

~~CONFIDENTIAL//X1~~

UNITED STATES GOVERNMENT
memorandum
IG-9806-01

DATE: 4 October 2001

REPLY TO
ATTN OF: Inspector General

SUBJECT: Office of the Inspector General Semiannual Report to Congress -
INFORMATION MEMORANDUM

TO: DIR

Thru: D/DIR _____ D/SECRETARIAT _____

1. (~~U//FOUO~~) This memorandum advises you that the NSA/CSS Office of the Inspector General submitted to the Department of Defense Inspector General the Semiannual Report to the Congress on Intelligence-Related Oversight Activities for the period 1 April 2001 - 30 September 2001. For your information, I am providing you with a copy of this report.

2. (~~U//FOUO~~) If you require additional information, please contact [redacted] Deputy Inspector General, on 963-3544s.

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

[redacted]

[redacted]
(b) (6)

ETHAN L. BAUMAN
Inspector General

cc: SID
IAD
CoS

Encl:
a/s

This Document May Be Declassified
Upon Removal of Enclosure and Marked
"UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~."

~~CONFIDENTIAL//X1~~

Approved for Release by NSA on 03-30-2021, FOIA Case # 55478

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE



SEMIANNUAL REPORT FOR THE PERIOD
1 APRIL 2001 - 30 SEPTEMBER 2001

~~CONFIDENTIAL//X1~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

FOR THE PERIOD April 1, 2001 THROUGH September 30, 2001

1. (U) Resident Signals Engineering Program; NSA/CSS IG, IN-01-0008, 22 May 2001

Summary. ~~(C)~~ The Resident Signals Engineering (RSE) Program is designed to satisfy the Agency's critical requirement for Signals Engineers through a 4-year Program to develop this increasingly complex multidisciplinary skill. An NSA/CSS Office of the Inspector General (OIG) inspection looked at Program performance and cost effectiveness. We found that, on balance, the Program appears worth the cost since there are no academic or industry programs to develop Signals Engineers of this caliber; the Regional Security Operations Centers (RSOCs) are not currently used for resident tours or PCS assignments; there is no future TDY or PCS funding line item for the RSE Program; [redacted]

Management Action. (U//~~FOUO~~) Management concurred with our recommendations and will work to obtain the PCS and TDY funding to enable this mission-critical technical development Program to continue. A decision on the need to improve RSE retention rates will be made in the near-term when the size of the next class of Program inductees is known.

Overall Report Classification: (U) ~~CONFIDENTIAL~~

2. ~~(C)~~ [redacted] Division; NSA/CSS IG, [redacted]

Summary. ~~(C)~~ The OIG inspected a [redacted] Division to determine how well prepared this Signals Intelligence Directorate (SID) organization is to serve as a test bed for TRAILBLAZER (TB). During the inspection, we found that the Division had not established a baseline, set performance goals, or adopted a methodology to gauge improvements attributable to TB efforts. [redacted]

Management Action. (U//~~FOUO~~) Management agreed to establish a linguist/analyst efficiency baseline; set performance goals for each new TB-sponsored initiative; and require that all new tools and systems developed under TB automatically track appropriate performance data.

Overall Report Classification: (U) ~~TOP SECRET//COMINT~~

~~CONFIDENTIAL//X1~~

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

~~CONFIDENTIAL//X1~~

3. (U) **Information Technology Standards (Part 1); NSA/CSS IG, AU-01-0001,**
13 June 2001

Summary. (U//~~FOUO~~) At the request of the Chief Information Officer (CIO), the OIG conducted an audit survey to determine the extent of unauthorized purchases of information technology (IT) products that are not on the NSA/CSS Enterprise Solutions (NES) Products Baseline. The survey consisted of hands-on use of transactional data systems and a review of logical architectures, data elements, data element representation, and information derived from the systems that use these data elements. We found that the [redacted] had not agreed to play a role in enforcing the NES baseline, although the CIO IT Planning Policy and Guidance for FY2001 assigns such a role. Part 2 will look at [redacted] the CIO-sponsored initiative to associate IT asset management processes and data repositories.

Management Action. (U//~~FOUO~~) Management officials stated that they had discussed the importance of compliance with IT standards with the [redacted] but the CIO did not clarify whether the CIO IT Planning Policy and Guidance for FY2001 had been formally coordinated with this Group. Although the survey did not include recommendations, an expanded outreach program would help familiarize responsible Agency personnel with the CIO policy requirements.

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

4. (U) **Information Technology Investment Management Processes; NSA/CSS IG,**
AU-00-0006, 25 June 2001

Summary. (U) The purpose of the Information Technology Management Reform Act (ITMRA) of 1996 is to ensure that federal agencies implement a process to base their IT decisions on evidence of direct benefit to mission. The implementing DoD guidance provides a framework for IT investment management (ITIM)—not as isolated acquisitions—but as part of each agency's investment portfolio. To assess the Agency's approach to ITIM, the OIG's auditors used data-gathering and evaluation techniques prescribed by the General Accounting Office and the Office of Management and Budget and endorsed for use within DoD and the Intelligence Community. [redacted]

Management Action. (U//~~FOUO~~) To address the conditions identified in this review, management needs to take steps to establish Investment Review Boards; commit to a comprehensive plan to implement policies, processes, and procedures.

~~CONFIDENTIAL//X1~~

~~CONFIDENTIAL//X1~~

that comprise the elements of sound ITIM; and perform periodic self-assessments—using the same structured questionnaire employed in this review—to objectively assess its progress.

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

5. (U) **Micro-Purchase Credit Card Program;** NSA/CSS IG, ST-01-0007, 5 July 2001

Summary. (U//~~FOUO~~) The DoD mandated that all DoD components implement a Micro-Purchase Credit Card (MPCC) program. In October 2000, the Agency's Senior Acquisition Executive (SAE) asked the OIG to review the MPCC program. The OIG reviewed the internal management controls incorporated into the Agency's MPCC program to prevent waste and abuse. The review found that internal controls are weak in two areas: (1) card certifying officers (CCOs) do not adequately review invoices prior to payment and (2) CCOs and cardholders do not receive written appointment letters that spell out their personal responsibilities and pecuniary liability. We also found that the draft NSA/CSS Regulation 61-07, "Use of Government-wide Commercial Purchase Card," has not been finalized and disseminated nor does it require cardholders to promptly enter purchasing data into the MPCC automated system, which the CCO uses to monitor cardholder spending.

Management Action. (U//~~FOUO~~) Management has agreed to require CCOs to trace selected invoices on the billing statements to the underlying documentation. New cards will not be issued until appointment letters are received from the Contracting Group. Management agreed to incorporate the recommendations of the OIG report in the NSA/CSS Regulation (NSAR) 61-07, and to publish the regulation by 30 July 2001. Once NSAR 61-07 is finalized, the Contracting Group will send all CCOs new appointment letters that state the new requirements and responsibilities, including individual pecuniary liability.

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

6. (U) **Field Advocate Office;** NSA/CSS IG, IN-01-0002, 10 July 2001

Summary. (U//~~FOUO~~) The Field Advocate's Office serves as the NSA focal point for all field-related matters except mission activities and information technology issues. An inspection looked at the office's efficiency and effectiveness and its partnering with other NSA/CSS Headquarters stakeholders supporting the field. The inspection found that the Field Advocate's Office has established its authority over field issues yet its responsibilities are not documented; the Office's governance over other field support organizations is not codified; and Certain field

~~CONFIDENTIAL//X1~~

~~CONFIDENTIAL//X1~~

support functions, e.g., the Cryptologic Services Group budget, the reassimilation process, and the detail process, need further refinement.

Management Action. (U//~~FOUO~~) Management concurred with all recommendations and agreed to formalize its status as the field advocate by documenting its commitment to the field in a mission and functions statement and codifying its relationships with and governance of other field support offices in Service Level Agreements. Management also plans to strengthen accountability for those assigned to mentor reassimilating field personnel.

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

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

7. (U) [redacted] Partnership Contract; NSA/CSS IG, [redacted]

Summary. (U//~~FOUO~~) To create a pool of high-technology private-sector companies from which it can draw, in 1996 the Agency began using a procurement vehicle known as a partnership contract. NSA's first partnership contract to be conducted jointly with another Intelligence Community agency was for the

[redacted] Project. [redacted]

[redacted] Key findings of the audit include: NSA's Business Strategy for the [redacted] contract was abandoned without adequate risk analysis; procurement officials have not removed the root causes of contract administration deficiencies identified in numerous OIG reports; and [redacted] contractors were receiving award fees (AFs) that were much more generous than those they were receiving from other DoD Components for similar services.

Management Action. (U) The Senior Acquisition Executive (SAE) stated that future contracts would strictly adhere to the revised regulation, NSA/CSS 5000R. The SAE set up a review team that is conducting a comprehensive analysis to attack the root causes of persistent contract administration deficiencies. The team will also determine which management controls are needed to ensure that AF payments achieve the intended result. The SAE stated that advance AF payments would be used only when necessary.

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

~~CONFIDENTIAL//X1~~

~~CONFIDENTIAL//X1~~

8. ~~(U//FOUO)~~ **Intelligence Oversight Review of Red Teaming and Information Assurance Readiness Assessments; NSA/CSS IG, ST-01-0002, 27 July 2001** X

Summary. ~~(U//FOUO)~~ The mission of NSA's Red Team is to improve the operational readiness and defensive information operations (DIO) capabilities of DoD entities. The NSA DIO Red Team is a sophisticated interdisciplinary "opposing force" effort that uses active and passive capabilities to expose and exploit customer information operations (IO) vulnerabilities. The OIG reviewed activities conducted by the Agency's Red Teaming and Information Assurance (IA) Readiness Assessments organization and, overall, we found the organization to be control-conscious. Red Team managers and employees demonstrate a positive attitude toward internal controls. Red Team program authorities are well documented in laws and regulations, except for the need to: (1) update and review applicable Agency directives and regulations; (2) standardize Red Team operational documentation and procedures; and (3) document, file, and centralize all Red Team operations and the authorizations to conduct them.

Management Action. ~~(U//FOUO)~~ Management, in consultation with the Associate General Counsel for Information Systems Security, concurred with all recommendations and agreed to update and finalize policy and procedures at the Information Assurance Directorate signature level. Management also agreed to update Red Team standard operating procedures, and the Office of Policy will update Agency directives and regulations to reflect the most current DCI and DoD guidance for IO related activities. Red Team management is currently instituting procedures to ensure their personnel are made aware of the legal protocols related to Red Team operations; write detailed written procedures for describing, documenting, and obtaining approvals to conduct Red Teaming; and standardize procedures for conducting and documenting intelligence oversight training.

Overall Report Classification: (U) ~~SECRET//COMINT//NOFORN~~

9. (U) **GPRA Related Activities at NSA/CSS; NSA/CSS IG, IN-00-0001, 6 August 2001**

Summary. ~~(U//FOUO)~~ The Government Performance and Results Act (GPRA) was enacted in 1993 to increase federal program effectiveness and accountability by focusing on program results, service quality, and customer satisfaction. Although not legally binding on NSA, GPRA prescribes planning, goal setting, and performance measuring processes that are in line with what the Agency needs to do to achieve transformation. The OIG conducted a special study to update a 1999 OIG survey regarding the extent to which NSA had adopted key aspects of GPRA. The latest study found Agency-level Strategic and Business Plans are in place, but there is no regular schedule to review/update existing plans and develop future plans; progress is evident in setting and managing by performance objectives,

~~CONFIDENTIAL//X1~~

~~CONFIDENTIAL//X1~~

but there is no process to ensure that senior officials' performance plans and contracts contain measurable goals linked to the Agency's Strategic and Business Plans. The Agency is collecting and relying on performance data more efficiently—and to a greater degree—than in 1999, but Agency leadership has not articulated exactly what performance information it needs for decision making.

Management Action. (U) The Chief Financial Manager and Office of Executive Programs concurred with all recommendations and agreed to implement a planning calendar, ensure that senior contracts link to Agency-level objectives, and to facilitate a process whereby NSA leadership identifies the performance metrics needed to run the Agency.

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

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

10. (U) **Evaluation of the Assessment of NSA/CSS Information Systems Security;** NSA/CSS IG, AU-01-0010, 10 August 2001

Summary. (U//~~FOUO~~) Last October, the President signed into law the Government Information Security Reform Act (GISRA). The law requires each Federal agency to provide assurances that its systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability. An audit found that in the area of physical and personnel security, compliance with information security policies is very strict. [Redacted]

[Redacted]

Overall Report Classification: (U) ~~CONFIDENTIAL~~

11. (U) **Conflict of Interest,** NSA/CSS IG, IV-00-0046, 10 April 2001

Summary. (U) An OIG investigation found that an Agency senior official attended, as a part-time contractor employee, a meeting with NSA officials at which his industry employer initiated a discussion of NSA funding for a potential contract. In addition, the senior official subsequently telephoned one of the Agency representatives present at the meeting to inquire about the Agency's decision in the matter involving his part-time employer. Although the investigation found that the

~~CONFIDENTIAL//X1~~

~~CONFIDENTIAL//X1~~

senior official did not actually "represent" his company to the government, it was concluded that the senior official created the appearance of doing so. A verbal counseling was administered.

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

12. (U) **Preferential Treatment and Personal Services Issues, NSA/CSS IG, IV-00-0055, 15 June 2001**

Summary. (U) An OIG investigation found that an Agency senior official displayed a preference for the services of two specific contractor employees by moving an Agency support contract to whatever company employed these employees. This was done with no effort to obtain their services competitively or by allowing the contractor to substitute other personnel. Additionally, the investigation found that the senior official and his assistant treated the contract as if it were a personal services contract by exercising relatively continuous supervision and control over the two contractor employees throughout their tenure in the office. Through coordination with the senior official and his assistant, the contractor employees in question were able to remain working on contracts under the senior official's purview over the course of employment with three different companies. The senior official was given a verbal reprimand, while adverse action on his assistant is pending.

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

13. (U) **Misuse of Government Travel Card and Forgery of Official Documents, NSA/CSS IG, IV-00-0054, 13 August 2001**

Summary. (U) An OIG investigation found that an Agency employee misused his Government Travel Card during an extended TDY to Fort Belvoir. During the course of the 14-week TDY, the employee used the card to charge meals for himself and his family outside the TDY area (\$212.73), for unauthorized gasoline purchases (\$901.40), and unauthorized purchases from local retail stores (\$671.93). Also during the course of the TDY, the employee filed interim RTAs in which he requested reimbursement for unauthorized POV miles, totaling \$1407.76. The investigation also found that the employee forged the signature of his approving official on each of the four RTAs he submitted for estimated and reimbursable expenses. The Report of Investigation has been forwarded to Employee Relations and administrative action is pending.

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

~~CONFIDENTIAL//X1~~