES

## (U) Special Studies Completed in the Reporting Period

(U) **Research Directorate's (RD) Compliance Program**

(U//~~FOUO~~) This study focused on the oversight that RD's Office of Compliance (RV) performs to ensure that SIGINT data is handled in accordance with NSA/CSS obligations to protect U.S. person privacy. Our review found that major requirements of RD's compliance program must be documented to ensure that RD personnel can reference IO policies and procedures and ensure the continuity of the RD/RV IO program. We also found that control enhancements are needed to monitor IO training for the RD workforce.

(U) **Advisory Report: [redacted] Compliance with NSA/CSS Authorities**

(U//~~FOUO~~) The review focused on implementation of SIGINT and information assurance policies and procedures within [redacted] a technology demonstration that uses cloud computing. Our review found that, because of the rapid [redacted] development cycle, controls on data ingestion and on [redacted] participants are implemented manually to comply with NSA/CSS authorities, leaving [redacted] compliance vulnerable to human error. These controls are not sustainable outside the tightly controlled [redacted] environment.

(U) [redacted]

(U//~~FOUO~~) The study found that [redacted] effectively satisfies most requirements and improves situational awareness. However, SIGINT will not always reliably warn of an attack in time to support actions that might [redacted]

(~~S//REL TO USA, FVEY~~) [redacted] is the unclassified name for [redacted] Its procedures [redacted]

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

(U//~~FOUO~~) NSA/CSS effectively oversees support to [redacted] However, improvements to mission management of [redacted] and [redacted] are needed.

(U//~~FOUO~~) NSA/CSS must engage combatant commanders to develop clear information needs and provide feedback on capability limitations. The current information need is overly broad and based on outdated [redacted] procedures.

(U) **Assessment of Management Controls Over FAA §702 – Revised and Reissued**

(U//~~FOUO~~) NSA/CSS operates under the authority of §702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA §702), a key source of information on foreign targets. For the Agency to retain this important tool, it must ensure compliance with FAA §702 targeting and minimization procedures. The original report, also published in the

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

reporting period, was revised because new information received after publication affected the findings.

(~~U//FOUO~~) Although the OIG did not discover non-compliance with the targeting and minimization procedures, we identified six areas in which controls over compliance with FAA §702 should be improved: assessment of performance against compliance standards, lack of [redacted] dissemination process, documentation deficiencies, automation, and training update and enforcement.

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

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

(U~~//FOUO~~) NSA's third-party partners are nations other than Australia, Canada, New Zealand, and the United Kingdom with which the U.S. government has national SIGINT arrangements. The purpose of the review was to determine whether policies and procedures are in place to ensure compliance with authorities for sharing [redacted] with third-party partners. [redacted]

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

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

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

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

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

(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 known to 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~~) Although we directed responsibility for this recommendation to SID, no NSA element is addressing system configuration management standards in accordance with NSA/CSS Policy 1-12. In December 2012, SID requested TD assistance in drafting a plan to baseline and document configuration system data. Without system configuration management documentation, NSA leadership has limited assurance that the systems are configured to retain and purge FISA data as legally required. Neither SID nor TD has provided a response.

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

## (U) Ongoing Special Studies

(U) **External Service Provider**

(U//~~FOUO~~) The study objective is to identify and assess compliance of NSA's external service provider with Intelligence Community policies and procedures for

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

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

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

(U//~~FOUO~~) The objectives of this study are to identify challenges in tracking and accounting for personnel in the extended enterprise and make recommendations to improve tracking and accountability in the field.

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

(U//~~FOUO~~) The objective of this study is to determine the accuracy and effectiveness of auditing control framework for analyst queries in SIGINT systems.

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

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

(U//~~FOUO~~) The objective of this review is to evaluate TD oversight activities to determine compliance with SIGINT and information assurance policies and procedures.

(U)

(U//~~FOUO~~) The objective of this study is to determine whether properly manages access to NSA-hosted data.

(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 activities comply with U.S. law and other directives.



Release: 2019-07
NSA:09307

(U) This page intentionally left blank.



Release: 2019-07
NSA:09308

# (U) INVESTIGATIONS

## (U) Summary of Prosecutions

(U//~~FOUO~~) In the reporting period, the OIG referred several cases to two Offices of the United States Attorney. The cases are under consideration. For example, the OIG received an anonymous complaint alleging that a contractor was running a personal business using government resources while billing a government contract. An OIG investigation into the allegation revealed that the subject had overcharged the government approximately $30,000. The case was referred to a United States Attorney for prosecution.

(U//~~FOUO~~) The OIG also investigated an allegation that an employee had a conflict of interest between his official government duties and his employment negotiations with an Agency contractor. The case was referred to a United States Attorney for criminal prosecution. Although the allegation against the subject, violation of Title 18 USC §208, Acts Affecting a Personal Financial Interest, was substantiated through an administrative investigation, the United States Attorney declined to prosecute. The subject resigned from government service in August 2009, and no further administrative action was sought.

## (U) Agency Referrals

(U//~~FOUO~~) The Investigations Division referred six investigations involving Agency employees to Employee Relations for disciplinary action. Fourteen investigations substantiating contractor misconduct were referred to the Contracting Office.

## (U) OIG Hotline Activity

(U//~~FOUO~~) The Investigations Division fielded 406 contacts through the OIG Hotline.

## (U) Investigations

(U//~~FOUO~~) Forty-eight investigations were opened and 49 were closed in the reporting period.

### (U) Significant investigation

(U) The OIG completed an investigation that resulted in the substantiation of multiple allegations against a Senior Executive assigned to the Agency.

(U//~~FOUO~~) In May 2011, the OIG received a complaint alleging that the Senior Executive was wasting Agency resources by conducting unnecessary official travel and using a government cellular telephone for personal communications and had failed to follow security procedures. The investigation did not substantiate the allegation of improper official travel but did determine that the subject had improperly used a government telephone, failed to protect the password to a classified computer system, and knowingly caused inaccurate travel vouchers and timesheets to be submitted, in violation of DoD 5500.07-R, *Joint Ethics Regulation*, and NSA/CSS policies.



Release: 2019-07
NSA:09309

The employee's misconduct resulted in improper receipt of approximately $1,500 in travel reimbursements and $2,000 in personal telephone calls and credit for 118 labor hours. The Final Report of Investigation was forwarded to Employee Relations, and administrative action is pending.

### (U) Contractor labor mischarging

(U//~~FOUO~~) The OIG opened five investigations into contractor labor mischarging during the reporting period. Eight cases of contractor labor mischarging were substantiated, resulting in the recovery of $251,000.

### (U) Time and attendance fraud

(U//~~FOUO~~) The OIG opened six investigations into employee time and attendance fraud and substantiated six existing cases. As a result of the investigations, three employees resigned from the Agency, one employee was suspended, and the OIG anticipates a monetary recoupment of $37,000 to the Agency. Administrative action against two employees is pending.

### (U) Computer misuse

(U//~~FOUO~~) The OIG opened 15 investigations involving allegations of computer misuse. During the reporting period, the OIG substantiated three cases of employee misuse of IT systems and substantiated contractor misuse in 11 cases. Cases substantiated against government employees were referred to Employee Relations for administrative action, and cases substantiated against contractors were referred to the Contracting Office.

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

## (U) Audits

(U) **Operations**

- (U) Key Management Infrastructure Program
- (U) Export Controls
- (U) Geospatial Analysis Tools

(U) **Finance**

- (U) Civilian Pay and Benefits
- (U) Fair Labor Standards Act Overtime Overpayments

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

(U) **Information Technology**

- (U) [redacted] Program
- (U) Human Resources Management System
- (U) Security System Testing of NSA/CSS Systems in Support of the Federal Information Security Management Act of 2002

## (U) Inspections

(U) **Field Inspections**

- (U) NSA/CSS Representative to U.S. Southern Command
- (U) NSA/CSS Europe and Africa
- (U) NSA/CSS Representative to the Central Intelligence Agency
- (U//~~FOUO~~) [redacted]
- (~~S//REL TO USA, FVEY~~) [redacted]

(U) **Joint Inspections**

- (U) Meade Operations Center

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

## (U) Special Studies

(U) **Information Technology**

- (U) [redacted] Compliance with NSA/CSS Authorities



Release: 2019-07
NSA:09311

(U) **Operations**

- (U) Research Directorate's Compliance Program
- (U) [redacted] (b)(3)-P.L. 86-36

(U) **Federal Compliance**

- (U) Assessment of Management Controls Over FAA §702



Release: 2019-07
NSA:09312

# (U) APPENDIX B
# AUDIT REPORTS WITH QUESTIONED COSTS

(U)

| Report | Number | Questioned Costs | Unsupported Costs |
|---|---|---|---|
| For which no management decision had been made by start of reporting period | 0 | 0 | 0 |
| Issued during reporting period | 0 | 0 | 0 |
| For which management decision was made during reporting period | 0 | 0 | 0 |
| Costs disallowed | 0 | 0 | 0 |
| Costs not disallowed | 0 | 0 | 0 |
| For which no management decision was made by end of reporting period | 0 | 0 | 0 |
| (U) Because 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)



Release: 2019-07
NSA:09313

(U) This page intentionally left blank.



Release: 2019-07
NSA:09314

# (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.



Release: 2019-07
NSA:09316

# (U) APPENDIX D
# RECOMMENDATIONS SUMMARY

(U//~~FOUO~~) The OIG made 422 recommendations to NSA management in reports issued in the first and second quarters of FY2013: 80 in the first and 342 in the second. During the first and second quarters, the Agency implemented 18 and 146 recommendations, respectively.

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

- (U) Follow-Up Inspection of NSA/CSS Accuracy in Aligning Military Joint Duty Assignments with Billet Specifications (24 January 2008)
- (~~C//REL TO USA, FVEY~~) Audit of the Agency's Third Party Infrastructure (18 December 2009)
- (U) Audit of Management of Agency's Firewalls (25 November 2009)
- (U) Joint Inspection of Alaska Mission Operations Center (8 October 2010)
- (U) Special Study of SIGINT Support to [redacted]
- (U) Audit of High-Performance Computing (14 October 2011)
- (U) Review of Restaurant Fund, CWF, and Museum Gift Shop (23 July 2012)
- (~~TS//SI//NF~~) [redacted]

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

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



Release: 2019-07
NSA:09317

(U) This page intentionally left blank.



Release: 2019-07
NSA:09318