(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) ***For the Period October 1, 2005 Through March 31, 2006***

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

(U) **Controls on Laptop Computers;** NSA/CSS IG; ST-05-0015; 25 October 2005

(U//~~FOUO~~) **Summary.** After conducting many investigations of missing laptop computers, the Compromise and Computer Forensics Office asked the NSA OIG to review the Agency's inventory processes and determine whether the Agency has adequate controls to track and account for laptop computers. Over the past 3 years, the Compromise and Computer Forensics Office conducted [ ] investigations of missing laptops but was unable to locate [ ] ([ ] classified, [ ] of unknown classification, and [ ] unclassified) of the [ ] laptops. Such losses, while financially immaterial, raise counterintelligence concerns.

(U//~~FOUO~~) **Management Action**. To address the root cause of the losses—the lack of hand receipts for laptops—the Security, Logistics, and OIG organizations are strengthening the enforcement of laptop controls, including penalties for personnel who do not comply with the hand receipt requirement and managers who fail to enforce it. The three organizations will meet every 90 days to discuss the enforcement of the hand receipt policy and ways to hold managers accountable

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

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

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

(U//~~FOUO~~) **Summary.** [ ]

(U) **Management Action**. Management agreed to act on all our recommendations. However, Signals Intelligence Directorate and Information Technology Directorate are still working out the appropriate division of effort and responsibilities for managing and optimizing data flow.

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

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

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

(U) **Misuse of Government Resources**; NSA/CSS IG; IV-05-0027; 17 November 2005

(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. We substantiated the misuse allegation and referred the matter to the NSA/CSS Office of the General Counsel, for consideration of referral to the DOJ.

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

(U) **Category.** Other (Intelligence Oversight)

(U) **Contractor Performance Management and Evaluation of the GROUNDBREAKER Contract**; NSA/CSS IG; AU-05-0002; 16 December 2005

(U//~~FOUO~~) **Summary.** This audit focused on improving the use of rewards and penalties to motivate the contractor to optimize performance. Our audit found that, although the modernization goal of May 2004 had slipped by 17 months, the contractor received $10.7 million out of a possible $20.9 million in award fees for modernization. In this case, award fees were not used in a way that motivated the contractor to meet a crucial performance goal. Additionally, millions of dollars in service credits (penalties for failure to deliver agreed-to services) that should have been credited to the Agency were not recorded as accounts receivable and reported on financial statements. This ultimately cost the Government $300,000 in finance or interest charges from July 2002 to March 2005.

(U) **Management Action.** After initially nonconcurring with our recommendation to improve modernization incentives, management revised its position and is developing new, more objective incentive criteria. Corrective actions are now under way or completed on all six recommendations.

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

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

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

(U) **Advisory Report on the Audit of the [redacted] Procurement and Associated Infrastructure Program**; NSA/CSS IG; [redacted]

(U//~~FOUO~~) **Summary.** The advisory report identified potential issues that surfaced during the survey phase of our audit of the [redacted] Procurement and Associated Infrastructure Program. We curtailed our survey after reviewing a zero-based review of Cryptanalysis Exploitation Services, which included [redacted] Our survey supported the conclusions of the zero-based review: lack of sustained funding threatens the [redacted] infrastructure; the physical facilities are inadequate; acquisition

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

practices are inconsistent; and there is insufficient mission assurance for [redacted] In addition, our survey indicated that the Portfolio Management Office lacked sufficient authority over program execution and resources.

(U) **Management Action.** Since the recommendations for [redacted] in the zero-based review are related to the indications noted during our audit survey, we will track completion in the OIG Followup system.

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

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

(U) **Nuclear Command and Control (NC2) Program**; NSA/CSS IG; AU-04-010B; 23 January 2006

~~(S)~~ **Summary.** Our audit revealed that the [redacted] Board and management of the Nuclear Command and Control Program (NC2) [redacted]

(U) **Management Action.** Management agreed to act on all recommendations.

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

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

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

(U) **Aerospace Data Facility**; NSA/CSS IG; INSCOM IG; NSG IG; AIA IG; JT-06-0001; 23 January 2006

~~(S)~~ **Summary.** The joint inspection found that the Aerospace Data Facility has [redacted]; 2) NSA HQ organizations have not provided policy, standards, or oversight of various efforts across the Extended Enterprise; and 3) the lack of a mission management tool hinders the site's ability to optimize its role in consolidated mission planning and execution.

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

(U) **Management Action.** Management concurred with the recommendations and is taking appropriate corrective action.

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

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

(U//~~FOUO~~) **Red Team Targeting of the** [redacted] NSA/CSS IG; [redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) **Summary.** The National Defense Authorization Act of Fiscal Year 2000 directs the National Counterintelligence Executive (NCIX) to submit an annual report to the Secretary of Energy and the Director of the Federal Bureau of Investigation on the security vulnerabilities of the computers of the DOE's national laboratories. [redacted]

[redacted]

(U//~~FOUO~~) **Management Action.** NSA management has amended the Red Team process and procedures to require, for each exercise, [redacted]

[redacted]

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

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

(U) **Post-Accreditation Process for Information Technology Systems**; NSA/CSS IG; ST-05-0018; 16 February 2006

(U//~~FOUO~~) **Summary.** Our special study of the post-accreditation process for information technology systems sampled [redacted] systems that recently went through the accreditation process and were [redacted] of the systems were not operational and, [redacted]

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

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

[redacted]

(U) **Management Action.** The Information Assurance Directorate responded that it is working on a post-accreditation process that satisfies the recommendations of the OIG report.

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

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

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

~~(C)~~ **SIGINT Activities** [redacted] NSA/CSS IG, INSCOM IG; AIA IG;

[redacted]

~~(S)~~ **Summary.** A joint team of inspectors from the AIA, INSCOM, and NSA Inspectors General conducted an inspection of [redacted]

[redacted]

(U) **Management Action.** The report makes ten recommendations to improve the effectiveness and efficiency of SIGINT operations. Most of these recommendations focus on the need to bring greater definition to the authorities, responsibilities and functions with respect to the operational roles of the SIGINT sites. Management concurred in all recommendations and corrective action is being taken.

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

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

(U) **"Persistent Cookies" on the NSA Public Website;** NSA/CSS IG; ST-06-0015; 21 March 2006

(U~~//FOUO~~) **Summary.** The OIG conducted an inquiry into the circumstances and implications of the Agency's usage of "persistent cookies" on its public website, NSA.gov. We concluded that, during a past system upgrade, a number of cookie properties were unintentionally reset, extending their expiration beyond the intended settings. As a result, the website was inadvertently using "persistent cookies" instead of the usual "session cookies." Once aware of the situation, the Agency immediately disabled the "persistent cookies" and restored the intended session length settings. Based upon our interviews, contacts, and reviews of databases and technical literature, we concluded the Agency's inadvertent "persistent cookies" did not collect user information or any personally identifiable information on visitors to the NSA.gov website.

(U//~~FOUO~~) **Management Action.** Corporate Communications Strategy Group personnel have begun documenting the programming code with comments where system changes could inadvertently enable different types of cookies. The Group intends to have comprehensive procedures written and implemented by July 2006, and has suspended any system upgrades until then.

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

(U) **Category.** Other

(U//~~FOUO~~) **Special Study of Executive Level Management of Systems Development at NSA/CSS;** NSA/CSS IG; ST-05-0004; 22 March 2006

(U//~~FOUO~~) **Summary.** At the corporate level, NSA/CSS needs a formal, stable, unified methodology to enable its leadership team to wield effective oversight of key development programs. This is even more necessary as the Agency accelerates transformation efforts. The existing disparate approaches to program oversight in several Agency organizations should be unified into an overarching methodology under the leadership of one organization or individual. An OIG benchmarking study of two information-intensive organizations in the private sector and one major DoD development program supported the conclusion that until NSA/CSS adopts such a methodology, its leaders will not have the requisite degree of insight into all aspects of key enterprise initiatives. By the end of the study, it was clear that the Agency needs such a methodology to lead the work force successfully through the pervasive changes underway in its mission and core business.

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

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

(U//~~FOUO~~) **Interim Report on the Audit of NSA's Computer Security Incident Response;** NSA/CSS IG; AU-05-011A; 24 March 2006

~~(S)~~ **Summary.** During our audit of NSA's Computer Security Incident Response, the NSA/CSS Information Systems Incident Response Team (NISIRT) told us about a vulnerability created by default settings [redacted]

(U) **Management Action.** The Information Technology Directorate responded that it is working to secure current and future [redacted] which satisfies our recommendation.

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

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

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

(U//~~FOUO~~) **Misuse of the Agency's Unclassified Network;** NSA/CSS IG; ST-05-0019; 28 March 2006

(U//~~FOUO~~) **Summary.** After expending considerable resources to address misuse of the Internet by Agency affiliates, the NSA/CSS Information Systems Incident Response Team (NISIRT) asked the OIG to review the adequacy of the Agency's policies regarding usage of NSA's unclassified network. We concluded that the Agency's current policies, the Computer Security Incident Report process and a new "Smart Filter" which will deny user access to inappropriate web sites are adequate tools for dealing with misuse. However, we also found that many affiliates are not aware of current policies, and that managers are not informed of misuse by their subordinates.

(U//~~FOUO~~) **Management Action.** Management agreed to implement annual training on Internet policies for affiliates, and NISIRT agreed to advise managers of policy violations so they can hold subordinates accountable.

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

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

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

(U//~~FOUO~~ [redacted] **Dorsey Road Warehouse;** NSA/CSS IG; [redacted]

~~(S)~~ **Summary.** While investigating a procurement matter involving computer equipment shipped to the Dorsey Road Warehouse (DRW) [redacted] We undertook a special study to determine whether DRW [redacted]

~~(S)~~ **Management Action.** In response to our findings, the Associate Directorate for Security and Counterintelligence and Associate Directorate for Installations and Logistics developed short- and long-term strategies [redacted] These strategies addressed our concerns, and we will track implementation through our followup system. We consider implementation a high priority that should be funded as such.

(U) **Overall Report Classification.** SECRET

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

(U) **Category.** (U) Infrastructure and Environment

(U) **False Labor Charges by an Agency Contractor;** NSA/CSS IG; IV-05-0031; December 2005

(U//~~FOUO~~) **Summary.** During a routine Security background check, suspicions surfaced about the accuracy of labor charges by an NSA/CSS contractor employee. An OIG investigation substantiated that, during a 22-month period, the contractor employee falsely billed 751 labor hours to an Agency contract, amounting to approximately $35,000 in false charges. The matter was referred to the DOJ for a prosecutive opinion, and the NSA/CSS Office of the General Counsel is seeking restitution from the involved company.

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

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

(U) **Time and Attendance Investigations**; NSA/CSS IG; IV-05-0008 (10 Nov 2005); IV-05-0035 (4 Oct 2005); IV-06-0014 (10 Mar 2006); IV-06-0026 (24 Mar 2006); IV-06-0021 (30 Mar 2006)

(U//~~FOUO~~) **Summary.** The OIG substantiated five allegations of Time and Attendance abuse, wherein employees claimed hours in excess of those they were determined to have actually worked. In the aggregate, these cases will result in the recovery of approximately $44,000.00 in funds paid to employees for hours falsely claimed.

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

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

(U) **Unauthorized Commitment of Government Funds and Intentional Falsifications;** NSA/CSS IG; IV-05-0015; March 2006

(U//~~FOUO~~) **Summary.** An NSA/CSS employee made an unauthorized commitment of Government funds by accepting approximately [redacted] equipment without a contract. The employee and an Agency contractor then attempted to conceal the unauthorized action by creating and back-dating a fictitious "Loan Agreement," and by providing the OIG with false testimony. The employee and contractor violated applicable Federal regulations and possibly Title 18, United States Code, Section 1001.

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

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

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

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U) Completed from 1 October 2005 – 31 March 2006

(U//~~FOUO~~) **Advisory Report on Activities Associated with Expeditionary SIGINT Deployments to Hostile Areas**; NSA/CSS IG; ST-06-0001; 23 January 2006

(U//~~FOUO~~) **Summary.** A February 2005 after-action report raised serious concerns about the activities and processes associated with the deployment of NSA/CSS personnel to hostile areas. The issues were referred to the OIG, which conducted extensive research to determine if a formal review was needed. Based on interviews of [redacted] organizations involved in the deployment process and [redacted] returnees from hazardous area deployments, such as [redacted] we concluded that some aspects of the process, especially training by enabler organizations, have improved considerably over the last 2 years. Processes to ensure appropriate and timely candidate selection, pre-deployment mission training, IT support, and corporate resolution of issues raised in after-action reports need to be standardized and implemented across the Agency.

(U) **Management Action.** Corrective measures addressing the issues are already underway; as such, we do not plan to undertake a formal review at this time. However, the issues raised merit continued action and followup by Agency management. We plan to revisit these processes again in 1QFY07 to assess progress.

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

(U) **Category.** Joint Warfighting and Readiness (b)(3)-P.L. 86-36

(U) Ongoing

(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] related to counterterrorism. The primary objectives of this inspection include the following: a) determining whether the [redacted] 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 [redacted] personnel comply

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

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

with Internal Management Controls and other Agency regulations and policies governing personnel and organizational management; and c) assessing how well [redacted] 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] 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.

(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.

(U) Planned

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

(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)~~ **Office of Middle East and North Africa**; 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 [redacted] Our inspection will evaluate the mission effectiveness of MENA and its ability to satisfy requirements and information needs levied on the organization.

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

~~(S)~~ **Background**. The OIG plans to conduct a regional review of [redacted] sites that are focused on [redacted] including support to counterterrorism. Our review will assess site operations, compliance with intelligence oversight requirements, [redacted] and local support activities.

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

~~(S)~~ **Backgound**. 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 the efforts to provide [redacted]

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

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