

~~SECRET//20291123~~**(U) SEMIANNUAL REPORT TO THE CONGRESS****(U) For the Period April 1, 2006 Through September 30, 2006****(U) Office of Physical Security's Practices Relative to Protest Activity;**
NSA/CSS IG; ST-06-0012; 28 April 2006

~~(U//FOUO)~~ **Summary.** An article published in *The Sun* on 13 January 2006 alleged that NSA monitored members of the Baltimore Pledge of Resistance, a peace group tied to the Baltimore Emergency Response Network, as they prepared to protest at Fort Meade. The article also alleged that NSA used law enforcement agencies to track the activists. We conducted this special study to (a) identify the NSA Police authorities relative to the activities of protesters on or near NSA property; (b) determine if policies and procedures were in place to ensure compliance with those authorities; and (c) determine if the policies and procedures were followed on 3 July 2004 during protests at NSA by the Baltimore Pledge of Resistance peace group. We found that NSA Police were authorized, pursuant to Section 11 of Public Law 86-36, to protect buildings, grounds, and property solely under the administration and control of, and used extensively by NSA. We also concluded that NSA police acted in accordance with applicable authorities, policies, and procedures while performing duties associated with the protest activity. Finally, the Agency made no attempt to use the Signals Intelligence system to monitor this protest activity.

(U) Overall Report Classification. CONFIDENTIAL//REL to USA, AUS, CAN, GBR, NZL**(U) Category.** Homeland Defense**(U) Time Synchronization Issue;** NSA/CSS IG; ST-06-0013; 19 May 2006

~~(S)~~ **Summary.** One of the many challenges the Agency faces when analyzing complex signals is the accurate measurement and retention of time-related information. To accomplish its various missions, NSA must reliably affix accurate time date stamps and, when available, geolocation information on all collected signals. After receiving reliable indications that NSA's ability to affix and retain accurate time measurement is deficient, the OIG announced its intention to begin a special study of this subject. In response to similar indications, the Director, NSA announced the creation of the Time and Frequency Coordination Authority (TFCA or Authority) in May 2006. As a result, we curtailed the special study to give the TFCA a chance to address the deficiencies we have reason to believe exist. We will therefore make periodic inquiries into TFCA's progress in the coming months.

(U) Overall Report Classification. TOP SECRET//COMINT**(U) Category.** Joint Warfighting and Readiness

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: ~~20291123~~

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

~~SECRET//20291123~~

~~SECRET//20291123~~

(U) **Oversight Review of Restaurant Fund, CWF, and Gift Shop;** NSA/CSS IG;
AU-06-0015; 2 June 2006

(U//FOUO) **Summary.** A firm of Certified Public Accountants (CPAs) issued unqualified opinions on the reliability of the financial statements of the Agency's Restaurant Fund, Civilian Welfare Fund, and the Cryptologic Museum Gift Shop. Our oversight review of the CPA audit found no problems in the conduct of the recent audit by the CPA firm but identified two concerns: high-speed internet connection and nonappropriated fund instrumentality (NAFI) contract. Without a connection to high-speed internet service, the NAFI's business and accounting services will continue to be highly inefficient. The current NAFI contract (and all option years) for the contract with the CPA firm that reviews Agency NAFIs has expired. A new competitive effort needs to be awarded and in place before 30 September 2006 so that the contracted CPAs can be on hand to observe the ending inventory.

(U) **Management Action.** Management concurred with and is implementing our recommendations.

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

(U) **Category.** Financial Management

(U) **Award Fee Contracts;** NSA/CSS IG; AU-06-0002; 30 June 2006

(U//FOUO) **Summary.** As of 1 October 2005, NSA had award fees on [redacted] contracts valued at over [redacted]. Our audit reviewed [redacted] award fee contracts valued at [redacted] with total available award fees of [redacted] about 78 percent or [redacted] of the award fees were paid out. We concluded that the Agency needs a consistent approach to these contracts so award fees achieve their purpose: to help control program risk and improve contractor performance. The Agency's ability to evaluate contractor performance is impeded by (1) failure to document a basis for the award fee percentage; (2) award fee plans that do not allow for meaningful ratings (3) inconsistent evaluation methodologies; and (4) the absence of formal training in how to administer award fee contracts. We also question the use of Time & Material-Award Fee contracts because they place a heavy administrative burden on the Agency and do not emphasize acquisition outcomes.

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

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

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

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

(U) **Military Interdepartmental Purchase Requests and Economy Act Orders;** NSA/CSS IG; AU-05-0008; 12 July 2006

(U//FOUO) **Summary.** Over the last 2 fiscal years, Military Interdepartmental Purchase Requests (MIPRs) and Economy Act Orders (EAOs) represented [redacted] and [redacted] percent, respectively, of the total funds (over [redacted] for each year) used to purchase goods and services for NSA. Our audit found that the current practice of delegating the authority to approve MIPRs/EAOs to Senior Executives or Flag Officers is not achieving the

~~SECRET//20291123~~

~~SECRET~~#20291123

intent of the law; MIPRs/EAOs are not reviewed by a Contracting Officer or an independent entity to see if there is a valid reason for bypassing the Contracting Group; and the originating offices at NSA did little to monitor the billing and accounting for MIPRs and EAOs and did not always verify that goods and services were delivered;

(U//~~FOUO~~) **Management Action.** Management concurred with our recommendation to update the draft policies to strengthen internal controls over MIPRs/EAOs but nonconcurred with the recommendation to establish a separate Agency oversight mechanism. This was resolved when management agreed that the Acquisition Program Managers will now be responsible for oversight of MIPRs and EAOs.

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

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

(S) [redacted] NSA/CSS IG; [redacted]

(S) **Summary.** Our special study on [redacted] found the Cryptanalysis and Exploitation Services (CES) organization to be control conscious, with many strong management controls in place to ensure the integrity of [redacted] CES can further improve internal controls over [redacted] provided the procedures for handling [redacted] are formally reissued, properly coordinated, and fully address the procedural and compliance issues cited in our report.

(U) **Management Action.** Management concurred in our findings and recommendation, agreed to take corrective actions, and plan to complete all actions by 31 December 2006.

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

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

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

(U) **Followup Report on the** [redacted] NSA/CSS IG; [redacted] 21 July 2006

(S) **Summary.** Since 2003, the Agency [redacted] at NSA/CSS Hawaii. [redacted] initiatives were the subject of a finding and recommendation in the February 2005 Joint IG report at Hawaii. We closed the recommendation to address key policy shortfalls based on actions planned by the Directorate of Engineering (DE) and Corporate Planning. During a followup inspection, we found that [redacted]

[redacted] and DE and Corporate Planning have not issued two policies that address deficiencies noted in the 2005 Joint IG Report.

(S) **Management Action.** Management decided to withdraw the FY2006 funds [redacted] and agreed to complete the relevant policy documents by January 2007.

(U) **Overall Report Classification.** TOP SECRET//COMINT//TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL

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

~~SECRET~~#20291123

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

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

(U) **FY2006 Report on Compliance with the Federal Information Security Management Act at NSA/CSS;** NSA/CSS IG; AU-06-0009; 31 July 2006

(U//~~FOUO~~) **Summary.** NSA is making a concerted effort to address the weaknesses identified in our FY2005 audit of compliance with *The Federal Information Security Management Act (FISMA)*. Despite continuing impediments, the Agency's Chief Information Office (CIO) made progress in carrying out the Plan of Action and Milestone to address the certification and accreditation (C&A) of Agency systems - identified as a material weakness in FY2002. By June 2006, about [redacted] of all Agency systems and [redacted] of mission-critical systems (compared to [redacted] a year ago) were fully accredited. Our FY2006 FISMA review found weaknesses from prior years that were not fully mitigated: [redacted]

(U) **Management Action.** The CIO continues to make progress in addressing FISMA requirements. This includes holding bi-weekly meetings to track and report C&A progress and challenges for mission-critical systems. In addition, the Office of Information Assurance Services reviewed C&A data for accuracy, and the CIO engaged an outside firm to do a complete review of NSA's operational information security program. This resulted in [redacted] recommendations, which the CIO has used to baseline its budget for FY2007. This improved the CIO's ability to capture important IT security performance measures, as required by FISMA legislation.

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

(U) **Category.** Information Technology Management

(U) **Alaska Mission Operations Center;** NSA/CSS IG, AIA IG; NNWC IG; JT-06-0002; 4 August 2006

(S) **Summary.** A joint team of inspectors from the Air Intelligence Agency (AIA), Naval Network Warfare Command (NNWC), and NSA Inspector General conducted the first joint inspection of the Alaska Mission Operations Center (AMOC). Although the AMOC was officially 2 years old at the time of this inspection, we found no Concept of Operations or Implementation Plan for establishing the Center. Although progress is being made in attaining the presumed intent for the AMOC, progress is impeded by the lack of clearly defined authorities, responsibilities, processes, and chains of command. We also found that the Intelligence Oversight program needs many adjustments - some major and some minor, and Mission Operations was in transition, taking on new missions from other sites and working to expand [redacted] Overall, communications and computer systems and Network operations were well managed, but [redacted]

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

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

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

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

(U) **Asset Management and Cost Allocation for GROUNDBREAKER Contract;** NSA/CSS IG; AU-06-0001; 18 September 2006

(U//FOUO) **Summary.** The GROUNDBREAKER (GB) contract supports the Agency's non-mission Information Technology (IT) infrastructure. Each month GB bills the Agency for basic services in four service areas: Distributed Computing, Networks, Telephony, and Enterprise Management. Our audit recommendations focused on improving asset management, personnel data, and other areas. In asset management, we found process deficiencies in physical inventories and discrepancies in inventory data that contributed to a [redacted] percent inventory record error. Based on the results of our random statistical sample for October 2005, we projected the Agency may have been over billed by \$346,630. Regarding personnel data, [redacted]

[redacted] Based on this process, our sample indicated a potential over payment of about \$126,000 for October 2005.

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

(U) **Overall Report Classification.** CONFIDENTIAL//PROPIN

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

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

(U//FOUO) **Joint Defense Facility Pine Gap;** NSA/CSS IG, AIA IG; NNWC IG, INSCOM IG; JT-06-0003; 21 September 2006

(U//FOUO) **Summary.** A joint team of inspectors from the the Air Intelligence Agency (AIA), Naval Network Warfare Command (NNWC), Intelligence and Security Command and NSA Inspectors General conducted a joint inspection of the Joint Defense Facility Pine Gap (JDFPG). We found a very strong mission focus at the site. However, two problems that impede mission operations require immediate attention from senior leadership:

[redacted]

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

(U) **Overall Report Classification.** TOP SECRET//COMINT//TALENT KEYHOLE//REL TO USA, AUS, GBR

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

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

(U) **NSA's Ability to Detect, Contain, and Recover from Computer Security Incidents;** NSA/CSS IG; AU-05-011B; 26 September 2006

(U//~~FOUO~~) **Summary.** The audit objective was to determine if NSA/CSS has effective and efficient internal controls to prevent, detect, analyze, contain, and recover from computer security incidents affecting the NSA/CSS computing environment. Our findings corroborate the Chief Information Officer's assessment that [redacted]

[redacted]

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

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

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

(U) **Category.** Information Technology Management

(U) **Corporate Communications Strategy Group;** NSA/CSS IG; IN-05-0003; 27 September 2006

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

(U//~~FOUO~~) **Summary.** Our organizational inspection found that the Agency's communications and multimedia activities have not been centralized in the Corporate Communications Strategy Group. As seen in OIG reviews of other corporate enablers, the mission organizations eventually regrow these functions, using mission funds and personnel, when corporate sponsors cannot provide support. For example, we found that the Corporate Communications Strategy Group is not aware of nor does it have oversight over Agency contracts - totaling about [redacted]

[redacted]

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, CAN, GBR, NZL

(U) **Category.** Information Technology Management

~~SECRET//20291123~~

(U) **Time and Attendance Investigations;** NSA/CSS IG, IV-05-0034, 18 July 06; IV-06-0011, 22 May 2006; IV-06-0013, 12 September 2006; IV-06-0027, 15 August 2006; IV-06-0030, 7 September 2006; IV-06-0033, 20 Jun 2006; IV-06-0035, 4 August 2006; IV-06-0036, 29 June 2006; IV-06-0043, 20 June 2006; IV-06-0046, 15 September 2006; IV-06-0052, 26 September 2006

(U) **Summary.** The OIG substantiated eleven allegations of Time and Attendance fraud. In the aggregate, these cases will result in the administrative recoupment of approximately \$93,000 in Government funds paid for duty hours falsely claimed.

(U) **Overall Report Classifications.** UNCLASSIFIED//FOR OFFICIAL USE ONLY (all referenced investigations)

(U) **Category.** Other (Fraud)

(U) **Labor Mischarging;** NSA/CSS IG; IV-06-0012; 26 September 2006

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that a contract employee mischarged 135 labor hours while working on NSA contracts during the 2003 – 2005 time period. This amounted to approximately \$19,000 in charges falsely billed against NSA contracts, and the contractor reimbursed NSA that amount. The contractor also terminated the employee. The United States Attorney's Office, District of Maryland, declined prosecution due to the contractor's cooperation and reimbursement to NSA.

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

(U) **Category.** Other (Fraud)

(U) **Labor Mischarging;** NSA/CSS IG; IV-06-0028; 26 September 2006)

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that a contract employee mischarged 185 labor hours while working on NSA contracts in 2005. This amounted to approximately \$36,300 in charges falsely billed against NSA contracts, and the prime contractor has agreed to reimburse the NSA by that amount. The prime contractor terminated the employee. The United States Attorney's Office, District of Maryland, declined prosecution due to the prime contractor's cooperation and reimbursement.

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

(U) **Category.** Other (Fraud)

(U) **Falsification of an Official Document;** NSA/CSS IG; IV-06-0034; 21 July 2006

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that a GG-13 NSA/CSS employee falsified the rating score on his 2005 Performance Review, forged management signatures, and submitted the document to the Agency in support of his 2006 promotion application. The matter was referred for disciplinary adjudication.

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

(U) **Category.** Other (Fraud)

~~SECRET//20291123~~

~~SECRET//20291123~~

(U) **Travel Voucher Fraud;** NSA/CSS IG; IV-06-0008, 26 September 2006;
IV-06-0009, 22 September 2006; IV-06-0024, 14 August 2006

(U//~~FOUO~~) **Summary.** The OIG substantiated three allegations of travel voucher fraud. Two investigations involved false travel expense report claims for Personally Operated Vehicle mileage by an NSA employee and an NSA military assignee. A third investigation involved an employee who repeatedly remained in country longer than necessary on OCONUS TDYs, and falsely claimed per diem on his travel vouchers. The Agency will recover a total of approximately \$20,000 in Government funds as a result of these three investigations.

(U) **Overall Report Classifications.** UNCLASSIFIED//FOR OFFICIAL USE ONLY
(all referenced investigations)

(U) **Category.** Other (Fraud)

(U) **Misuse of Government Resources;** NSA/CSS IG; IV-06-0023; 14 June 2006

(U//~~FOUO~~) **Summary.** The OIG's Offices of Intelligence Oversight and Investigations conducted a joint inquiry into an allegation that an NSA/CSS employee violated applicable law and regulation by using Government property for unauthorized and unofficial purposes. The inquiry substantiated the misuse allegation and the matter was referred to the NSA OGC for consideration of referral to the Department of Justice.

(U) **Overall Report Classification.** TOP SECRET//COMINT

(U) **Category.** Other (Misuse of Resources)

~~SECRET//20291123~~

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U) Ongoing

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

~~(U//FOUO)~~ **Inspection of the Information Warfare Support Center; NSA/CSS IG; IN-06-0001**

~~(S)~~ **Background** The Information Warfare Support Center (IWSC) began operations in November 1994 in response to the need for SIGINT support to Information Operations (IO). IWSC's mission is to provide the combatant commander(s) with [redacted]

[redacted]
related to counterterrorism. The primary objectives of this inspection include the following: a) determining whether the IWSC is executing its current missions and functions in an efficient and effective manner and in accordance with its charter, identifying any impediments to mission accomplishment; b) determining whether IWSC personnel comply with Internal Management Controls and other Agency regulations and policies governing personnel and organizational management; and c) assessing how well IWSC shares information with internal and external customers.

(U) Inspection of SID's Chemical, Biological, Radiological, Nuclear Mission; NSA/CSS IG; IN-06-0002

~~(S)~~ **Background.** Chemical, Biological, Radiological, and Nuclear (CBRN) terrorism is one of the most menacing threats to U.S. security, and from a Signals Intelligence (SIGINT) perspective, [redacted]

[redacted] work the CBRN target from varying perspectives. The inspection is evaluating CBRN mission performance, including examining the execution of CBRN as a transnational target, assessing the impact of Mission Build-Out, and reviewing any funding or human resource issues:

(U) Inspection of the Middle East and North Africa Product Line; NSA/CSS IG; IN-06-0006

~~(S)~~ **Background.** The mission of the Signals Intelligence Directorate's Deputy Directorate for Analysis and Production includes the countries located in the Middle East and North Africa (MENA). The Office of MENA creates analytic strategies, performs SIGINT development, and creates SIGINT products and services in response to customer Information Needs. It is also deeply involved in SIGINT production to support the Agency's counterterrorism activities. The primary objectives of the inspection include the following:

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

a) determine the effectiveness and efficiency in which the Middle East and North Africa Product Line organization is performing mission operations functions; b) identify impediments that the organization faces in SIGINT production; and c) determine whether the organization's personnel comply with Internal Management Controls and other Agency regulations and policies governing personnel and organizational management.

(U//FOUO) **Inspection of the Geospatial Exploitation Office; NSA/CSS IG; IN-06-0005**

~~(S)~~ **Background** The Geospatial Exploitation Office (GEO) began operations in

[Redacted]

The primary objective will be to assess GEO's mission effectiveness and their ability to satisfy requirements and information needs levied on the organization. The inspection will determine whether the current organization's missions and functions are being properly executed in an efficient and effective manner; whether missions and functions are accurately portrayed and being accomplished; establish whether missions performed are appropriately placed within the product line; and will identify any impediments, which hinder the efficient and effective execution of their missions and functions.

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

~~(S)~~ [Redacted] **Regional Review; NSA/CSS IG; [Redacted]**

~~(S)~~ **Background.** The OIG is completing a regional review of [Redacted] that are focused on [Redacted] including support to counterterrorism. Our review assesses site operations, compliance with intelligence oversight requirements, [Redacted]

[Redacted]

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

(U) **Special Studies of Presidentially-authorized Program; NSA/CSS IG**

(U//FOUO) **Background:** The OIG is performing continual audits of NSA's Presidentially-authorized counterterrorism program. The overall objectives are to determine whether there are appropriate policies and procedures in place for activities under the program consistent with the terms of the Presidential Authorization; to evaluate their efficiency and effectiveness in mitigating any high-risk activities associated with the program; and to identify any impediments to satisfying the requirements of the Presidential Authorization.

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

(U) Planned

(U) **Followup Review of Access to SIGINT Databases; NSA/CSS IG; ST-06-0003**

(U//FOUO) **Background.** Information sharing and data access continue to be major priorities across the Intelligence Community (IC). To jumpstart the information-sharing concept, several efforts were initiated, most notably [Redacted]

~~SECRET//20291123~~

[Redacted]

[Redacted]

counterterrorism activities. The objectives will be to determine if SID's process for granting database access is having the desired outcome, and, if not, what are the impediments. Additionally, we will determine the adequacy of security practices for terminating access once access is no longer needed.

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

~~SECRET//20291123~~