~~SECRET//X1~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

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

For the Period April 1, 2003 Through September 30, 2003

(U//~~FOUO~~) **Survey of Cryptologic Services Group, Naval Air Station, Key West, FL**; NSA/CSS IG, ST-03-0011, 22 May 2003

Summary. ~~(S)~~

Management Action. ~~(C)~~ Management concurred in all recommendations. The

Overall Report Classification. (U) SECRET//COMINT//TALENT KEYHOLE//X1

(U) **Followup Report on the NSA/CSS Operations Security Program**; NSA/CSS IG, ST-03-0001, 27 May 2003

Summary. (U) Our followup review focused on NSA's implementation of its Operations Security (OPSEC) Program, per DoD Directive 5205.2, *The DoD OPSEC Program*. Specifically, we determined the status of the proposal to reestablish the Agency's internal OPSEC program under the NSA Counterintelligence Center (NSACC) and the revision of NSA's two OPSEC policies. We found that reestablishment of the Agency's OPSEC Program and the revision of NSA/CSS Directive 120-01, *NSA/CSS Operations Security Program*, had stalled. The revision of NSA/CSS Directive 120-03, *National OPSEC Program*, to be issued as NSA/CSS Policy No. 3-6, was in the final stages of coordination.

Management Action. (U) In August 2002, the Director, NSA/Chief, CSS (DIRNSA) reestablished the NSA OPSEC Program under the NSACC, which subsequently merged with what is now the Associate Directorate for Security and

Counterintelligence (ADS&CI). In September 2003, the ADS&CI issued a comprehensive plan to reinvigorate NSA's OPSEC Program, and DIRNSA approved NSA/CSS Policy 5-12, *NSA/CSS Operations Security Program*. NSA/CSS Policy 3-6 is still being coordinated.

Overall Report Classification. (U) CONFIDENTIAL//X1

(U) **Medina Regional Security Operations Center (MRSOC)**; NSA/CSS IG; AIA IG; INSCOM IG; NSG IG; and NRO; JT-03-0002, 29 May 2003

Summary. (U~~//FOUO~~) The key findings of this joint inspection center on implementation of the jointness initiatives, site governance, and the adequacy of MRSOC's information technology infrastructure (ITI). MRSOC is making good progress in implementing some joint testbed initiatives, such as rating SCE commanders and establishing a J1. However, there are instances—especially with regard to common workforce training—where the desired end-state is not well defined, making it difficult to measure success. The original RSOC Concept of Operations, developed 10 years ago, is no longer an effective framework to guide decision makers at the sites or HQ in managing and deciding issues of governance, lines of authority, application of conflicting standards or regulations, and funding responsibility. The Joint IG team assessed the MRSOC ITI as woefully inadequate for the constantly expanding mission.

[redacted]

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

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

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

(U) **National Security Operations Center**; NSA/CSS IG, IN-02-0005, 29 May 2003

Summary. (U~~//FOUO~~) The National Security Operations Center (NSOC) manages the activities of the United States Cryptologic System around the clock, 365 days a year and serves as the command and control center for time-sensitive operations and a focal point for crisis response. An inspection team found that Agency leadership needs to define key roles and authorities and to review the responsibilities for Support to Military Operations (SMO). [redacted]

[redacted]

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

Management Action. (U//~~FOUO~~) Management is acting to address all the above issues. The Deputy Director agreed to update NSA/CSS Directive 10-7 to define the roles of the NSOC Executive Agent and the NSOC Director, including the latter's role as Crisis Manager.

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

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

(U) **Industrial Relations**; NSA/CSS IG, ST-02-0005, 4 June 2003

Summary. (U//~~FOUO~~) DIRgram-148 gave the Agency's Corporate Strategy Office (CSO) a key role—to oversee the Agency's relations with industry. However, our review found that the CSO has not provided strategic direction, confined its activities to its oversight role, or implemented appropriate processes and interfaces with NSA components that partner with industry. Also, efforts to acquire a competitive intelligence capability do not comply with DoD and NSA policies that require sponsors to define and validate a need, analyze alternatives, and develop an acquisition strategy. The CSO and [redacted] have not validated the need for this capability or developed a cohesive strategy to acquire it.

Management Action. (U) The Information Assurance Directorate (IAD) concurred with our recommendations, but the CSO questioned the report's factual accuracy and nonconcurred with the recommendations. Contrary to applicable regulations, the CSO did not specify the reason for nonconcurring or identify the allegedly inaccurate facts. Consequently, we referred the report to DIRNSA for resolution.

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

(U) **Oversight Review of the Audit of the Restaurant and Civilian Welfare Funds**; NSA/CSS IG, ST-03-0012, 26 June 2003

Summary. (U//~~FOUO~~) NSA's Restaurant Fund and Civilian Welfare Fund (CWF) are DoD revenue-producing nonappropriated fund instrumentalities (NAFIs) that operate under Army and NSA/CSS regulations for morale and welfare purposes. The financial statements of the two NAFIs were audited by a CPA firm audit firm, which issued unqualified opinions but noted significant problems with segregation of duties and asset security in the drug store operation. In performing the required oversight review of the independent audit, we identified management issues and control weaknesses and recommended improvements to maintain the overall integrity of both funds. We found that persistent management and control deficiencies have adversely affected the financial health of the drug store, while the Ft. Meade Flying Activity, transferred to the CWF in November 2001, lacks a formal program to monitor compliance with Federal Aviation Administration rules.

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

Management Action. (U) The Chief of Employee Morale Services instituted better controls in the drug store, and CWF has improved its oversight of the Flying Activity.

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

~~(C)~~ Office of NSA/CSS Representative [redacted] NSA/CSS IG, [redacted]

Summary. ~~(S)~~ [redacted]

Management Action. ~~(C)~~ Site officials agreed to indoctrinate all newcomers thoroughly and issue formal procedures for all positions; for its part, the Field Advocate Office is developing a plan to ensure that selectees get the requisite functional training before being sent to field sites. In addition, the Agency Contracting Group will compete the site's support contract, and [redacted] is strengthening internal controls.

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

(U) **FY2003 Audit Report on Compliance with the Federal Information Security Management Act**; NSA/CSS IG, AU-03-0007, 28 July 2003

Summary. ~~(C)~~ The audit assessed the progress made by the NSA/CSS Chief Information Officer (CIO) since last year's report on compliance with *The Government Information Security Reform Act*, which was replaced by *The Federal Information Security Management Act of 2002* (FISMA). This year, the DoD IG Office of Intelligence Review asked the OIG to use Office of Management and Budget (OMB) guidance to review the NSA CIO's progress report. We found measurable progress in the areas of physical security and security training. [redacted]

Management Action. (U) Regarding the overarching security policy, management hopes to complete a study of the mission assurance area during the first quarter of fiscal year 2004. The CIO will enforce the requirement for Security Audit Plans during

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

Certification and Accreditation Reviews. [redacted]

[redacted]

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

(U) **Selected Civilian Pay and Leave Entitlements**; NSA/CSS IG, AU-02-0007, 15 September 2003

Summary. ~~(S)~~ In 2001, NSA paid over [redacted] (including base pay, benefits, awards, and allowances). This audit looked at civilian pay and benefits in three categories and evaluated overall payroll system controls. On the whole, we found that employees were paid correctly, but we identified some significant control weaknesses. Controls are not sufficient to ensure that overtime and administrative leave payments are in accord with regulations; this resulted in overpayments of about $75,000. There was no mechanism to prevent Defense Intelligence Senior Level (DISL) executives from receiving premium pay and time-off awards. Some timekeepers and programmers can access and alter their own time and attendance (T&A) data; this violates the basic control principle of separation of duties. Also, eliminating unnecessary duplicate payroll tapes could free up badly needed storage space and save about $22,300 over 6 years.

Management Action. (U) Management agreed to train supervisors on their duties as certifying officials; change the employee category code for DISLs; set a schedule for removing unneeded payroll tapes; and institute controls to prevent improper access to T&A data.

Overall Report Classification. (U) SECRET//X1

(U) **Survey of System Security for NSA Payroll Operations**; NSA/CSS IG, ST-03-0003, 29 September 2003

Summary. ~~(C)~~ To support the payroll audit above (AU-02-0007), we conducted a survey of system security for the NSA [redacted] gets pay entitlement information from [redacted] NSA's Human Resource Management System, and processing hardware from [redacted] a mainframe complex [redacted] In 2001, management made six recommendations to give [redacted] disaster recovery capabilities (part of the Contingency Plan); at the time of our study, only one recommendation was completed.

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

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

~~SECRET//X1~~

Management Action. (U) Management is taking corrective actions, including the completion of all requirements to implement disaster recovery for [redacted]

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

(U~~//FOUO~~) **TRAILBLAZER 1/SIGINT Programs Systems Engineering and Technical Assistance Contract**; NSA/CSS IG, ST-03-0014, 30 September 2003

Summary. ~~(S)~~ The Acquisition and SIGINT Programs Offices mismanaged the administration of a large contract supporting the integration of major SIGINT transformation efforts. [redacted] The contract lacked a satisfactory and consistent task order system that could be used to regularly monitor contract expenditures. These circumstances led to contractor activity and costs that cannot be linked to specific tasks supporting the [redacted] effort and ultimately led to excessively high contractor labor rates. Our analysis found that: (1) sole source cost increases of over [redacted] were improperly based on an unusual novation process; (2) the task order system was not managed in accordance with the Statement of Work and Surveillance Plan, making it hard to effectively monitor the [redacted] of contractor work already completed; and (3) labor rates for at least 25 of the highest priced contractor personnel were excessive. These problems are directly related to inadequate management and oversight of the [redacted] contract. Approximately [redacted] in funds planned for FY2004 and FY2005 option years could be put to better use, depending on scope reductions and savings that result from competition.

Management Action. (U~~//FOUO~~) The Acting Senior Acquisition Executive (SAE) agreed not to exercise the FY2004 option for the contract. Rather, the Acting SAE will negotiate a transition period with the contractor, which will involve: (1) reducing the scope of the contract and (2) redirecting funds to one or more competitively awarded contracts for integrating the SIGINT transformation process. These actions greatly increase the likelihood that the Agency will obtain better value for approximately [redacted] in funds planned for the FY2004 and FY2005 option years.

Overall Report Classification. (U) SECRET//X1

(U) **GROUNDBREAKER Implementation**; NSA/CSS IG, AU-03-0001, September 2003

Summary. (U~~//FOUO~~) GROUNDBREAKER (GB) is the Agency's first large-scale IT outsourcing contract to support the non-mission IT infrastructure. This audit examined several aspects of GB implementation, especially contract management and performance monitoring. We concluded that key elements for managing a performance-based contract were missing. Some contract actions did not comply with laws, regulations, and contract terms; of particular concern was the transfer of [redacted]

to the contractor for unspecified "immediate needs" at the end of the fiscal year. Other actions not in compliance with law and regulation were the expenditure of about [redacted] in wrong year Operations and Maintenance (O&M) funds and work that exceeded the contract scope. The Contracting Officer and Program Manager did not implement a robust contract management program comprising an overall Governance Plan and a Quality Assurance Surveillance Plan (QASP). To date, the contractor has not implemented a disaster recovery plan, as called for in the contract.

Management Action. (U) Management would not agree to obtain a full accounting for the [redacted] and to implement a Governance Plan and QASP. As a result, the OIG referred the report to DIRNSA for resolution. The Comptroller will review the appropriation issues; and management will institute a compliant disaster recovery plan.

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

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

~~(C)~~ Office of NSA/CSS Representative [redacted] NSA/CSS IG [redacted]

[redacted]

Summary. ~~(S)~~ This inspection found that [redacted] provides excellent support to local customers but needs strategic guidance from NSA HQ on various activities; its mission statement has yet to be approved. The site also needs a single focal point at HQ for decisions on mission and IT issues. [redacted] In addition, contract oversight at [redacted] is inadequate, and the site lacks the required property accountability structure.

Management Action. ~~(C)~~ The Foreign Affairs Directorate is developing strategic guidance for many partnerships, including [redacted] and SID is working on a utilization strategy for assets at [redacted] Extended Enterprise Management will issue a formal process for managing field support, and Facilities Services has a plan to fix the power supply at [redacted] is trying to obtain a Contracting Officer's Representative with the requisite technical expertise for effective oversight, and he is also instituting a property accountability structure.

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

(U) [redacted] NSA/CSS IG; AIA IG; INSCOM IG; NSG IG, JT-03-0003, 30 September 2003

Summary. ~~(S)~~ This joint inspection of the [redacted] found the site in the midst of a major transformation, which has greatly affected the Command Climate, Mission Operations, and Mission Systems. The site's transformation is not codified in theater or worldwide architecture; this could jeopardize the entire effort. Specific transfer dates for most targets are needed, while the lack of a

fire-suppression system, first identified in 1988, seriously degrades the ability to protect human life and critical equipment. Moreover, management's implementation of [redacted] requires additional guidance and clarification from HQ; site leadership and HQ have divergent views on the authorities granted to site commanders.

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

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

(U) **Operational Network Evaluations Division**; NSA/CSS IG, IN-03-0002, 30 September 2003

Summary. (U//~~FOUO~~) Operational Network Evaluations (C44) performs security evaluations of operational computer networks for the DoD, the Intelligence Community, and other federal government customers. The customer receives a report that identifies vulnerabilities and recommends countermeasures and improvements. An inspection found that customers have a high regard for C44's products and services, but the lack of documented processes and functions gives rise to some confusion about the Division's role as part of the Defensive Information Operations (DIO) Vulnerability Discovery Triad. Although C44 is a well-managed organization with high morale, it did not have an approved Business Plan and a Mission and Functions Statement. Moreover, the DIO Triad has not been formally defined; the requirement process for network evaluations is also informal, which can lead to confusion.

Management Action. (U) Management agreed to write a Mission and Functions Statement and a Business Plan; to formalize the overall evaluation requirement process—including interactions with other IAD organizations; and to document C44's roles and responsibilities. Our recommendations on clarifying the DIO Triad, which crosses organizational lines, will appear in a special OIG report on the Discover Vulnerabilities function.

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

(U) **Conflict of Interest**; IV-02-0033, 2 June 2003

Summary. (U//~~FOUO~~) An OIG investigation found that an NSA civilian violated DoD regulations by representing his personal company before another federal agency in connection with government contracts. The investigation further concluded that there was a conflict, albeit unintentional, between the employee's outside employment and his official duties—a violation of the applicable Code of Federal Regulations. Since the employee's actions were also a probable technical violation of federal law, we forwarded the report to the Agency's Office of General Counsel for any action deemed appropriate.

Overall Report Classification. (U) SECRET//X1

(U) **Management Deficiencies in the Occupational Safety and Health Program;** NSA/CSS IG, IV-03-0009, 10 July 2003

Summary. (U) An OIG investigation of five injury accidents caused by a malfunctioning NSA elevator revealed management deficiencies in the Agency's Occupational Health, Environmental, and Safety Services (OHESS) organization. Specifically, we found that OHESS violated Federal health and safety regulations by: (1) failing to adequately oversee the Accident Investigations Program to ensure that responsible NSA health and safety officials were conducting adequate safety investigations and trend analyses; and (2) failing to ensure the prompt abatement of an unsafe working condition posed by a malfunctioning NSA elevator. We recommended that (1) OHESS coordinate with the NSA Designated Agency Safety and Health Official and the NSA Office of General Counsel to prescribe specific procedures for OHESS oversight of the NSA Accident Investigations Program; (2) all OHESS safety officials, and all other NSA/CSS employees responsible for conducting safety investigations, receive mandatory training regarding comprehensive safety investigations and the abatement of unsafe workplace conditions; and (3) senior OHESS officials be held accountable for Occupational Safety and Health Program deficiencies, as required by Section E3.1.1 of DoD Instruction 6055.1, *DoD Safety and Occupational Health Program*.

Management Action. (U) Senior OHESS leadership immediately devised a plan to implement the first two recommendations. In addition, NSA executive management is taking measures to carry out the third recommendation.

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

(U) **Time and Attendance Investigation;** NSA/CSS IG, IV-03-0036, 11 September 2003

Summary. (U~~//FOUO~~) An OIG investigation found that an NSA civilian violated DoD regulations and Agency guidance by knowingly and willfully submitting false and inaccurate timesheets. From June 2002 through March 2003, the shortfall to the Government totaled over 113 hours of unearned salary (approximately $3100). Since the employee's actions were also in possible violation of federal law, we forwarded our report to the Office of General Counsel for possible referral to the Department of Justice.

Overall Report Classification. (U) CONFIDENTIAL//X1