~~SECRET//X1~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

For the Period October 1, 2003 Through March 31, 2004

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

(U) **Meade Operations Center-Followup Inspection**; NSA/CSS IG; INSCOM IG, AIA IG, NSG IG, JT-03-0005, 3 October 2003

Summary. (U~~//FOUO~~) The followup inspection found that the [redacted] the Meade Operations Center, [redacted] but was still awaiting a decision on its governance and its place in the organizational structure. Morale had improved under new, stable leadership. We recommended that the Signals Intelligence Directorate (SID) assign a suspense date to finalize its proposal for governance and to place an agenda item titled "Implementation Plan for MOC Governance" at the next Joint Issues Board Meeting.

Management Action. (U) Management is taking appropriate corrective action.

Overall Report Classification. (U) TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//X1

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

Category. (U) Joint Warfighting and Readiness

~~(S)~~ [redacted] NSA/CSS IG, [redacted]

Summary. ~~(S)~~ We visited selected [redacted] sites to ensure that policies and internal controls for its intelligence activities are carried out with due regard for the law. We found that processes exist to validate that intelligence activities comply with the law; however, we also found four areas of concern regarding policies and internal controls: [redacted]

Management Action. (U~~//FOUO~~) Management concurred with all recommendations and agreed to publish formal policies and agreements that reflect current responsibilities; incorporate OIG suggestions to improve the control environment; conduct rigorous security reviews—and act on the results; and ensure that valuable SIGINT assets are both properly safeguarded and fully utilized.

Overall Report Classification. (U) TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//X1

Category. (U) Joint Warfighting and Readiness

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

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1~~

(U~~//FOUO~~) **Deployment Services, Analysis and Production Directorate**; NSA/CSS IG, IN-03-0003, 21 November 2003

Summary. (U~~//FOUO~~) The Deployment Services organization in the Analysis & Production Directorate (A&P) was created to optimize agility in responding to rapidly changing intelligence needs. The organization also manages the training and development of the analytic work force. We found that Deployment Services did a good job of getting the right person in the right job at the right time—particularly in a crisis—and had forged effective partnerships with the Associate Directorates of Human Resource Services (ADHRS) and Education and Training (ADET). However, workforce development needed attention from A&P leadership, starting with an analysis of future training needs engendered by new toolsets. Human resource databases, developed and maintained by Deployment Services staff, are labor intensive. PeopleSoft database services from ADHRS should eventually allow production personnel to concentrate on mission-centric work.

Management Action. (U) A&P Directorate, Deployment Services, ADHRS, and ADET are taking corrective action on all of the recommendations.

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

Category. (U) Human Capital

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

(U) **Information Assurance Solutions Division**; NSA/CSS IG, IN-03-0009, 23 December 2003

Summary. (U~~//FOUO~~) The Information Assurance Directorate's (IAD) [redacted] The division follows a well-documented process and methodology, and earns high praise from its customers regarding risk management. The inspection found that the division was accepting many projects that did not meet [redacted] requirements; in order to perform testing, the [redacted] division had to do the customer's work—a waste of Agency resources. Long lulls between projects were inefficient and frustrating to the division's cadre of technical experts. Correcting the problem depends on an effective IAD-wide requirements and prioritization process and a mechanism to deploy [redacted] skills where they are most needed.

Management Action. (U~~//FOUO~~) The [redacted] division has since been reassigned to the [redacted] as part of the IAD reorganization. This reassignment of the [redacted] function should resolve most of the concerns specific to the [redacted] division. The larger IAD issues are addressed in our special study on IAD Corporate Issues.

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

Category. (U) Information Technology Management (Systems Security)

(U) **Ft. Gordon Regional Security Operations Center**; NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-04-0001, 13 January 2004

Summary. ~~(C)~~ A joint inspection of the Ft. Gordon Regional Security Operations Center (GRSOC) by a team from the Service Cryptologic Elements and NSA/CSS found problems that directly affected the site's effectiveness and must be addressed at a high level: (1) assigning enough people and resources to accomplish the expanding mission; (2) acquiring space to accommodate mission growth and a continuity of operations facility; and (3) specifying which Headquarters organization is responsible for resolving field mission and support problems. The team also found two perennial problems that are not confined to GRSOC and require innovative solutions by senior leadership: (1) [redacted] (2) "Jointness Initiatives" are not getting the level of Higher Headquarters support needed for success.

Management Action. (U) Management is taking appropriate corrective action.

Overall Report Classification. (U) TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//X1

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

Category. (U) Joint Warfighting and Readiness

(U) **Vulnerability Assessments Division**; NSA/CSS IG, IN-03-0004, 23 January 2004

Summary. ~~(C)~~ Vulnerability assessments are an important tool to help protect the nation's critical infrastructure of telecommunications and information systems, per National Security Directive 42 (NSD-42) and Presidential Decision Directive 63. The Vulnerability Assessment division is part of the Discover Vulnerabilities (DV) triad of services offered by IAD organizations; it performs high-level assessments that identify vulnerabilities in the operational information systems of DoD, Intelligence Community, and selected private sector customers. The inspection found that the organization provides a valuable service and enjoys a high degree of customer satisfaction, but the workload, at the time of the inspection, was uneven and insufficient for the [redacted] assignees. Moreover, information sharing with other Triad members and with the larger DV community is minimal. Two issues that contribute to the division's workload problems are the absence of both a centrally managed IAD requirements process and a single codified management process for the triad of DV services.

Management Action. (U) Management has already taken steps to improve its control environment, particularly in the area of time and attendance. Recommendations that require action above the Vulnerability Assessment division, symptomatic of larger IAD process and policy issues, are addressed in our special study on IAD Corporate Issues.

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

Category. (U) Information Technology Management (Systems Security)

(U) **Selected System Engineering Contracts**; NSA/CSS IG, ST-03-0019, 30 January 2004

Summary. (U//~~FOUO~~) This special study reviewed [redacted] system engineering contracts to ensure proper competition. We found that only [redacted] were sole source actions, and they were supported by Competition in Contracting Act (CICA) justifications and documentation. The remaining actions were either 8(a) awards to small disadvantaged businesses, orders legitimately placed on previously awarded competitive actions, or competitively awarded contracts. We did identify potential issues with [redacted] sole source contracts regarding questionable cost growth, continuing lack of competition, and failure to perform market research. These [redacted] contracts will be covered in a separate report.

Management Action. (U) The Acquisition organization and the Competition Advocate recently took steps to make it more likely that competition would be utilized to the maximum extent practicable.

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

Category. (U) Acquisition Management

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

(U) **Information Assurance Directorate – Corporate Issues**; NSA/CSS IG, ST-03-0016, 19 February 2004

Summary. (U//~~FOUO~~) Organizational inspections of three IAD divisions, two of which are summarized in this Semiannual Report (Information Assurance Solutions and Vulnerability Assessments) and one from the previous Report (Operational Network Evaluations) surfaced four common themes regarding IAD corporate functions that negatively impact the overall Discover Vulnerabilities (DV) activity. This study offered an overarching view of how DV processes are sometimes at cross-purposes with one another and recommended measures to align them with corporate IAD goals. Key findings of the study that warrant further corporate attention are: (1) a porous IAD requirements process that is not centralized and lacks sufficient corporate structure and oversight to ensure consistent handling of customer requests; (2) an ineffective, non-cohesive corporate marketing strategy; (3) lack of central management of DV activities; and (4) ineffective knowledge management.

Management Action. (U) IAD leadership concurred with all of the recommendations and has begun to implement corrective measures to address the findings.

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

Category. (U) Information Technology Management

(U) **Summary of OIG Efforts Related to the Congressional Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001**; NSA/CSS IG, ST-04-0015, 25 February 2004

Summary. (U//~~FOUO~~) The IG, DoD has started a review of the Factual Findings and Record of the "Joint Inquiry Into Intelligence Community Activities Before and After

the Terrorist Attacks of September 11, 2001," dated 10 December 2002. Specifically, Recommendation 16 of this report tasks the IG, DoD to review the findings and record of the Joint Inquiry "to determine whether and to what extent personnel at all levels should be held accountable for any omission, commission, or failure to meet professional standards." On 12 November 2003, the Director, NSA wrote to the Congress in response to Recommendation 10 of the same report. His letter referred to a series of specific areas in which the Agency has been energetically responding to the issues that gave rise to the recommendation.

(U) At the request of the DoD Deputy Inspector General for Intelligence, the NSA OIG summarized its efforts related to the Director's response. Since 2001, about half of the OIG's reviews, including inspections, audits, and special studies, have been germane to the Director's response. The NSA OIG's report summarized 55 reviews (over 40 completed) for the period 2001 to 2004. The OIG grouped the reviews into two categories: *technological solutions and programs* (includes research and technology initiatives, acquisition management, organizational transformation, and mission and systems security); and *collaboration and information sharing* (includes relations with partners and customers, and joint inspections with the service cryptologic elements). It should be noted that the summary of each review describes conditions as they existed at the time of the review. Those conditions may be, and in many cases certainly are, materially different as of the date of this Semiannual Report.

Overall Report Classification. (U) TOP SECRET//COMINT/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, and NZL//X1

Category. (U) Other

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

(U) **Campaign Supplemental Funding**; NSA/CSS IG, AU-03-0004, 9 March 2004

Summary. ~~(S)~~ This report summarized the results of our audit of the supplemental funds NSA received to respond to the events of 9/11 and the invasion of Iraq. After 9/11, Congress bolstered the Agency's budget with four emergency supplemental appropriations [redacted] for the war on terrorism and the Iraqi conflict. NSA's Directorate of Finance (DF) had to manage these large supplemental appropriations under extraordinary pressure and time constraints. Our review focused on the first two supplemental appropriations, which were received from September 2001 to September 2002 and totaled [redacted] The audit found that when NSA requested the initial emergency supplemental, there was no formal process for developing and documenting this type of request and tracking the underlying requirements. Two factors made the task even harder: the Agency had only a short time in which to submit the requests, and DoD failed to issue specific guidance to supplement the general guidance published by OMB shortly after 9/11. The Agency's situation was not unique; as reported by GAO, DoD's failure to issue specific internal guidance caused uncertainty on appropriate uses of the emergency funds throughout its components. For the second supplemental, we encountered difficulty in completely tracking the actual expenditure categories in the accounting system to the requirement areas because the reporting "categories" did not correlate.

Management Action. (U~~//FOUO~~) Since the current administration plans to continue funding the war on terrorism through supplemental appropriations, it is important to have an efficient process for managing them; it should facilitate accurate accounting that tracks how funds are used to the approved requirement. DF recently developed a template (including description, justification, requested funds, initiating organization, and point of contact for documenting each requirement in a supplemental request) to standardize Agency requests for supplemental appropriations. Properly used, the template should ensure that requirements are documented and trackable, which will help maintain the Agency's credibility with Congress.

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

Overall Report Classification. (U) SECRET//X1

Category. (U) Financial Management

(U) **Report of Inquiry: Usefulness of [redacted] Analysis**; NSA/CSS IG, [redacted]

Summary. ~~(S)~~ In August 2003, an analyst alleged that he published a report in [redacted] and that the report's editing resulted in the deletion of a significant amount of information. The analyst believed that the deleted information would have been useful to other analysts [redacted] Our inquiry concluded that the editing was performed in accordance with established policies and procedures regarding sanitization of reports containing sensitive information. Additionally, the deleted information was retained for potential future use.

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

Overall Report Classification. (U) TOP SECRET//COMINT//X1

Category. (U) Other

(U) **Access to Signals Intelligence Databases**; NSA/CSS IG, IN-04-0001, 11 March 2004

Summary. (U~~//FOUO~~) A key NSA goal is to share information in Agency databases more freely among all parts of the extended enterprise and with Agency customers. Just as this inspection commenced, the Signals Intelligence Directorate (SID) announced a new policy for gaining access to these databases. As a result, we curtailed the inspection but made recommendations to ensure that access requests are handled in accordance with the new transformation goal. We found that SID's efforts to streamline database access had gathered considerable momentum.

Management Action. (U~~//FOUO~~) To sustain this momentum, SID officials agreed to publish a policy framework to guide those who make mission-related decisions on whether to grant access to SID databases; document the main steps in the new process, along with time limits for each step; and spell out the authorities, roles, and responsibilities of all parties involved in processing requests to access SID databases.

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

Category. (U) Joint Warfighting and Readiness

(U) **Possible Violations of Federal Law,** NSA/CSS IG, IV-04-0003, 12 March 2004

Summary. (U~~//FOUO~~) Pursuant to a 1995 agreement between the Justice Department and the agencies of the Intelligence Community, we requested that the NSA General Counsel refer to the General Counsel of another Intelligence Community agency allegations of possible criminal misconduct by an employee of that agency and the results of our inquiry.

Overall Report Classification. (U) TOP SECRET//COMINT//NOFORN//X1

Category. (U) Other

(U) **Time and Attendance Investigations**, IV-03-0022 (12 December 2003), IV-03-0047 (9 December 2003), IV-03-0059 (5 February 2004)

Summary. (U~~//FOUO~~) The OIG substantiated three separate and substantial "Time and Attendance Abuse" allegations where employees claimed hours in excess of what they actually worked. Combined, these cases will result in the recoupment of almost $30,000 in funds paid to employees for hours falsely claimed. One of these investigations uncovered rampant timecard abuse in one particular Agency organization and resulted in findings against six of that organization's employees.

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

Category. (U) Other

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

(U) **Attack Sensing and Warning Program**; NSA/CSS IG, AU-03-0003, 24 March 2004

Summary. ~~(S)~~ The purpose of the Attack Sensing & Warning (AS&W) program is to detect unauthorized intrusions or malicious attacks on DoD systems and networks. The audit looked at the Agency's [redacted] major AS&W projects. We found that this [redacted] program has never undergone the type of independent formal review required by DoD and NSA acquisition regulations. Furthermore, no one has determined when future program capabilities will be fielded and how much they will cost. The audit also found that the Defensive Information Operations officials have no formal process for passing research and development (R&D) topics or requirements to the Defense Computing Research Office.

Management Action. (U~~//FOUO~~) Management has agreed to place the AS&W program in the appropriate category, schedule a milestone review, conduct Operational Testing & Evaluation, and coordinate R&D efforts with the Defense Computing Research Office to share information and avoid duplication of effort.

Overall Report Classification. (U) SECRET//NOFORN//X1

Category. (U) Other (Major Acquisition Program)

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

(U) **Counter Encryption Programs**; NSA/CSS IG, AU-03-0002, 31 March 2004

Summary. ~~(S)~~ The purpose of the audit was to determine if a counter encryption program is capable of meeting current and projected customer requirements to counter specific instances of strong encryption.

Management Action. (U) Management concurred in the recommendation to complete the necessary program documentation and to provide it to the MDA at the scheduled interim review date of April 2004.

Overall Report Classification. (U) TOP SECRET//COMINT-ECI-KES//X1

Category. (U) Other (Major Acquisition Program)