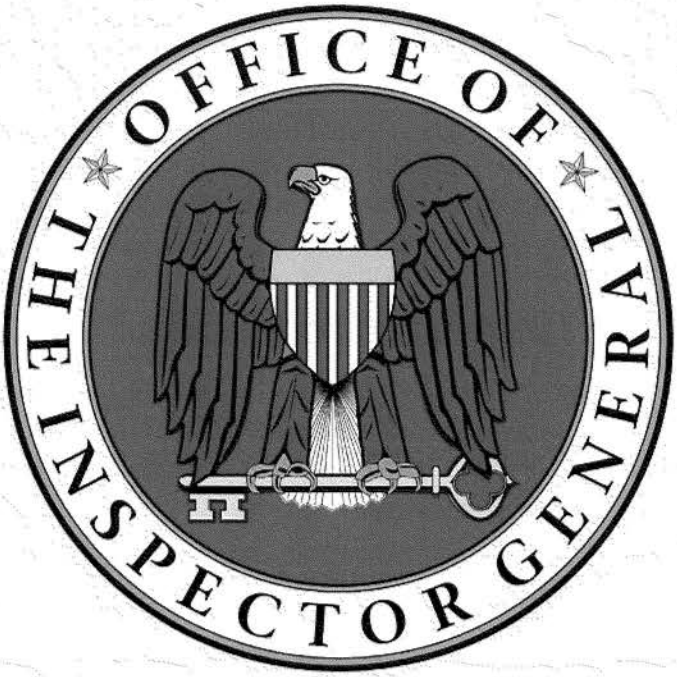
NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE



(U) SEMI-ANNUAL REPORT TO CONGRESS
1 October 2013 to 31 March 2014

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

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: ~~20390430~~

(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 October 2013 and 31 March 2014. The report is mandated by the Inspector General Act of 1978.

(U) During the reporting period, the NSA OIG completed 17 audits, inspections, and special studies.

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

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

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

(U) The Investigations Division fielded 398 contacts from the OIG Hotline. The team opened 58 investigations and closed 45 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 512 recommendations issued in the reporting period, 278 have been closed.

(U) In the last Semi-Annual Report to Congress, we reported that NSA had contracted with an independent public accounting firm (IPA) to audit the Agency's financial statements with OIG oversight and that the contract was under protest. The protest has been resolved, and the IPA was reinstated on 30 January 2014. As a result, the audit schedule has been compressed. The IPA is preparing to begin internal control testing.

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 DIR
ODNI 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
§5(a)(2)	Recommendations for corrective action	N/A
§5(a)(3)	Significant outstanding recommendations	2-4, 10
§5(a)(4)	Matters referred to prosecutorial authorities	12
§5(a)(5)	Information or assistance refused	N/A
§5(a)(6)	List of audit, inspection, and evaluation reports	14-15
§5(a)(7)	Summary of significant reports	N/A
§5(a)(8)	Audit reports with questioned costs	16
§5(a)(9)	Audit reports with funds that could be put to better use	17
§5(a)(10)	Summary of reports for which no management decision was made	N/A
§5(a)(11)	Significant revised management decisions	1
§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.

(U) Significant Revised Management Decisions

(U) No management decisions have been significantly revised.

(U) AUDITS

(U) Audits Completed in the Reporting Period

(U) **Audit of the Agency's System Vulnerability Tracking**

(U//~~FOUO~~) We reviewed the migration of plans of action and milestones (POA&Ms) from a legacy database to the new [redacted] database. We found a lack of consistency in the accounting and documentation of POA&M weaknesses identified and stored in the old database and later migrated to the [redacted] database. Risk Assessments & Authorization [redacted] reauthorizes systems [redacted] and plans to wait until the reauthorization to ensure that weaknesses in [redacted] are accurate and complete.

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

(U//~~FOUO~~) NSA contracted with an independent public accounting firm (IPA) to audit the financial statements of the NSA CWF for the years ending 30 September 2012 and 2011 and provide a report on internal control over financial reporting and compliance with laws and regulations. In its audit of the CWF, the IPA found a significant deficiency in internal controls on financial reporting. The IPA also found that the CWF financial statements were fairly presented, in all material respects, in conformity with U.S. Generally Accepted Accounting Principles, except for the effects of not capitalizing certain fixed assets.

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

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

(U//~~FOUO~~) The NSA/CSS FLIP program was established to encourage NSA civilian cryptologic personnel to acquire and maintain foreign language capabilities. Many multi-linguists are receiving FLIP even though they do not meet all requirements. Because of poor internal controls on FLIP, we found [redacted] of questionable costs. The Agency must improve its controls and policies to ensure the accurate disbursement of FLIP. The Agency must also implement controls to ensure the accuracy of test data in the Enterprise Learning Management database.

(U) Significant Outstanding Recommendations

(U) **Audit Report on 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. [redacted] 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, [redacted] insecurities had the potential to compromise national security.

(U) **Finding** 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 [redacted] insecurity database.

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

(U//~~FOUO~~) **UPDATE:** NSTISSI 4003 has been revised and is the new draft CNSSI No. 4003; formal issuance is anticipated in May 2014. NSA/CSS Policy Manual 3-16 can now be updated and is expected to be finalized in 60 days. The COMSEC incident reporting system was developed and has been operational on SIPRNet since January 2012, and IAD's insecurities analysts are independently investigating insecurities at all levels of government. The recommendation was originally due to be resolved by 28 September 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).

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

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

(U//~~FOUO~~) **UPDATE:** The which includes has been in development and testing since 2010 and has now achieved initial operational capability. This recommendation was originally due to be resolved by 30 November 2011.

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

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

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

(~~C//REL TO USA, FVEY~~) **Finding** purchase controls

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

(U//~~FOUO~~) **UPDATE:** Draft NSA/CSS Policy 6-32, *NSA/CSS Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)*, is awaiting final signatures and is expected to be published by 31 July 2014. This recommendation was originally due to be resolved by November 2011.

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

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

(U) **UPDATE:** The incident response process that will be satisfied when revised NSA/CSS Policy 6-32 has been implemented. The policy is awaiting final signatures and is expected to be published by 31 July 2014. This recommendation was originally due to be resolved by September 2011.

(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 2013 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 have developed with previously closed recommendations.

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

(U~~//FOUO~~) **UPDATE:** A high-level requirements document and a POA&M document have been created, and discussions were held to identify possible mission assurance sites. A cost estimate has been completed with an estimate of approximately [redacted] Analysis of alternatives and a schedule and strategy to engage in the FY2016 budget cycle must be completed. This recommendation was originally due to be resolved by December 2011.

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

(U) Ongoing Audits

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

(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 Intelligence Community Whistleblower Protection Act of 1998. 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 contractors ADET training.

(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 complies with DoD and Agency guidance and has implemented corrective actions to satisfy previous recommendations.

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

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

(U) **Oversight of the Restaurant Fund and Civilian Welfare Fund**

(U) The audit objective is to ensure that the audit of the Restaurant Fund and the CWF for FY2013 by an independent public accounting firm accords with government auditing standards. We will also assist the contracting officer by closely monitoring the auditors and providing technical guidance in accordance with the contract.

(U) **NSANet Server Security**

(U~~//FOUO~~) The audit 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.

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

(U) INSPECTIONS

(U) Inspections Completed in the Reporting Period

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

(U~~//FOUO~~) The OIGs of NSA/CSS, Army Intelligence and Security Command (INSCOM), and the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA) jointly inspected NSAT.

(U~~//FOUO~~) NSAT faces challenges posed by [redacted] Most of NSAT's workforce is [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 special challenges. NSAT [redacted] Of particular concern to service leaders were [redacted] Each service is left to make arrangements for these individuals [redacted]

(U) **Limited-Scope Field Inspection of the [redacted]**

(U~~//FOUO~~) This was the first inspection of the [redacted] which began operation in 2007. [redacted] The limited-scope inspection focused on intelligence oversight, IT and communications, financial processes, property accountability practices, safety, security, facilities, and emergency management.

(U~~//FOUO~~) Areas in particular need of increased attention at [redacted] are property accountability and property management procedures and emergency action and continuity of operations planning.

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

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

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

(U~~//FOUO~~) **Limited-Scope Field Inspection of [redacted]**

(U~~//FOUO~~) We conducted this inspection at the request of SIGINT Directorate leadership. The inspection team found support agreements; acquisition, contract oversight, TEMPEST, and

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

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

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

COMSEC compliant with the governing standards. However, the [redacted] could be improved.

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

(U//~~FOUO~~) The NSA/CSS and INSCOM OIGs conducted a joint follow-up inspection of [redacted] communications and computers functional area to review corrections made to satisfy recommendations from a July 2011 joint inspection and to inspect the state of [redacted]

(U//~~FOUO~~) The state of the [redacted] functional areas has greatly improved since the 2011 inspection. However, several problem areas found during the follow-up inspection still require attention.

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

(S//SI//~~REL TO USA, FVEY~~) This was the first inspection of [redacted] headquarters since its inception in [redacted] Although the inspection team heard only praise for [redacted] mission accomplishments, [redacted] faces challenges of rapidly evolving technology, ensuring that the equities of all stakeholders are appropriately considered as [redacted] evolves in response to advances in technology, Intelligence Community requirements, and new technical and operational paradigms at the parent agencies. [redacted] leadership must take the lead to formally document and maintain records on agreements that significantly change the [redacted] mission, including updating the [redacted] Terms of Reference to reflect its current role and activity in the [redacted]

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

(U) Significant Outstanding Recommendations

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

(U) Ongoing Inspections

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

(U//~~FOUO~~) The Inspections Division and INSCOM conducted a joint inspection of [redacted] The final report is in coordination.

(U) **Field Inspection of NSA/CSS Representative to the United States Special Operations Command (NCR SOCOM)**

(U//~~FOUO~~) The Inspections Division conducted a field inspection of NCR SOCOM from 28 October to 19 November 2013. The final report is in coordination.

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

(U//~~FOUO~~) The Inspections Division, INSCOM, Fleet Cyber Command, and AFISRA conducted a joint inspection of NSAG from 2 to 14 March 2014. The working draft report is in coordination.

(U) SPECIAL STUDIES

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

(U) Special Studies Completed in the Reporting Period

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

(U//~~FOUO~~) We studied [redacted] 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 [redacted] auditing control framework.

(U) **Technology Directorate (TD) 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 reliably and verifiably follow 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 do not meet NSA/CSS 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 of improper handling of NSA mission data. Recent compliance incidents validate our concerns.

(~~S//NF~~) **Management Controls for the FAA §702** [redacted]

(~~S//SI//NF~~) [redacted]

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

~~(S//NF)~~ The OIG concluded that the management controls implemented for the [redacted] provided sufficient assurance of compliance with the governing documents. We identified no findings in the study and made no recommendations to management.

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

(U//~~FOUO~~) IV, a directorate compliance component, is tasked with providing the IAD Director with reasonable assurance that IAD personnel reliably and verifiably follow the legal authorities and policies affecting U.S. person privacy and mission compliance. Our review uncovered weaknesses in policies, procedures, internal controls, incident reporting, monitoring of programs and processes, and IO training. During its short life span, IV has had a high rate of turnover of personnel with experience in policy, oversight, and compliance, including its first Chief. IAD managers understand the importance of oversight and compliance and are committed to making changes necessary to ensure a robust oversight and compliance program throughout IAD.

(U//~~FOUO~~) We identified areas in which IAD can strengthen controls to ensure compliance: developing policy and guidance to establish standards and accountability, conducting and documenting compliance reviews, and enforcing and monitoring mission compliance and IO training.

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

(~~TS//SI//NF~~) [redacted]

(~~TS//SI//REL TO USA, FVEY~~) We made seven recommendations to [redacted] and four to [redacted] many of which were closed before report publication.

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

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

(~~TS//SI//REL TO USA, FVEY~~) We made four recommendations to [redacted] and one to [redacted]

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

(U) **Annual FAA §702 Report to Congress**

~~(S//NF)~~ By statute, this report details the Agency's compliance with FAA §702 and describes incidents of non-compliance with procedures for targeting non-U.S. persons outside the United States and incidents involving minimization of U.S. person information. For the 12-month period ending 31 August 2013, the OIG completed two reports on implementation of FAA §702. In compliance with the targeting and minimization procedures of FAA §702, NSA/CSS [redacted] disseminated [redacted] intelligence reports.

(U//~~FOUO~~) **Advisory Report on Concerns about** [redacted]

~~(S//REL TO USA, FVEY)~~ The National Reconnaissance Office (NRO) OIG and the NSA/CSS OIG conducted a joint review to assess [redacted]

(U//~~FOUO~~) This joint review resulted in two reports. The NSA OIG advisory report focused primarily on concerns about [redacted] based on NSA/CSS OIG data collection.

(U//~~FOUO~~) Our survey found mixed assessments of [redacted] and the effectiveness of processes to address [redacted] These inconsistencies and the broad reach of [redacted] data to customers worldwide [redacted]

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

(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.

(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] 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 due to be resolved by 30 September 2008.

(U) Ongoing Special Studies

(U//~~FOUO~~) **Cybersecurity: Integrating Dual SIGINT and Information Assurance (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 cybersecurity

mission regarding [redacted] information 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 (IDA)**

(U//~~FOUO~~) The objective of this review is to determine whether controls established by the Agency, in conjunction with IDA, ensure compliance with Executive Order 12333 and all laws and policies for [redacted]

(U//~~FOUO~~) [redacted] **Program Compliance with Signals Intelligence Policies and Procedures**

(U//~~FOUO~~) The objective of this study is to evaluate the [redacted] program's compliance with signals intelligence policies and procedures on collection, processing, retention, minimization, and dissemination of U.S. person information.

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

(U//~~FOUO~~) The objective of this study (requested by eight members of the Senate Judiciary Committee) is to describe how data is collected, stored, analyzed, disseminated, and retained under §215 and §702 authorities in effect in 2013, the steps taken to protect U.S. person information, the restrictions on using the data and how the restrictions are implemented, what has contributed to non-compliance incidents, what NSA has done to minimize recurrence, how analysts use the data to support their intelligence missions, and the oversight and compliance activities performed by the 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) INVESTIGATIONS

(U) Summary of Prosecutions

(U) One case prosecuted during the reporting period (see "Significant Investigations" section).

(U) Agency Referrals

(U//~~FOUO~~) The Division referred 16 investigations involving Agency personnel to Employee Relations (ER) for disciplinary action. One employee was dismissed from the Agency, one employee received a suspension, two employees received written reprimands, and disciplinary action is pending against 12 employees.

(U//~~FOUO~~) Fourteen investigations substantiating contractor misconduct were referred to the Maryland Procurement Office for action, resulting in the proposed recoupment of more than $160,000.

(U) OIG Hotline Activity

(U//~~FOUO~~) The Investigations Division fielded 398 contacts through the OIG Hotline.

(U) Significant Investigations

(U) Potential criminal activity

(U//~~FOUO~~) The OIG substantiated an allegation that senior leadership of an NSA/CSS organization failed to report potential criminal activities discovered by subordinate team members during the course of their assigned duties.

(U//~~FOUO~~) The NSA Red Team emulates adversary activity to assess the IT security of DoD and the federal government. As part of an assessment for the [redacted] the Red Team conducted an electronic vulnerability survey of a U.S. military information system in 2011. The team was able to compromise and access data from a senior official's unclassified computer and discovered evidence of possible criminal activity in the computer accounts belonging to the official. Red Team senior leadership decided not to disseminate a report. The OIG investigation concluded that leadership failed to comply with standard operating procedures that require a report of potential criminal activity.

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

(U) Misuse of a SIGINT system

(U//~~FOUO~~) The OIG substantiated an allegation that a U.S. Navy sailor deliberately and without authorization misused a SIGINT system.

(U//~~FOUO~~) After an audit of the SIGINT system, it was determined that the sailor used the system to query a telephone number belonging to a U.S. person. Although no information had been retrieved through the query, the subject violated Executive Order 12333, *United States Intelligence*

Activities, U.S. Signals Intelligence Directive SP0018, *United States Signals Intelligence Directive*, DoD Directive 5240.1-R, *Legal Compliance and U.S. Persons Minimization Procedures*, and 5 C.F.R. §2635.704, *Standards of Conduct for the Executive Branch*. A Navy Criminal Investigative Service investigation is pending.

(U) Misuse of government resources and labor mischarging

(U//~~FOUO~~) In April 2012, the OIG received an anonymous complaint alleging misuse of government resources and labor mischarging by an NSA contractor assigned to NSA Georgia. The investigation identified more than $61,000 in fraudulent labor charges. The contractor was removed from NSA access in October 2012, and the case was referred to the Office of the U.S. Attorney for the Southern District of Georgia in April 2013 and accepted for prosecution. In November 2013, the subject entered a guilty plea to one felony count of making false statements. The subject faces a maximum penalty of five years imprisonment and a $250,000 fine. The Court can also order the subject to pay $62,000 in restitution; she has already paid $10,000.

(U) Investigations

(U//~~FOUO~~) Fifty-eight investigations were opened and 45 were closed in the reporting period.

(U) Contractor labor mischarging

(U//~~FOUO~~) During the reporting period, the OIG opened two contractor labor mischarging investigations and substantiated two cases. The two closed cases resulted in the proposed recoupment of more than $159,000. Twelve investigations remain open.

(U) Time and attendance fraud

(U//~~FOUO~~) During the reporting period, the OIG opened eight investigations into employee time and attendance fraud. The OIG substantiated six cases, which resulted in one employee's dismissal from the Agency and the proposed recoupment of $37,000. Action against the remaining five employees is pending. Nine time and attendance investigations remain open.

(U) Computer misuse

(U//~~FOUO~~) During the reporting period, the OIG opened 11 investigations of allegations of computer misuse by three employees and eight contractors. The OIG substantiated one case of employee misuse of IT systems and substantiated 13 cases of contractor misuse. The case substantiated against the government employee was referred to ER and resulted in the employee receiving a written reprimand. The remaining case involved a contractor using NSA/CSS resources in support of a U.S. Air Force contract. The results of this investigation were referred to a USAF contracting officer.

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

(U) Audits

(U) Operations and Support

- (U) Foreign Language Incentive Pay

(U) Information Technology

- (U) Audit of the Agency's System Vulnerability Tracking

(U) Financial

- (U) Oversight Review of the Civilian Welfare Fund

(U) Inspections

(U) Field Inspections

- (U) Limited-Scope Inspection of the
- (U) Limited-Scope Inspection of

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

(U) Joint Inspections

- (U) NSA/CSS Texas Cryptologic Center
- (U)
- (U//~~FOUO~~) Follow-Up Inspection of the
- (U)

(U) Special Studies

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

(U) Operations

- (U//~~FOUO~~) Auditing Control Framework for Analyst Queries of SIGINT System Databases
- (U) The Technology Directorate Mission Compliance Program
- (~~S//NF~~) Management Controls for the FAA §702
- (U) Information Assurance Directorate Office of Oversight and Compliance Mission Compliance Program
- (~~TS//SI//REL TO USA, FVEY~~)

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

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

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

(U) **Information Technology**

- (U) Advisory Report on Concerns about Data Quality

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

(U) **Federal Compliance**

- (U) Annual FAA §702 Report to Congress

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

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

(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) APPENDIX D
RECOMMENDATIONS SUMMARY

(U//~~FOUO~~) The OIG made 512 recommendations to NSA management in reports issued in the first and second quarters of FY2014: 280 in the first and 232 in the second. During the first and second quarters, the Agency implemented 237 and 205 recommendations, respectively.

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

- (U) Inspection of the Corporate Communications Strategy Group (27 September 2006)
- (U//~~FOUO~~) Joint Inspection of Menwith Hill Station (13 September 2007)
- (U) Audit of the Agency's Transition to Internet Protocol Version 6 (29 March 2008)
- (U) Audit of [redacted] on the Agency's Unclassified Network [redacted]
- (U) Audit of Mission Assurance – Continuity of Operations Compliance and Testing (17 August 2010)
- (U) Review of Data Sharing with Third-Party Partners (20 September 2010)
- (U) Audit of the [redacted]
- (U) Joint Inspection of NSA/CSS Representative to U.S. Central Command (4 March 2011)
- (U) Audit of NSA Police (9 May 2011)
- (U) Audit of the Agency's Wireless Networks and Devices (22 November 2011)
- (U) Audit of the Government Purchase Card Program (10 September 2012)
- (U) Special Study of [redacted]
- (U//~~FOUO~~) Joint Inspection of Aerospace Data Facility Colorado (11 September 2012)
- (U) Audit of Fair Labor Standards Act Overtime Payments (21 March 2013)
- (U) Limited-Scope Field Inspection of Navy Information Operations Command Pensacola (12 April 2013)
- (U) Special Study of the External Service Provider's [redacted] (1 May 2013)
- (U) Audit of the Agency's Small Business Program (10 May 2013)
- (U) Audit of the Agency's Suspension and Debarment Process (26 September 2013)

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

(U) This page intentionally left blank.

blank page