

# (U) SEMIANNUAL REPORT TO THE CONGRESS

(U) *For the Period April 1, 2009 through September 30, 2009*

(U//~~FOUO~~) **Foreign Language Incentive Pay Program**; NSA/CSS IG; ST-09-0005;  
13 May 2009

(U//~~FOUO~~) **Summary** A special study found that the Foreign Language Incentive Pay (FLIP) program does not always meet its goals of encouraging civilian Language Analysts (LA) to acquire and maintain language skills and influencing them to remain in language analysis positions.

[redacted] Since the implementation of the Defense Language Proficiency Test (DLPT) [redacted] the DoD standard, language readiness for [redacted] for which the [redacted] is the test of record, [redacted]

[redacted] the Agency's investment in the FLIP program, which increased from [redacted] in FY06 to [redacted] in FY07. Although the annual FLIP validation process is working well, FLIP management controls are weak.

(U) **Management Action** The NSA CoS has begun to take action on the recommendation for a program review in which the Signals Intelligence Directorate will participate.

(U) **Overall Report Classification** SECRET//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

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

(U//~~FOUO~~) **NSA/CSS Texas**; NSA/CSS IG; AFISRA IG; INSCOM IG; NNWC IG;  
JT-09-0002; 1 July 2009

(S//~~REL TO USA, FVEY~~) **Summary** The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency, Intelligence and Security Command, Naval Network Warfare Command, and NSA inspected NSA/CSS Texas (NSAT). Since a 2006 inspection, NSAT has taken on additional global missions such as [redacted]

[redacted], while broadening the scope of others, including [redacted] and Customer Relations.

Several responsibilities, such [redacted] have transferred to other sites. Key points from the inspection include: 1) NSA HQ/Signals Intelligence Directorate has delegated mission to NSAT [redacted] 2) NSAT leadership has been effective in [redacted]

(U) **Management Action** Management concurred with all recommendations and corrective actions are underway.

(U) **Overall Report Classification** TOP SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

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

Approved for Release by NSA on 07-01-2019,  
FOIA Case # 79825 (litigation)

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~20320108~~

Release: 2019-06  
NSA:08893

~~SECRET//REL TO USA, FVEY~~

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

(U) **Interim Report of NSA/CSS on Mission Assurance**; NSA/CSS IG; IN-09-0003;  
8 July 2009

~~(S//REL TO USA, FVEY)~~ **Summary** The OIG's inspection of mission assurance provided background on implementation of the mission assurance policy objectives and addressed the organizational placement of the Agency's Enterprise Mission Assurance (EMA) function. Placement of EMA within the [redacted] is inconsistent with EMA's corporate responsibilities outlined in NSA/CSS Policy 1-4, *Mission Assurance* (1 February 2006). The consensus among the senior leaders was that [redacted] would be a more appropriate site for EMA [redacted]. The inspection also found that some progress has been made on several Policy 1-4 objectives; however,

[redacted]

(U//FOUO) **Management Action** EMA was transferred [redacted] EMA [redacted] will continue to collaborate with the Technology Directorate to [redacted] and embed mission assurance principles in governance, planning, and acquisition programs. The goal of both organizations is to ensure that the nation's SIGINT and Information Assurance missions will continue to operate through any disruption.

(U) **Overall Report Classification** SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

~~(S)~~ **OIG Inquiry into the Red Team [redacted] Incident**; NSA/CSS IG;

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

~~(S//REL)~~ **Summary** The objectives of the inquiry were to establish the facts surrounding the incident, evaluate responsibility, and assess compliance with internal controls and their adequacy for preventing future incidents. The inquiry found that Red Team controls were not adequate to prevent the human errors [redacted]

[redacted]

[redacted] had discontinued the [redacted] when problems became evident. Poor communication between Red Teams and with Red Team Operations Management contributed to the incidents. Although human error caused the [redacted] Red Team managers are responsible for the control environment in which the errors occurred.

~~(S//REL)~~ **Management Action** In response to our inquiry, Red Teams stopped [redacted] pending approval to resume, stopped operations, and removed Red Team personnel from [redacted] to ensure data integrity. Red Team management updated training processes and materials and conducted a training "stand-down" to ensure that all employees understood Standard Operating Procedures and policies. Red Team management is re-emphasizing and clarifying responsibilities to minimize the likelihood of recurrence. Information Assurance Directorate management concurs with the findings and has begun corrective action.

~~SECRET//REL TO USA, FVEY~~

(U) Overall Report Classification SECRET//REL TO USA, FVEY

(U) Category Information Security and Privacy

~~(U//FOUO)~~ **FY2009 Audit Report on Compliance with the Federal Information Security Management Act at NSA/CSS**; NSA/CSS IG; AU-09-00011; 24 July 2009

~~(U//FOUO)~~ **Summary** The Agency's emerging mission in the Comprehensive National Cybersecurity Initiative (CNCI) depends, in part, on the Agency's ability to protect its systems and networks. The Federal Information Security Management Act (FISMA) measures the adequacy and effectiveness of the information security environment upon which this emerging mission is based. The FY2009 FISMA Report records the progress the Agency has made in strengthening information technology (IT) security processes and in tracking Agency-wide and system deficiencies. However, more work must be done to correct the material weakness reported in August 2006 regarding [redacted]

[redacted] the NSA/CSS Information Systems Incident Response Team developed a formal follow-up system for [redacted] and Contractor Accreditations and Inspections continues to meet a self-initiated goal of [redacted]

(U) **Management Action** Management concurred with all recommendations, and corrective actions are underway.

(U) Overall Report Classification TOP SECRET//COMINT//NOFORN

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

(U) Category Information Security and Privacy

~~(U//FOUO)~~ **Audit of Associate Directorate for Education and Training Information Technology Infrastructure Problems**; NSA/CSS IG; AU-09-0019; 28 July 2009.

~~(U//FOUO)~~ **Summary** The principal audit objective was to determine whether the Associate Directorate for Education and Training (ADET) IT servers are adequately controlled and operated in accordance with guidelines, policies, and regulations. [redacted] ADET experienced a significant server crash when [redacted]

[redacted] The audit found that [redacted] contributed to this problem. The incident highlighted the need for ADET to bring the [redacted] into compliance with the certification and accreditation process.

~~(U//FOUO)~~ **Management Action** Action is underway to rebuild and restore approximately [redacted] web pages and [redacted] applications that were lost at an estimated cost of [redacted]. To facilitate improvements in the VUport infrastructure, ADET has requested the expertise of the Technology Directorate (TD) and is considering transferring its systems management to TD. The OIG recommended that ADET ensure that [redacted] comply with the certification and accreditation process. ADET agreed to do so by 30 September 2009.

(U) Overall Report Classification TOP SECRET//COMINT/TALENT KEYHOLE//REL TO USA, FVEY

(U) Category Information Security and Privacy

(U//~~FOUO~~) Advisory Audit Report on Strengthening Contract Administration to Protect Agency Resources; NSA/CSS IG; AU-09-0001; 6 August 2009

(U//~~FOUO~~) Summary Contract administration has been a longstanding problem at NSA. Over the last decade, the OIG reported contract administration problems in 65 audit, investigation, and inspection reports. Yet deficiencies addressed in one report almost invariably recur in the next. These deficiencies included inadequate invoice certification, out-of-scope work, award fee contract administration deficiencies, and other oversight concerns. These weaknesses were caused by inadequate training, over-reliance on contractors, and failure to follow policies and procedures. A powerful example of the consequences of poor contract administration can be seen in the OIG's ongoing effort to uncover contract labor mischarging. To date, recoveries from fraudulent billings or out-of-scope work exceed \$1.4 million. The advisory audit found that, although recent initiatives to address staffing shortages and reform policies have produced some improvement, the Agency must develop a comprehensive and consistent approach to correct these deficiencies. Contracting Officers and contracting specialists reported in two OIG surveys that they do not have time to perform contract administration adequately. The OIG proposed that the Senior Acquisition Executive with the Senior Leadership Team establish a contract administration process within the Directorate of Acquisition to provide adequate contract management, including oversight of Contracting Officer's Representatives.

(U) Overall Report Classification SECRET//REL TO USA, FVEY

(U) Category Acquisition Processes and Contract Management

(U//~~FOUO~~) Report of Investigation Regarding Alleged Improprieties at NSA Georgia; NSA/CSS IG; IV-09-0003; 14 August 2009

(U//~~FOUO~~) Summary A former Navy linguist [redacted] at NSA/CSS Georgia (NSAG) from 2004 until 2007 alleged that the [redacted] program at NSAG had unlawfully intercepted and processed U.S. person communications. [redacted]

[redacted]

~~(S//REL TO USA, FVEY)~~ The OIG found no targeting of U.S. persons by [redacted]. The investigation involved [redacted] interviews of the complainant, more than [redacted] witness interviews, [redacted] and the forensic analysis of [redacted] records. Analysis showed that [redacted] handled approximately [redacted] during the period the complainant's allegation covered (2004-2005) and that [redacted] (.022 percent) [redacted] were incidentally collected U.S. communications. [redacted]

[redacted] Incidental collection of U.S. person communications is a by-product of collection against legitimate foreign targets. The forensic data and relevant testimony showed that [redacted] personnel handled incidentally collected U.S. person communications in accordance [redacted]

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

(b) (3) - P.L. 86-36  
Release: 2019-06  
NSA:08896

with USSID SP0018, marking and deleting them as appropriate.

(U//FOUO) The complainant also alleged that, solely for entertainment purposes, [redacted] had shared [redacted]. The OIG found no merit to this allegation. [redacted]

(U//FOUO) The complainant also made two allegations regarding unlawful activity involving [redacted]

[redacted] The OIG investigation determined that these allegations were without merit.

(U) Overall Report Classification TOP SECRET//COMINT//NOFORN

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

(U) Category Questionable Activities

(U) NSA/CSS Commercial Solutions Center; NSA/CSS IG; IN-09-0002; 27 August 2009

(U//FOUO) Summary The NSA/CSS Commercial Solutions Center (NCSC) is meeting its customers' needs and succeeding in its role as the NSA front door for industry partners. Overall, NCSC [redacted]

[redacted] The NCSC has adequate information to manage its annual budget and predict anticipated funds for the following year. Some senior Agency leadership, especially from the Signals Intelligence Directorate (SID), believe that the NCSC would be more effective if its functions were moved into SID. The OIG inspection found no evidence to support this assertion. Although NCSC is achieving its mission well, the inspection revealed the need for: 1) comprehensive training for platform managers, whose role is critical to NCSC success, 2) an overarching acquisition strategy for Consolidated Cryptologic Program procurements that exceed [redacted] and 3) changes to the current Issue Resolution Process to ensure compliance with NSA/CSS Policy 3-13 guidance to disseminate information technology vulnerability alerts quickly.

(U) Management Action NCSC and SID management concurred on the recommendations.

(U) Overall Report Classification TOP SECRET//COMINT//REL TO USA, FVEY

(U) Category Acquisition Processes and Contract Management

(U) [redacted] NSA/CSS IG; IN-09-0005;

(S//REL TO USA, FVEY) Summary The inspection found that the [redacted] suffers from lack of strategic direction because of uncertainty surrounding [redacted]. The site's motivated workforce and strong leadership need [redacted] to achieve the [redacted] full potential [redacted]. The inspection revealed [redacted]

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

(b) (1)  
(b) Release 2019-08 6-36  
NSA-08897



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

~~SECRET//REL TO USA, FVEY~~

management controls in need of improvement. The current NSA/CSS [redacted] [redacted] The site's resource alignment must be evaluated regularly in light of the disappointing results. The site lacks a vetting process and tracking system to oversee its requests.

(U) **Management Action** [redacted] and associated Agency elements concurred on all recommendations and are taking corrective action.

(U) **Overall Report Classification** SECRET//COMINT//NOFORN

(U) **Category** Joint Warfighting and Readiness

(U) **Federally Funded Research and Development Center – Institute for Defense Analyses**; NSA/CSS IG; AU-08-0008; 16 September 2009

(U//~~FOUO~~) **Summary** The principal audit objective was to determine whether the Institute for Defense Analyses (IDA) contract is being administered effectively and in compliance with contracting and information systems security policies and procedures. The long term research partnership with IDA has yielded many Signals Intelligence and Information Assurance successes. However, our audit found that [redacted]

[redacted]

Officer's Representative is also needed to determine compliance with contracts, effectiveness of internal controls, and the cost efficiency of operations.

(U) **Management Action** The Technology and Acquisition Directorates, in conjunction with the Office of Mathematics Research Contracting Officer Representative, has initiated action on all OIG recommendations.

(U) **Overall Report Classification** TOP SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Acquisition Processes and Contract Management

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

(U//~~FOUO~~) [redacted] NSA/CSS IG; AFISRA IG; INSCOM IG; NNWC IG; [redacted] 16 September 2009

~~(S//REL TO USA, FVEY)~~ **Summary** The Inspectors General from the National Security Agency, Air Force Intelligence, Surveillance and Reconnaissance Agency, Army Intelligence and Security Command, and Naval Network Warfare Command conducted a joint inspection of the [redacted] which is jointly managed and has been an exemplar of First and Second Party mission partner collaboration [redacted]. The diversity of the mission partners working with full knowledge of all missions at [redacted] is both a strength and a burden. This [redacted] environment is key to the superior collaboration at site, but it is cumbersome when sharable information and tools reside on NOFORN and other systems. Personnel external to the site must be educated to understand site restrictions and proper classification to enable tools and information sharing. [redacted]

[redacted]

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

~~SECRET//REL TO USA, FVEY~~

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

~~SECRET//REL TO USA, FVEY~~



(U) **Management Action** Management concurred with all recommendations, and corrective actions are underway.

(U) **Overall Report Classification** SECRET//COMINT//TALENT KEYHOLE//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

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

(U) **Follow-up Audit of Contractor Space**; NSA/CSS IG; AU-08-0020; 30 September 2009

(U//~~FOUO~~) **Summary** Since 2003, NSA has tried unsuccessfully to alleviate chronic shortages of space by targeting increasing use of government space by contractors. The effort included contractor relocation, a restrictive contractor occupancy policy, and industry sponsored facilities. Although recommendations from a 2004 audit have been implemented, management of contractor space remains a significant problem. Our follow-up audit



(U) **Management Action** Management concurred with all recommendations.

(U) **Overall Report Classification** SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Human Capital

(U) **False Contractor Labor Claims**; NSA/CSS IG; IV-07-0031, IV-08-0016, IV-08-0017, IV-08-0018, IV-08-0019; 13 March 2009 – 12 August 2009

(U//~~FOUO~~) **Summary** Between 2004 and 2007, five contractors working the midnight shift on an Agency in-house contract submitted false and inaccurate timesheets to their companies. All five took days off and covered for each other, while claiming 8-hour shifts on their timesheets. Since they were working on a time and materials contract, the government was over-billed approximately \$116,000 as a result of this fraud. All the contractors have left their companies and no longer work on NSA contracts. The most egregious offender pled guilty to three counts of violating 18 U.S.C. Section 1001 (False Statements) and was sentenced to 30 days in prison and two years supervised release. The individual was also ordered to pay restitution of nearly \$75,000.

(U) **Management Action** The Office of Contracting and the prime contractor have been notified of the results of the investigation to facilitate monetary recovery.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

~~SECRET//REL TO USA, FVEY~~

~~SECRET//REL TO USA, FVEY~~

(U) **Category** Other (Procurement and Contract Administration)

(U) **Time Card Fraud**; NSA/CSS IG; IV-08-0004; 1 September 2009

(U//~~FOUO~~) **Summary** A GG-14 employee knowingly submitted falsified time sheets from August 2006 to January 2008 for a shortfall to the Government of 615.25 hours (approximately \$34,059).

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Standards of Conduct)

(U) **Procurement Fraud Initiative**; NSA/CSS IG; Several Control Numbers; 1 April 2009 to 30 September 2009

(U//~~FOUO~~) **IV-09-0015** A contractor employee fraudulently billed the government 525 hours (approximately \$58,000) over 14 months for late arrivals, early departures, and long lunches. The employee was terminated by the contractor during our investigation.

(U//~~FOUO~~) **IV-09-0024** A major contractor has a policy which directs employees to bill indirect time "under 59 minutes" to contracts instead of overhead. The OIG is coordinating a review with DCAA regarding this practice. The practice was discovered during an investigation of an employee who had billed Agency contracts 57 hours over 12 months for "overhead activities," such as reading company email or completing timesheets.

(U//~~FOUO~~) **IV-09-0026** A contractor employee fraudulently billed the government 117.5 hours (approximately \$14,000) over 12 months.

(U//~~FOUO~~) **IV-09-0031** A contractor employee fraudulently billed the government 502 hours (approximately \$85,000) over 19 months.

(U//~~FOUO~~) The OIG is continuing to investigate mischarging at cryptologic centers. Ten investigations are open for contract labor mischarging at the Hawaii site. The initial estimate of mischarging for these employees is almost \$400,000.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Procurement and Contract Administration)

~~SECRET//REL TO USA, FVEY~~



~~SECRET//REL TO USA, FVEY~~

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

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

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U//FOUO) [redacted] NSA/CSS IG; [redacted]

~~(S//REL)~~ Summary The inspection of the [redacted] is organized and managed to fulfill its mission requirements with few impediments. Its services are sought by customers within and outside NSA, and its products and services [redacted]

fight against terrorism. Based on our positive assessment of [redacted] is managed, we curtailed the scope of the inspection and reported only one deficiency: [redacted]

divisions are capable of operating as independent entities, [redacted] management has developed an organizational structure that produces an overall value greater than the sum of its parts.

(U) Management Action All action officials concurred with the recommendation that approval be obtained to operate the information systems.

(U) Overall Report Classification SECRET//COMINT//REL TO USA, FVEY

(U) Category Joint Warfighting and Readiness

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

(U//FOUO) Review of the President's Surveillance Program; NSA/CSS IG; ST-09-0002; 29 June 2009

~~(S//REL)~~ Summary In response to a provision of the FISA Amendments Act of 2008, the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and the Central Intelligence Agency completed a comprehensive review of the President's Surveillance Program that included, in accordance with the legislation, a description of: (A) all facts necessary to describe the establishment, implementation, product, and use of the product of the Program; (B) access to legal reviews of the Program and information about the Program; (C) communications with, and participation of, individuals and entities in the private sector related to the Program; (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and (E) other matters necessary for a complete a review of the Program. An unclassified report, a classified capstone report, NSA's individual classified report, and the classified reports of the other four OIGs were delivered to the Senate and House Intelligence Oversight and Judiciary committees in July 2009.

(U) Overall Report Classification TOP SECRET/[redacted] COMINT//ORCON//NOF ORN

(U) Category Joint Warfighting and Readiness

~~SECRET//REL TO USA, FVEY~~

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

~~SECRET//REL TO USA, FVEY~~

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

(U) [redacted] NSA/CSS IG; [redacted]  
25 September 2009 (both reports)

(S//REL) **Summary:** The OIG visited two [redacted] sites selected on the basis of risk, location, and [redacted]. The reviews assessed site operations, local customer support, and compliance with intelligence oversight requirements and [redacted]. Several findings and recommendations at each site addressed procedures and conditions that have arisen as a result of expanded missions of [redacted] including the need for quick computer network response time, updates to software, and accountability mechanisms. The review also made recommendations to address the implementation of the [redacted] and changes in site requirements and capabilities.

(U) **Management Action** [redacted] management at the site and [redacted] Headquarters concurred with the findings and are taking action to implement the recommendations.

(U) **Overall Report Classifications** TOP SECRET//COMINT//NOFORN [redacted]  
TOP SECRET//COMINT//NOFORN [redacted]

(U) **Category** Joint Warfighting and Readiness