Description of document:	National Security Agency (NSA) Inspector General (OIG) Semiannual Reports to Congress, 1997-2003
Requested date:	14-April-2008
Release date:	30-March-2021
Posted date:	19-April-2021
Source of document:	Freedom of Information Act Request 9800 Savage Road, Suite 6932 Ft. George G. Meade, MD 20755-6932 National Security Agency Attn: FOIA/PA Office Fax: 443-479-3612 (Attn: FOIA/PA Office) Submit FOIA Request Online

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 55478C
30 March 2021

This is the final response to your Freedom of Information Act (FOIA) request of 14 April 2008, for records pertaining to "[a] copy of each semi-annual and/or annual report produced by the National Security Agency's Inspector General since the establishment of the NSA IG position." As previously provided, your request has been assigned Case Number 55478. A copy of your request is enclosed. Your request has been processed under the FOIA and the documents requested are enclosed. Certain information, however, has been protected in the enclosures.

Some of the information withheld from the documents was found to be currently and properly classified in accordance with Executive Order 13526. This information meets the criteria for classification as set forth in subparagraph (c) of Section 1.4 and remains classified TOP SECRET and SECRET and CONFIDENTIAL as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause damage to the national security, to include exceptionally grave or serious damage. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA, 5 U.S.C. Section 552(b)(1).

This Agency is authorized by various statutes to protect certain information concerning its activities as well as names of its employees. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 50 U.S. Code 3024(i) and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Personal information regarding individuals has been protected in the enclosures in accordance with the sixth exemption of the FOIA, 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would

constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

  NSA/CSS FOIA/PA Appeal Authority (P132)
  National Security Agency
  9800 Savage Road STE 6932
  Fort George G. Meade, MD 20755-6932
  The facsimile number is 443-479-3612.
  The appropriate email address to submit an appeal is FOIARSC@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. You may also contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. OGIS contact information is: Office of Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, MD 20740-6001; e-mail: ogis@nara.gov; main: 202-741-5770; toll free: 1-877-684-6448; or fax: 202-741-5769.

Please be advised that records responsive to your request include documents containing other government agencies' information. Because we are unble to make determinations as to the releasability of the other agencies' information, the subject documents were referred to the appropriate agencies for review.

CIA has asked that we protect information pursuant to 5 U.S.C. 552 (b)(1) and (b)(3) 50 U.S.C 403g Section 6 of the CIA Act of 1949, and 50 U.S.C. 3024 National Security Act of 1947 Section 102A(i)(1). In addition, DIA has

asked that we protect information pursuant to 5 U.S.C. 552 (b)(1) and (b)(3) 10 U.S.C. 424. Those withholdings have been marked with the code OGA (Other Government Agency). Any appeal of the denial of CIA and DIA information should be directed to those agencies.

Sincerely,

RONALD MAPP
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD
1 APRIL 1997 - 30 SEPTEMBER 1997

Derived From: NSA/CSSM 123-2
Dated 3 September 1991
Declassify On: Source Marked "OADR"
Date of Source: 3 Sep 91

SEMIANNUAL REPORT

FOR THE PERIOD 1 APRIL 1997 – 30 SEPTEMBER 1997

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

COVER NOTIFICATION SYSTEM (C), IN-97-0002, 4 August 1997

Summary. ~~(S)~~ The National Security Agency (NSA) Cover and Sensitive Support Notification System was established to minimize the risk to Agency personnel in sensitive situations or locations, to protect their presence from disclosure, and to ensure that the proper officials are appropriately notified of such activities. During research for an inspection, the Office of Inspector General (OIG) found that the system [redacted] the Director [redacted] is responsible for reporting to the Department of Defense (DoD).

Recommendations. ~~(C)~~ Agency management concurred in all recommended improvements, including revision of National Security Agency/Central Security Service (NSA/CSS) Regulation 120-16 to facilitate compliance with DoD Directive 5105.61, which will set cover policy throughout DoD. [redacted]

DIRECTORATE OF OPERATIONS LABS (U), IN-96-0010, 19 May 1997

Summary. ~~(FOUO)~~ Over the past decade, independent labs were established within the Directorate of Operations (DO) to perform automated data processing tasks which go beyond routine support. Concerned about possible duplication of effort, DO management requested an OIG inspection. The inspection examined [redacted] software labs: [redacted] It found that the newly established [redacted] coordinates lab operations and performs oversight, but challenges remain: adopting a systematic approach to technology insertion, managing requirements, and defining performance measures.

Recommendations. ~~(FOUO)~~ Management responded with plans to establish an Oversight Board to coordinate lab activities and improve technology insertion. A Customer Council will be established to help manage requirements and implement performance measures.

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

PLANNING AND DECISION AID SYSTEM FOLLOW-UP AUDIT (~~FOUO~~), AU-97-0019, 24 July 1997

Summary. (~~FOUO~~) During an audit of the Agency's compliance with the Federal Acquisition Regulation, the OIG found that the proposed sole-source justification to support a contract award to [redacted] over five years was inadequate. The audit surfaced information which was contrary to statements in the sole-source justification.

Recommendations. (~~FOUO~~) Since comparison of the procurement history with current information did not support bypassing competition, the OIG recommended that the program office suspend the procurement, reevaluate the rationale for the justification, and initiate a competitive procurement. The program office subsequently concurred with the recommendations, and three qualified companies were invited to bid on a new 5-year requirement to upgrade the system. While the competitive award process was being readied, management reassessed the level of effort required under the contract. Two contractors submitted bids that were [redacted] The contract was eventually awarded for [redacted] less than the estimated cost of the original proposal (Funds Put To Better Use).

OFFICE OF [redacted] U),

Summary. (~~TS CCO UO~~) An inspection of the Office of [redacted] (A9) was conducted after a series of five incidents since [redacted] wherein A9 personnel improperly disseminated [redacted] BLARNEY in accordance with procedures specified in the Foreign Intelligence Surveillance Act. The inspection found that human error was the main cause of the five incidents, but standing procedures contributed to four of the incidents.

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

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

Recommendations. (~~S-CCO~~) In response to the inspection, A9 conducted a series of lessons-learned briefings for the entire A9 work force to explain the nature of the incidents and the corrective measures taken. The Agency will gather and review existing working aids and procedures for handling BLARNEY material and will consolidate and publish the information for all users.

EMERGENCY ACTION PLANS (U), AU-97-0003, 24 JULY 1997

Summary. (U) Emergency Action Plans (EAPs) are designed to prevent or mitigate damage to people, mission, and resources in the event of an emergency. NSA/CSS Regulation 25-14, "Emergency Action Planning for NSA Field Elements," requires field sites to submit EAPs and to update them annually in light of the risk assessed for the site. An audit found that field sites have not submitted timely EAPs and annual recertifications to Headquarters, as required by the regulation. This widespread noncompliance was traced to a lack of management emphasis on implementing the regulation and the fact that authority to ensure compliance was not assigned to appropriate organization components.

Recommendations. (U) The Agency concurred with the OIG recommendations and scheduled aggressive milestones for corrective action: to revise and ratify NSA/CSS Regulation 25-14, communicate the requirements to field elements, and ensure that non-compliance is promptly reported to Agency management.

MENWITH HILL STATION INSPECTION (U), IN-97-0001, 23 JULY 1997

Summary. (~~FOUO~~) An inspection of Menwith Hill Station (MHS) focused on staffing, support from Headquarters, and personnel administration. The OIG team found civilian morale to be good following the transition to Army Intelligence and Security Command management; however, concerns were identified in the areas of emergency preparedness, housing, promotion board membership, and representation of NSA civilians to site management.

Recommendations. (U) Management concurred in all OIG recommendations. MHS is developing and coordinating a current Emergency Action Plan and updating housing information with the Field Staffing Office. The Office of Personnel has developed an Agency policy concerning promotion board membership at multi-service field sites. The MHS Commander also named a senior spokesperson for NSA civilians at the site.

CASH MANAGEMENT: MENWITH HILL STATION (U), AU-96-0010, 4 August 1997

Summary. (~~FOUO~~) An audit of collection and disbursing operations at Menwith Hill Station (MHS) found that controls need strengthening to reduce the risk that fraud may occur and go undetected. A key internal control technique (separation of duties) had not been implemented over cash collections, and formal accountability had not been established over cash collections for the mass

transit bus service. Also, MHS had not established a debt collection program and was not meeting all the requirements for cash verification and balances.

Recommendations. (U) Agency management concurred with all recommendations. The MHS Deputy Disbursing Officer (DO) established procedures to ensure that cash verification teams perform quarterly reviews of cash holdings and imprest funds. The Deputy DO reduced excess cash balances; the site separated key duties in the area of cash collections, implemented formal accountability over cash collected by the bus service, and will set up a debt collection program.

√ CASH MANAGEMENT: [redacted] SITES (U), AU-97-0009, 27 MAY 1997

Summary. (~~FOUO~~) An audit of [redacted] sites found that the sites need to improve internal controls over disbursing operations and procedures for managing cash holdings. The audit identified problems in three areas:

- [redacted] had not established formal accountability and personal liability for disbursing operations and cash totaling [redacted]
- The [redacted] sites had excess cash balances totalling approximately [redacted] the excess holdings were not needed for operational requirements and could cost the U.S. Treasury [redacted] in unnecessary interest over a 6-year period (monetary benefit); and
- Internal controls are needed to safeguard assets in the area of cash collection and disbursing.

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

Recommendations. (~~FOUO~~) The Office of Finance and Accounting and Assistant Comptroller's Special Operations Office concurred with all recommendations. They will consolidate all cash holdings at [redacted] in a single account and establish formal accountability. Disbursing Officers will periodically review the levels of cash holdings for which they are responsible, and internal controls will be established over cash collection and disbursing activities at the [redacted] sites.

√ CASH MANAGEMENT: AGENT AND CASHIER FUNDS (U), AU-96-0007, 27 May 1997

Summary. (~~FOUO~~) An audit of 36 paying agents and cashiers in the Fort Meade area and at field sites found that improvements are needed in the oversight and management of cash holdings. Specifically, the audit found that although controls over disbursing were generally adequate, quarterly cash verification reviews were not always performed. Also, 20 agents or cashiers were holding [redacted] in excess cash, i.e., beyond what they

are likely to need for operational requirements. This could cost the U.S. Treasury [redacted] in unnecessary interest over a six-year period (monetary benefit).

Recommendations. (U) The Office of Finance and Accounting with all recommendations. Disbursing Officers will review cash holdings twice a year to ensure that they do not exceed operational requirements. They will also ensure that cash verification teams perform quarterly reviews of cash holdings and imprest funds and that any deficiencies noted by the teams are corrected.

JOINT INSPECTION OF [redacted] (~~S-TK~~), [redacted]

Summary. (~~S-TK~~) A joint inspection of the [redacted] conducted in March 1997 by the Inspectors General (IGs) of the U.S. Air Force Air Intelligence Agency, the Army Intelligence and Security Command, the Naval Security Group, NSA/CSS, and the National Reconnaissance Office (NRO). The inspection addressed operational effectiveness and the range of considerations associated with the site's preparations to accommodate the pending large influx of military personnel. Particular attention was devoted to identifying impediments to mission accomplishment, mission planning, mission systems and communications, and manpower and training issues.

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

Recommendations. (~~FOUO~~) The inspection report contained numerous recommendations for improvement. As the lead IG, NRO will provide detailed information on this inspection in their semiannual report.

JOINT INSPECTION OF KUNIA REGIONAL SIGINT OPERATIONS CENTER (~~FOUO~~), JT-97-0002, 21 April 1997

Summary. (~~FOUO~~) A joint inspection of Kunia Regional SIGINT Operations Center (KRSOC) was conducted in January 1997. Participants included IGs from the U.S. Air Force Air Intelligence Agency, the Army Intelligence and Security Command, the Naval Security Group, and NSA/CSS.

(~~FOUO~~) The inspection focused on four major areas: Command Management, Operations, Security, and Information Management. The inspection reported that the KRSOC was accomplishing its mission of producing SIGINT jointly. However, the following issues need to be addressed: lack of a site strategic plan, customer feedback problems, awards/recognition program shortfalls, and the need for a physical security plan along with information system instructions and training.

Recommendations. (~~FOUO~~) The inspection report contained numerous recommendations for improvement. Management agreed with these recommendations and has taken, or plans to take, corrective action.

INVESTIGATION OF INTELLIGENCE SUPPORT TO MILITARY OPERATIONS (~~FOUO~~), IV-97-0068, 6 AUGUST 1997

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

(~~C~~) [redacted] The Agency properly disseminated SIGINT on the incident to its customers, including the responsible military commander and security officials. However, NSA did not disseminate collateral information advising the commander of the travelers' affiliations with NSA or the military. As a result, the commander was unaware of the affiliations during the time of the incident.

(~~FOUO~~) After the travelers departed the foreign country safely, the NSA/CSS OIG investigated the matter. The OIG determined that the Agency's dissemination decisions were made in good faith, based on communications security issues and safety concerns. However, the collateral information should have been legally and securely provided to the command. Regulations allow the Agency to disseminate information (SIGINT or collateral) about U.S. persons when pertinent to their safety.

(~~FOUO~~) As a result, the Agency is taking steps to ensure personnel fully understand their intelligence gathering and reporting roles in support of the military.

DOD INSPECTOR GENERAL SEMIANNUAL REPORT TO THE CONGRESS	NAME OF ORGANIZATION: National Security Agency - OIG	REPORT CONTROL SYMBOL
		AS OF (Enter Date): 30 September 1997

SCHEDULE 1

AUDIT, INSPECTION & INVESTIGATIVE ACTIVITIES – CIVILIAN AND MILITARY PERSONNEL STRENGTH*

ORGANIZATIONAL ELEMENT	CIVILIAN		MILITARY		TOTAL	
	AUTHORIZED (1)	ACTUAL (2)	AUTHORIZED (3)	ACTUAL (4)	AUTHORIZED (5)	ACTUAL (6)
1. AUDIT						
a. CENTRAL AUDIT **						
b. OTHER AUDIT / INTERNAL REVIEW ***	17	15	0	0	17	15
c. CONTRACT AUDIT						
d. TOTAL AUDIT	17	15	0	0	17	15
2. INSPECTION	10	10	1	1	11	11
3. INVESTIGATION	8	7	0	0	8	7
4. TOTALS Other	7 42	7 39	0 1	0 1	7 43	7 40

SCHEDULE 2

AUDIT, INSPECTION & INVESTIGATIVE ACTIVITIES PROFESSIONAL AND ADMINISTRATIVE / SUPPORT PERSONNEL*

ORGANIZATIONAL ELEMENT	PROFESSIONAL PERSONNEL		ADMINISTRATIVE / SUPPORT PERSONNEL		TOTAL	
	AUTHORIZED (1)	ACTUAL (2)	AUTHORIZED (3)	ACTUAL (4)	AUTHORIZED (5)	ACTUAL (6)
1. AUDIT						
a. CENTRAL AUDIT **						
b. OTHER AUDIT / INTERNAL REVIEW ***	16	15	1	0	17	15
c. CONTRACT AUDIT						
d. TOTAL AUDIT	16	15	1	0	17	15
2. INSPECTION	10	10	1	1	11	11
3. INVESTIGATION	7	6	1	1	8	7
4. TOTALS Other	5 38	5 36	2 5	2 4	7 43	7 40

* Do not include augmented staff of some military components to supplement authorized strength. If information on augmentees is available, show as a footnote.

** Central Audit refers to the AIG - AUD, Army Audit Agency, Naval Audit Service, and Air Force Audit Agency.

*** Specify type of activity, e.g. internal review, military exchange, nonappropriated fund instrumentality.

Note: The NSA OIG has two Military augmentees (enlisted) working as inspector

DOD INSPECTOR GENERAL SEMIANNUAL REPORT TO THE CONGRESS	NAME OF ORGANIZATION: National Security Agency OIG	REPORT CONTROL SYMBOL
		FOR THE 6 MONTH PERIOD ENDING (Enter Date) 30 September 1997

SCHEDULE 3
OPERATING COSTS AUDIT, INSPECTION AND INVESTIGATIVE ACTIVITIES

ORGANIZATIONAL ELEMENT	OPERATING COSTS (S IN THOUSANDS)				
	CIVILIAN PERSONNEL (1)	MILITARY PERSONNEL (2)	TRAVEL (3)	OTHER (4)	TOTAL SIX MONTHS COSTS (5)
1. AUDIT					
a. CENTRAL AUDIT *					
b. OTHER AUDIT / INTERNAL REVIEW **					
c. CONTRACT AUDIT					
d. TOTAL AUDIT					
2. INSPECTION					
3. INVESTIGATION					
4. TOTALS Other					

* Central Audit refers to the AIG - AUD, Army Audit Agency, Naval Audit Service, and Air Force Audit Agency.

** Specify type of activity, e.g., internal review, military exchange, nonappropriated fund instrumentality.

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

DOD INSPECTOR GENERAL SEMIANNUAL REPORT TO THE CONGRESS	NAME OF ORGANIZATION: National Security Agency - OIG	REPORT CONTROL SYMBOL
		FOR THE 6 MONTH PERIOD ENDING (Enter Date) 30 September 97

SCHEDULE 7

FRAUD/THEFT INVESTIGATIVE CASE INVENTORY

CASE INVENTORY	NUMBER OF CASES
1. OPEN CASES - BEGINNING OF PERIOD [1]	54
2. CASES OPENED THIS PERIOD	40
3. TOTAL	94
4. CASES CLOSED THIS PERIOD [2]	49
5. OPEN CASES - END OF THIS PERIOD	45
6. CLOSED CASES BY FUNCTIONAL AREA	
a. PAY AND ALLOWANCE FRAUD [3]	7
b. NONAPPROPRIATED FUND FRAUD [4]	
c. PROCUREMENT PROGRAMS/SYSTEMS FRAUD	4
d. COMMISSARY FRAUD	
e. PROPERTY DISPOSAL PROGRAM/SYSTEMS FRAUD	
f. BRIBERY OF GOVERNMENT OFFICIALS	
g. CONFLICT OF INTEREST	
h. DAMAGE, WRONGFUL DESTRUCTION (INCLUDING ARSON)	
i. GOVERNMENT THEFT (OVER $1,000) [5]	
j. CHAMPUS FRAUD	
k. FRAUDULENT PERSONNEL ACTIONS	
l. SUBSISTENCE FRAUD	
m. OTHER [6]	38
n. TOTAL CASES CLOSED BY FUNCTIONAL AREA [2]	49

1/ Must match the number of open cases at the end of the prior period. Explain differences.
2/ Must match total of closed cases by functional area.
3/ Include travel/per diem fraud.
4/ Include military exchange stores and morale/welfare/recreation activities.
5/ Include larceny, theft or wrongful appropriation of Government property, funds, or services whether by forgery, embezzlement, computer fraud, burglary, robbery, and/or other means.
6/ Footnote categories included.

Other: Standards of Conduct
Misuse of Government Resources
False Statements
Mismanagement
Misuse of Government Credit Card
Foreign Intelligence Surveillance Act
Reprisal

DOD INSPECTOR GENERAL SEMIANNUAL REPORT TO THE CONGRESS	NAME OF ORGANIZATION	REPORT CONTROL SYMBOL
	National Security Agency-OIG	FOR THE 6 MONTH PERIOD ENDING (Enter Date) 30 September 97

SCHEDULE 8*
INVESTIGATIVE CASE RESULTS

CASE RESULTS	DOJ (1)	DOD (2)	LOCAL/STATE/FOREIGN (3)
1. LITIGATION RESULTS			
a. INDICTMENTS			
(1) DCIS			
(2) Military Services			
(3) Joint DCIS/Military Services			
b. CONVICTIONS			
(1) DCIS			
(2) Military Services			
(3) Joint DCIS/Military Services			
c. PRETRIAL DIVERSIONS			
(1) DCIS			
(2) Military Services			
(3) Joint DCIS/Military Services			
d. ARTICLE 15s			
(1) DCIS			
(2) Military Services			
(3) Joint DCIS/Military Services			
e. CIVIL SETTLEMENTS/JUDGMENTS			
(1) DCIS			
(2) Military Services			
(3) Joint DCIS/Military Services			
2. MONETARY OUTCOMES *($ Amount in thousands)*			
a. FINES/FORFEITURES			
(1) DCIS			
(2) Military Services			
(3) Joint DCIS/Military Services			
b. RESTITUTIONS			
(1) DCIS			
(2) Military Services (NSA)		659	
(3) Joint DCIS/Military Services			
c. RECOVERIES			
(1) DCIS			
(2) Military Services (NSA Cost Avoidance)		2,380	
(3) Joint DCIS/Military Services			
d. CIVIL SETTLEMENTS/JUDGMENTS			
(1) DCIS			
(2) Military Services			
(3) Joint DCIS/Military Services			

* To be completed by the Assistant Inspector General for Investigations (Defense Criminal Investigative Service data) and the Assistant Inspector General for Criminal Investigations Policy and Oversight (military criminal investigative organizations data).

Doc ID: 6723045

DOD INSPECTOR GENERAL SEMIANNUAL REPORT TO THE CONGRESS	NAME OF ORGANIZATION: National Security Agency - OIG	REPORT CONTROL SYMBOL
		FOR THE 6 MONTH PERIOD ENDING (Enter Date) 30 September 97

SCHEDULE 9*
INVESTIGATIVE CASE RESULTS (ADMINISTRATIVE ACTIONS)

CASE RESULTS	INVESTIGATIVE ACTIVITY		
	DCIS (1)	MILITARY SERVICES (2)	TOTAL (3)
1. CONTRACTOR ACTIONS			
a. DEBARMENTS			
b. SUSPENSIONS			
c. OTHER ACTIONS			
2. PERSONNEL ACTIONS			
a. REPRIMANDS			9
b. DEMOTIONS			
c. TERMINATIONS (Resignation)			1
d. OTHER (Suspension, Counseling)			9
3. MANAGEMENT ACTIONS			

* To be completed by the Assistant Inspector General for Investigations (Defense Criminal Investigative Service data) and the Assistant Inspector General for Criminal Investigations Policy and Oversight (military criminal investigative organizations data).

SCHEDULE 10
NUMBER OF INSPECTION REPORTS ISSUED

CATEGORY		NUMBER OF REPORTS ISSUED
1. GENERAL	N/A	
2. SPECIAL	N/A	
3. OTHER	N/A	
4. TOTAL	N/A	

Doc ID 6723043

INSPECTOR GENERAL SEMIANNUAL REPORT TO THE CONGRESS	NAME OF ORGANIZATION: National Security Agency - OIG	REPORT CONTROL SYMBOL
		FOR THE 6 MONTH PERIOD ENDING (Enter Date) 30 September 97

SCHEDULE 11*
DOD HOTLINE PROGRAM

PROGRAM ANALYSIS	NUMBER OF CALLS AND LETTERS
1. TOTAL CALLS AND LETTERS Less Request for Information and Wrong Number Calls Total Allegations Received	N/A
a. DOD HOTLINE	
b. GAO HOTLINE	
c. OTHER SOURCES	
d. TOTAL ALLEGATIONS RECEIVED	
2. DISPOSITION	N/A
a. SUBSTANTIVE ALLEGATIONS	
(1) Referred to Other Federal Agencies and Departments	
(2) Referred to DoD Components for Information *(No investigation required)*	
(3) Supplemental and Follow-up Contacts with Hotline Sources	
(4) Referred to DoD Components for Action *(Investigation, Audit, or Inspection)*	
(5) Hotline Source Asked to Contact Cognizant Agency Directly *(Allegation appears to warrant some action, but not by the IG, DoD)*	
(6) Subtotal (Substantive)	
b. NONSUBSTANTIVE ALLEGATIONS	
c. TOTAL	
3. STATUS OF ALLEGATIONS REFERRED TO DOD AUDIT, INSPECTION, AND INVESTIGATIVE COMPONENTS	N/A
a. CLOSED	
b. OPEN END OF PERIOD	

* To be completed by the Assistant Inspector General for Social Programs (AIG-SP) only.

SCHEDULE 12*
CONTRACT AUDIT FOLLOW-UP RESULTS
SIGNIFICANT POST-AWARD AUDITS

TYPE OF REPORT	NUMBER OF REPORTS	
	STATUS *(Prior Period)* 970430 (1)	STATUS *(Current Period)* 970930 (2)
1. UNDECIDED *(Less than 6 months old)* 1/	0	0
2. UNDECIDED *(More than 6 months old)* 1/	0	0
3. ACTION COMPLETED DURING PERIOD 2/	1	1
4. ACTION INCOMPLETE, IN LITIGATION *(More than 12 months old)* 3/	0	0
5. ACTION INCOMPLETE, NOT IN LITIGATION *(More than 12 months old)* 3/	3	2
	5	5

* To be completed by the Assistant Inspector General for Audit Follow-up (AIG-AFU) only.

1/ These represent reports for which the extent of support for the audit positions has not yet been decided. (Also in Criminal Investigations)

2/ These are closed reports.

3/ These categories represent reports for which the extent of support for the audit positions has been decided, but actions with the contractor have not yet been completed.

~~SECRET~~

[redacted]

UNITED STATES GOVERNMENT

memorandum

DATE: 20 April 1998 IG-8537-98

REPLY TO ATTN OF: Inspector General

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

TO: DDI, DDO, DDP, DDS, DDT

1. (~~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 October 1997 - 31 March 1998. For your information, I am providing you with a copy of this report.

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

[redacted] (b)(6)

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

ETHAN L. BAUMAN
Inspector General

Encl:
a/s

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1, X3, X5, X6, X7, X8~~

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

~~SECRET~~

~~SECRET~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD
1 OCTOBER 1997 - 31 MARCH 1998

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1, X3, X5, X6, X7, X8~~

SEMIANNUAL REPORT
FOR THE PERIOD 1 OCTOBER 1997 – 31 MARCH 1998

ADVISORY REPORT ON [redacted] (FOUO) (U), [redacted]

Summary. (~~FOUO~~) In April, 1997, Deputy Chief For Technical Services requested audit assistance from the NSA/CSS Office of the Inspector General (OIG) in deciding whether the NSA/CSS should continue to develop and maintain [redacted] even though commercial software with comparable functionality is available. The review found that user requirements and cost information had not been developed and, as a result, the decision to fund in-house software was proving difficult. To assist management, the OIG developed cost information for [redacted] and identified comparable commercial products and costs. The analysis indicated that after 2.5 years, commercial software would pass the break-even point and be more cost-effective. However, to make an informed decision, management needs accurate and current user requirements. A decision on whether to centralize the [redacted] function at NSA/CSS could greatly affect cost projections. Thus, it is essential to develop reliable cost/benefit models for all options under consideration.

[redacted] CRYPTOLOGIC OPERATIONS CENTER (FOUO), [redacted] (C)

Summary. (~~C~~) A joint inspection found the [redacted] to be in transition, due to a vaguely defined mission, dwindling customer interest in its primary target sets, and lower activity levels over the past 7 years. The site would like to be more engaged in area collection efforts but is unclear as to its future posture within the [redacted] An apparent lack of involvement and firm direction by NSA/CSS Headquarters elements has engendered a sense of drift. The inspection also found that the [redacted] and NSA/CSS failed to address many of the deficiencies and recommendations noted in a 1995 joint inspection report, resulting in numerous repeat findings and observations.

Recommendations. (~~FOUO~~) The inspection report contained numerous recommendations for improvement. Management agreed with these recommendations and has taken, or plans to take, corrective action.

[redacted]

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

YEAR 2000 (U), IN-97-0015, 10 December 1997 (~~S-HVCCO~~)

Summary. (~~FOUO~~) To minimize disruptions to Agency operations, the Director issued guidance holding the NSA/CSS Chief Information Officer (CIO) personally accountable for ensuring that Agency systems are Year 2000 (Y2K) compliant by December 1998. At the CIO's request, the OIG conducted an inspection to gauge the Agency's progress on this key issue. The OIG found that NSA/CSS was behind schedule in all five compliance phases mandated by DoD; many Agency managers did not appreciate how Y2K could affect NSA's mission or what they must do to achieve compliance. The inspection concluded that the task is simply too large for the level of manpower currently applied, although resource requirements remain unclear. Radical rescoping of the problem offers the best hope of making critical systems compliant in time.

Recommendations. (~~FOUO~~) All five of the Agency's Key Components concurred in the three recommendations: to develop and implement progress measures, perform risk management, and develop contingency plans. The Agency CIO will monitor progress on the Key Components' actions.

PERSIAN GULF DIVISION (~~S~~), IN-98-0004, 28 January 1998 (~~S-HVCCO~~)

Summary. (~~S~~) An Intelligence Oversight (I.O.) inspection evaluates an organization's compliance with Executive Order (E.O.) 12333, "United States Intelligence Activities," which is implemented by DoD Directive 5240.1," DoD Intelligence Activities," and DoD 5240.1R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons." An I.O. inspection of the Persian Gulf Division (M44) found that the new organization has established good compliance procedures and has also fostered acute awareness of U.S. Signals Intelligence (SIGINT) Directive 18, which states additional responsibilities specific to the U.S. SIGINT system.

TEMPORARY DUTY TRAVEL PROCESS (U), AU-97-0006, 3 MARCH 1998 (~~FOUO~~)

Summary. (~~FOUO~~) The recent reinvention of the temporary duty travel process within the Agency was designed to streamline the process for travellers, decentralize travel budget responsibility, and reduce travel costs by as much as $30 million over a 5-year period. An OIG audit, which was conducted before the process was fully automated, found the new process generally in compliance with

applicable regulations, although such areas as confirmatory and invitational travel needed improvement to achieve full compliance with regulations. The audit also found several features of the new process which, if improved, could decrease travel costs, including using the Commercial Travel Office or the American Express card to obtain rebate income for the Agency and limiting lodging costs.

Recommendations. (U) The Deputy Director for Support Services concurred with all recommendations and is taking corrective action.

TIME AND MATERIALS/AWARD FEE CONTRACTS (U), AU-97-0001, ~~10 February 1998~~

Summary. ~~(FOUO)~~ Time and Materials (T&M) contracts reimburse the contractor for actual hours worked at negotiated fixed rates (which include a profit margin). Since a T&M contract gives the contractor no incentive to control costs, the Federal Acquisition Regulation (FAR) specifies that T&M contracts may only be used when it is impossible to estimate accurately the extent, duration, or cost of the work to be performed. An OIG audit focused on an unusual hybrid used by NSA/CSS: the T&M/Award Fee (T&M/AF) contract. In reviewing a sample of T&M/AF contracts totaling [redacted] the audit found three areas of concern:

- Given the inherent cost risk of T&M contracts, the FAR requires a Determination and Findings (D&F) statement which clearly justifies using this instrument;
- Contracting Officers and their representatives are not routinely performing the extensive oversight required by T&M/AF contracts; and
- Award fee plans by their nature do not contain measurable criteria.

Recommendations. ~~(FOUO)~~ The Office of Contracting (N1) has improved the D&F statements for the contracts discussed in the audit report. To improve contract oversight, Chief, N1 issued a policy reminder and agreed to modify or recompete three contracts where the credentials of contract employees failed to meet contract requirements. However, the N1 did not agree with the key point in the audit regarding establishing measurable criteria to justify award fees. Within this context, the OIG remains concerned about the risks of providing award fees to contractors based on subjective criteria and plans to reassess the use of T&M/AF contracts in about 2 years.

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

~~SECRET~~

UNITED STATES GOVERNMENT

memorandum

DATE: 20 October 1998 IG-8723-98

REPLY TO ATTN OF: Inspector General

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

TO: DDI, DDO, DDP, DDS, DDT

1. ~~(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 1998 - 30 September 1998. For your information, I am providing you with a copy of this report.

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

[redacted] (b)(6)

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

ETHAN L. BAUMAN
Inspector General

Encl:
a/s

cc: DIR
D/DIR
EXEC DIR
EXREG
LAO

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

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1, X3, X5, X6, X7, X8~~

~~SECRET~~

~~SECRET~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD
1 APRIL 1998 - 30 SEPTEMBER 1998

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1, X3, X5, X6, X7, X8~~

~~SECRET~~

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

~~SECRET~~ NSA/CSS OIG

SEMIANNUAL REPORT
FOR THE PERIOD 1 APRIL 1998 – 30 SEPTEMBER 1998

JOINT INSPECTION OF THE MEDINA REGIONAL SIGINT OPERATIONS CENTER (MRSOC) (U), JT-98-0001, 2 April 1998

Summary. (C) The inspection, conducted jointly by the IGs of the Service Cryptologic Elements and NSA/CSS, found the MRSOC to be making steady progress in resolving mission impediments. The intelligence target is effectively worked by highly enthusiastic personnel. Customer satisfaction is high, and organizational support is solid. Effective mechanisms are in place to monitor mission performance and ensure customer satisfaction. On the other hand, the workplace presents serious problems: aging facilities, lack of space, old latrines, an inadequate backup power system, and poor indoor air quality.

Recommendations. (C) Leadership is working this area hard, but costs associated with improvements total [redacted] The new [redacted] will solve some of the problems, but NSA support is needed to help the MRSOC address the many facilities issues.

SELECTED TELECOMMUNICATIONS CENTERS (U), IN-97-0013, 13 April 1998

Summary. (U) Recent advances in telecommunications technology, like the [redacted] The OIG reviewed data from telecommunications centers at [redacted] field sites to gauge the impact of [redacted] technology. The inspection found that reductions in communicator billets were often offset by the need for skilled network managers and systems administrators to maintain and optimize this new technology. [redacted]

Recommendations. (U) After consulting with the sites to determine the skills currently needed to optimize [redacted] technology, management agreed to make appropriate changes to the

military occupational specialty codes and the respective Tables of Distribution to ensure that new assignees have the requisite skills and training.

DIRECTORATE OF OPERATIONS TERRORISM CUSTOMER CENTER, W9B (U), IN-98-0005, 17 April 1998

Summary. (~~S~~) The OIG conducted an organizational inspection of Terrorism Customer Center, the Agency focal point on counterterrorism (CT) for the intelligence, military, and law enforcement communities. The inspection found that morale was high in the Center, but the organization had not developed a strategic plan for the next 2 to 5 years.

Recommendations. (U) The Director for Counterterrorism (DCT) has acted on all the inspection recommendations. Most notably, the DCT is working to develop a long-term strategy that encompasses an Agency-wide CT process.

OFFICIAL REPRESENTATION AND CONFIDENTIAL MILITARY FUNDS (U), AU-97-0016, 13 May 1998

Summary. (U) Since these funds support functions that are unusually sensitive, the Comptroller requested an audit to coincide with assignment of a new funds manager. The audit reviewed internal controls and sampled FY 1996-97 transactions to determine whether the money was used for allowable purposes. The audit concluded that the funds are controlled and monitored appropriately; however the independent annual reviews, required by Agency policy, had not been conducted since 1991.

Recommendations. (U) The Comptroller determined that independent reviews should be conducted every 2 years; responsibility is now assigned to the Office of General Counsel and the Directorate of Plans, Policy and Programs. He also determined that the current level of cash held by Special Operations is necessary to support mission requirements.

LATIN AMERICA AND CARIBBEAN DIVISION (~~S~~), IN-98-0001, 28 May 1998

Summary. (~~S~~) An intelligence oversight inspection of the Latin America and the Caribbean Division found that personnel were keenly

aware of their responsibilities in regard to United States Signals Intelligence Directive (USSID) 18; however, the Division did not have a formal program to make sure that everyone is familiar with the basic intelligence oversight documents: Executive Order (E.O.) 12333, "United States Intelligence Activities," and the Department of Defense and Agency directives and regulations which implement it.

Recommendations. ~~(FOUO)~~ Management concurred with all of the OIG's recommendations. As a result of the inspection, management identified a point of contact for Intelligence Oversight who is responsible for ensuring that all Division personnel are familiar with their individual responsibilities pursuant to E.O. 12333 and its implementing directives. The Division has now established a familiarization and compliance program which includes periodic reminders to all personnel, briefings for newcomers, and procedures for reporting possible violations of E.O. 12333.

[redacted] (U),

[redacted]

Summary. ~~(FOUO)~~ At the request of the Deputy Director for Technology and Systems (DDT), the OIG conducted an audit of the [redacted] The auditors found deficiencies in procurement practices and contract administration. They also discovered that one contractor had not met contractual obligations concerning occupational health, environmental, and safety services. Finally, [redacted] were controlled and accounted for by the contractor, with no oversight by government personnel.

Recommendations. ~~(FOUO)~~ The [redacted] the Office of Contracting, and the Deputy Director for Support Services concurred with all recommendations; corrective actions are underway.

NARCOTICS, CRIME, AND ALIEN SMUGGLING CUSTOMER CENTER (U), IN-98-0002, 12 June 1998

Summary. ~~(C)~~ The OIG conducted an inspection of the Customer Center for Narcotics, Crime, and Alien Smuggling. The OIG team found an enthusiastic work force committed to customer satisfaction and well focused on current mission and near-term initiatives addressing [redacted] perception of disparate treatment pervade the two organizational elements; the elements are devising corporate information technology solutions to analytic and other needs; and the elements do not have

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

a formal program to ensure that all personnel are familiar with Executive Order E.O. 12333. Both the new Director of Crime and Narcotics and the new Customer Center leadership are committed to resolving concerns raised prior to and in the course of the inspection.

Recommendations. (U) Management has already completed the required actions in response to the OIG's recommendations aimed at ensuring organizational element compliance with all the basic intelligence oversight requirements.

JOINT INSPECTION OF THE FORT GORDON REGIONAL SIGINT OPERATIONS CENTER (GRSOC) (U), JT-98-0002, 17 July1998

Summary. ~~(C)~~ The inspection, conducted jointly by the IGs of the Service Cryptologic Elements and NSA/CSS, found that the GRSOC was effective in executing its critical mission and the Operations Directorate was outstanding. However, the investments needed to sustain this level of performance had not been made. In addition, military personnel are burdened with non-mission duties that, combined with frequent extended deployments, limit their availability to conduct mission and develop their cryptologic skills.

Recommendations. ~~(C)~~ Additional efforts are needed to ensure continuity during the rotation of military personnel. RSOC leadership had recognized this shortcoming and began taking steps to address the issue prior to the inspection.

IMPROPER PAYMENTS TO NSA CONTRACTOR (U), AU-98-0003, 21 September 1998

Summary. ~~(FOUO)~~ A caller to the NSA IG alleged that NSA had made improper payments to a contractor who was charging the government (as direct labor) for hours that contract employees spent in training. The contract had no provisions requiring or authorizing the government to pay for training. The audit concluded that the government improperly paid [redacted] for labor hours spent acquiring skills and expertise that the contract statement of work (SOW) had specified as prerequisites for winning the procurement.

Recommendations. ~~(FOUO)~~ Management agreed to negotiate with the contractor to recover the [redacted] and amend the SOW to state explicitly that the contractor is responsible for training its employees.

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

OFFICE OF [redacted] (U), [redacted]

Summary. (~~C~~) The Office of [redacted] is a major part of the National Cryptologic Strategy for the next century. The OIG conducted a special review of this Office's activities to determine (1) the extent and adequacy of policies, procedures, and internal controls governing the office's operations and (2) whether existing policies and internal controls provide reasonable assurance that these activities are carried out with due regard for legal, operational, and other risks. Overall, this review found that the Office's internal control system can provide reasonable assurance that Directorate of Operations and Directorate of Technology and Systems objectives are being accomplished when key policy and procedure documents completely address all aspects of the process. However, the key process documents do not fully describe the requirements flow from all sources; define risk criteria for approvals; and establish a comprehensive set of standard operating procedures for operations.

Recommendations. (~~FOUO~~) Management agreed to update and finalize policy and procedures for requirements and approvals.

ADVISORY ON CONTRACT ADMINISTRATION (U), AU-98-0012, 28 August 1998

Summary. (~~FOUO~~) This advisory review presented a history of Contract Administration (CA) issues reported since 1992 by the OIG and external organizations, corrective actions taken by management, current issues, and management comments. The review found a recurring pattern of CA and contracting officer representative (COR) deficiencies, despite previous corrective actions taken by management. Primary causes of these deficiencies were CORs lacked training and/or experience including certification criteria; an absence of written detailed duties and responsibilities, procedures on performance monitoring, and billing oversight; and minimal COR oversight and accountability. The report also outlined key attributes of effective CA and examples of "best practices" that could be implemented at NSA.

Recommendations. (U) Management concurred with the report's conclusion that CA needs more oversight and is initiating actions to address deficiencies cited in the report.

SENSITIVE INFORMATION (U), ST-98-0003, 31 August 1998

Summary. (~~C~~) A special review found the Office of Cryptanalysis was in substantial compliance with the Directive for Handling Sensitive Information and had implemented adequate controls.

[redacted]

Recommendations. (~~FOUO~~) Management concurred with all recommendations and agreed to document all corrective actions in the planned revision of the Directive.

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

[redacted] PROGRAM (U), [redacted]

Summary. (~~S~~) [redacted] the program has spent approximately [redacted] on equipment and contractor services. The OIG conducted an audit and found that [redacted] is operating without the prioritized requirements and long-range plan it needs to operate efficiently and expand to additional sites. The audit also found that oversight of [redacted] invoices by responsible Agency personnel is not adequate because charges are not traced to supporting documentation.

Recommendations. (~~FOUO~~) [redacted] managers have agreed to provide the Agency with a long-range written plan. The Office of Contracting will develop additional guidance for certification of invoices, and the Contracting Officer will meet with the COR to review his duties and responsibilities in detail.

MIPRs PROCESSED BY THE [redacted] OFFICE (U), AU-97-0006, 14 September 1998

Summary. (~~FOUO~~) The audit of Military Interdepartmental Purchase Requests (MIPRs) processed by the [redacted] Office was initiated after the OIG was contacted by Agency employees who were

concerned about possible misuse of the instrument. The Program Office sponsored 80 MIPRs which did not directly support an approved Agency mission; it also initiated procurement requests that used [redacted] of external customer funds for purposes other than those stated on the MIPR.

Recommendations. (~~FOUO~~) Managers agreed to establish oversight of the MIPR acceptance process, implement internal controls over the associated PR process, and terminate the project. The Comptroller agreed to make necessary accounting adjustments to return customer funds.

FOLLOWUP AUDIT ON THE SPECIAL PROCESSING LABORATORY (U), AU-98-0007, 29 September 1998

Summary. (~~FOUO~~) In April 1996, the OIG issued a report on the Special Processing Laboratory (SPL) which focused on the issue of contract oversight. The objective of this followup audit was to determine whether management corrected the previously-identified contracting deficiencies. This followup review confirmed that management corrected the deficiencies. The key improvements found were: reconciliation of contractor invoices to the Cost/Schedule Status Report prior to expending funds; a detailed Statement of Work for the current SPL contract on contractor qualifications; and completed training on the responsibilities of CORS for appropriate contracting personnel.

Recommendations. (~~FOUO~~) There were no recommendations for this followup audit and management agreed with the findings.

FOLLOWUP REVIEW OF THE [redacted] INSPECTION (U), [redacted]

Summary. (~~FOUO~~) The OIG evaluated management actions following the FY 1996 OIG inspection of the [redacted] organization which recommended actions to correct organizational problems. The followup inspection found that management has made major improvements in the work environment. Employees and management alike provided evidence of gains and beneficial outcomes. For example, the work force described the new performance measures as equitable and consistent; awards are distributed fairly, and employees like the fact that recognition is not based solely on output but also recognizes contributions to the organization; and

after the team was disbanded, most of its members received desirable new assignments and were subsequently promoted or recognized as high achievers, which restored their morale and self-respect.

Recommendations. ~~(FOUO)~~ There were no recommendations for this followup inspection and management agreed with the findings.

SPECIAL EMPHASIS AREA: YEAR 2000 PROJECTS (U)

COMMERCIAL OFF-the-SHELF (COTS) PRODUCTS (U), AU-98-0013, ONGOING

~~(FOUO)~~ The objective of this ongoing audit is to determine whether the Agency has taken prudent actions to reduce its operational risks associated with reliance on COTS information technology products. Specifically, the audit is focusing on the Agency's methodology used to determine COTS compliancy for critical mission and administrative systems, and verification of the validity of current year 2000 product evaluations. Additionally, the audit is verifying that responsibility and accountability has been assigned to ensure the compliance of specific COTS products. Planned report date is January 1999.

RENOVATION AND TESTING OF IN-HOUSE AND CUSTOMIZED SOFTWARE (U), AU-99-0004 , PLANNED

~~(FOUO)~~ The objective of this planned audit is to evaluate whether the Agency has identified all of its in-house developed and customized software that supports NSA mission critical systems and whether Key Components are taking adequate steps to ensure that their systems will continue to function at the millennium. Planned report date is June 1999.

CONTINUITY OF OPERATIONS - CONTINGENCY PLANNING (U), AU-99-0005, PLANNED

~~(FOUO)~~ The objective of this planned audit is to evaluate whether the Agency is adequately assessing its year 2000 risks and developing contingency plans that can successfully manage those risks. The audit will evaluate individual contingency plans for adequacy and, in particular, whether external dependencies have been sufficiently taken into account. Planned report date is September 1999.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNITED STATES GOVERNMENT

memorandum

IG-9071-99

DATE: 16 April 1999

REPLY TO ATTN OF: Inspector General

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

TO: DDI, DDO, DDP, DDS, DDT

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 October 1998 - 31 March 1999. For your information, I am providing you with a copy of this report.

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

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

[redacted] (b)(6)

ETHAN L. BAUMAN
Inspector General

Encl:
a/s

cc: DIR
D/DIR
EXEC DIR
EXREG
LAO

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD
1 OCTOBER 1998 - 31 MARCH 1999

SEMIANNUAL REPORT
FOR THE PERIOD 1 OCTOBER 1998 – 31 MARCH 1999

(U) CONTRACT COST AND PRICING DATA, AU-98-0006, 8 October 1998

Summary. (U) This audit evaluated Agency procedures for handling, processing, and reporting on defective pricing actions. No instances of noncompliance with prescribed regulations were noted. Contracting Officers' (COs) resolutions of defective pricing issues were generally supportable and documented in the contract file. We found that, overall, management had an effective contract audit followup system, and the semiannual status report on contract audits was generally current, accurate and complete.

Recommendations. (U) The audit noted three areas for improvement: Maryland Procurement Office (MPO) guidance needs to be updated so it more accurately reflects current operating procedures; current MPO guidance does not clearly state the procedures available that COs may use to address defective pricing issues within the required timeframe; and a post-award issue identified by the Defense Contract Audit Agency in 1993 is still unresolved. Management concurred with the findings, agreed to update and revise MPO guidance, and to settle the outstanding post-award issue.

(U) NSA INTELLIGENCE SUPPORT TO COUNTERTERRORISM, IN-98-0006, 23 November 1998

Summary. (U//~~FOUO~~) This inspection focused on the Agency's support to the customers engaged in the fight against international terrorism. The primary aim was to gauge customer satisfaction and to see if there were any areas that could be improved. The team surveyed eight counterterrorism (CT) customers and visited [redacted] NSA offices of primary interest and support organizations. Overall, the inspection found these customers to be very satisfied with the support they receive from NSA. Moreover, the National SIGINT Requirements Redesign Team is working to streamline the entire requirements process, thereby enhancing NSA's ability to support CT. Of the customers interviewed, about 80 percent complained that distribution restrictions on special series reports, [redacted] keep the reports from reaching some of the people who need to act on them.

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

Recommendations. (U//~~FOUO~~) As a result of this finding, two Operations organizations are conducting a review of the [redacted] will explain the process to customers who want to request expanded distribution and will coordinate all requests.

(U) NSA'S QUICK REACTION DEPLOYMENT OPERATION, IN-98-0007, 25 November 1998

Summary. (U//~~FOUO~~) This intelligence oversight inspection of [redacted] NSA's quick reaction capability deployment operation, assessed whether [redacted] is in compliance with Executive Order (E.O.) 12333 and its implementing directives and regulations. The inspection also reviewed quick reaction deployment procedures for reporting possible violations and educating all personnel about their individual responsibility regarding compliance with these authorities. The inspection found [redacted] management and staff to be compliant with E.O. 12333 and its derivative document requirements; it maintains a healthy dialog with the Office of General Counsel (OGC) and is commendably proactive in advising the OGC of upcoming deployments with E.O. 12333 implications.

Recommendations. (U) Management of the [redacted] program concurred with recommendations to enhance the organization's existing E.O. 12333 compliance program. Every new assignee will receive an intelligence oversight briefing, and an OGC representative will visit the [redacted] location annually to discuss E.O. 12333 and related requirements with all [redacted] personnel.

(U//~~FOUO~~) JOINT INSPECTION OF THE [redacted]

Summary. (U) The inspection, conducted jointly by the IGs of the NSA/CSS and Air Intelligence Agency, found that the day-to-day mission is being carried out effectively and consistent with NSA/CSS policy, guidance, and direction. There is good communication throughout the organization and between key functional areas. Two functional areas that do not meet standards are physical security and safety. There are a number of findings in these areas requiring the attention of [redacted] and NSA/CSS management.

Recommendations. (U) The inspection report contained numerous recommendations for improvement. Management agreed with these recommendations and has taken, or plans to take, corrective action.

(U) COMSEC MATERIAL MANAGEMENT, AU-97-0018, 6 January 1999

Summary. (U//~~FOUO~~) Communications Security (COMSEC) material control is based on a system of centralized accounting and decentralized custody and protection.

Recommendations. (U) Management has agreed to develop a prioritized list of procedures for COMSEC account managers and train them to use automated tools to ensure that data in the Central Office of Records is current and accurate. They will improve followup on delinquent accounts to achieve compliance with the national standards for safeguarding COMSEC materials. To improve risk management, COMSEC assistance visits will be prioritized to make sure that large accounts with delinquent inventories are audited at least biannually. A formal memorandum of agreement with DSS has already resulted in more frequent coverage of assigned accounts.

(U) FUNDING FOR OPERATIONS SUPPORTING LAW ENFORCEMENT, AU-98-0002, 7 January 1999

Summary. (U//~~FOUO~~) As a by-product of its Signals Intelligence (SIGINT) collection activities, NSA reports are produced that benefit law enforcement activities. The Consolidated Cryptologic Program funds broken out directly for support to law enforcement were supplemental appropriations in FY97 and FY98. Resulting from Congressional budget actions, these funds are earmarked for equipment and travel to support counterterrorism. In addition, NSA receives funds from the Department of Defense (DoD) Counterdrug Intelligence Program (CDIP).

Recommendations. (U) The Director of Crime and Narcotics agreed to develop a uniform written planning procedure for committing CDIP funds in order to meet DoD and Agency guidance.

(U) ADVISORY ON INTELLIGENCE OVERSIGHT SURVEYS, ST-99-0005, 22 January 1999

Summary. (U) The OIG has broad responsibility to inspect for compliance with the Constitution, laws, executive orders, directives, regulations and rules governing intelligence oversight and the conduct of the Agency's missions. In 1997, the OIG concluded that if the Agency only used traditional methods, existing resources would allow us to cover just a fraction of the Agency's people and programs. In order to expand coverage, the OIG developed a new technique: the Executive Order (E.O.) 12333 Survey Program. With management input, the OIG wrote separate questionnaires tailored to elements in all five Key Components. Detailed analyses of the survey results were provided to the senior management of each organization surveyed. Our analysis of the survey results shows that Agencywide, there is no single method or program for ensuring E.O. 12333 compliance and awareness. Despite the lack of standardized familiarization procedures, employees seem generally aware of how the rules govern the conduct of their missions, although not all are able to cite the particular E.O. 12333 section or DoD Regulation 5240.1-R procedure that applies. Some managers have begun using the survey as a training tool.

(U//~~FOUO~~) OVERALL REPORT ON THEMED REVIEWS - LAW ENFORCEMENT, ST-99-0004, 3 February 1999

Summary. (U//~~FOUO~~) During FY98, the OIG conducted a series of inspections and audits that focused, in whole or in part, on a single theme: the Agency's mission to support the nation's law enforcement community. This report captures and interrelates findings, observations, and recommendations from the individual themed projects. This review found much that was heartening, particularly the extent to which everyone involved is dedicated to serving the law enforcement customer. Based on customer interviews, the OIG concluded that these external customers appreciate the support they get from NSA. Where there were procedural glitches or controls that needed improving, the OIG was able to enlist management to remedy the problem.

[redacted]

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

(U) JOINT INSPECTION OF BAD AIBLING STATION (BAS), JT-99-0002, 5 February 1999

Summary. (U//~~FOUO~~) The inspection, conducted jointly by the IGs of the Service Cryptologic Elements and NSA/CSS, found that uncertainty about the site's future and changing guidance and direction affecting the operations have contributed to a general decay in station facilities and infrastructure. A host of new initiatives to repair, improve, or establish facilities to address some of the most important concerns is underway. However, force protection and infrastructure security issues present major problems requiring resources beyond that now available for the Station to support. BAS leadership was critical of the NSA operations mission transition planning process, despite the existence of the BA Transition Team. In general terms, station management expressed a high degree of dissatisfaction and frustration about the lack of NSA guidance, feedback, and even routine communication to the site with respect to mission transition planning. There is, however, universal support from senior leadership at the station for the creation at NSA Headquarters of a "station advocate" for BAS with access to the agency's top leaders. In light of the decision to keep BAS open, NSA and the Army's Intelligence and Security Command (as the Executive Agent) must redefine roles and responsibilities of the various organizations to ensure complete understanding.

Recommendations. (U) The inspection report contained numerous recommendations for improvement. Management agreed with these recommendations and has instituted a formal process for tracking all of its corrective actions.

(U) OFFICE OF SECURITY SERVICES - SUPPORT, AU-98-0014, 8 March 1999

Summary. (U//~~FOUO~~) The OIG is conducting a managemen the Office of Security Services (OSS) in two phases. The f placed special emphasis on management controls in the suppc The review found that the overall policies and procedures that management has established to control and account for ammunition, badges, uniforms, radios, and weapons provide reasonable assurance to preclude future significant losses through misappropriation or theft. Also, OSS management did not have a process to involve the Office of Facilities Services in plans and decisions about security for construction, renovation, or lease of real property. Thus, security concerns of the OSS were not addressed early on, increasing potential security risks and the cost of security retrofits. In addition, the OSS was not in compliance with NSA/CSS Regulation 120-12, *Personnel Security Program for Continued Access*, which requires a reinvestigation polygraph at 5-year intervals for all NSA employees and contractors with access to Sensitive Compartmented Information. The second phase of the review will focus on the OSS mission.

Recommendations. (U//~~FOUO~~) Management agreed with all recommendations and to initiate action to develop a formal approval process to ensure security provisions in current and future plans for Agency real property construction, renovation, or lease. In addition, management has developed a strategy to address the Agency's current noncompliance regarding reinvestigation polygraphs; however, management needs to make decisions regarding the polygraph billet shortage within the OSS, and an incentive/retention program for polygraphers. Finally, if it is not feasible to acquire polygraph skills internally, management may require concurrence from the Human Resources Review Group for outside hiring authority.

(U) MISCONDUCT REGARDING OFFICIAL TRAVEL, IV-97-0061, 9 March 1999

Summary. (U//~~FOUO~~) This investigation substantiated allegations of misconduct by an Agency employee related to official travel. Briefly summarized, the OIG found the employee improperly accepted $12,854 in compensation from a non-Federal entity for official government travel expenses without prior authorization on 17 occasions; improperly served in a position of fiduciary responsibility for the entity; knowingly submitted false, duplicate, and improper claims to the government relating to official travel; improperly converted 130,000 frequent flier miles for personal use;

and improperly claimed 51.25 regular hours, credit hours and/or overtime while in a travel status. The employee resigned from the Agency and appropriate collection action has been taken to recover $5,774 due to the Government.

(U) TRAVEL IMPROPRIETIES AND NEPOTISM BY A SENIOR OFFICIAL, IV-98-0002, 16 March 1999

Summary. (U//~~FOUO~~) This investigation found the senior official had solicited airline upgrade coupons that were provided based on the official's senior position; changed a personal trip to an unnecessary TDY that was charged to the Agency; and violated nepotism laws and regulations by advocating the hiring of a spouse. The official received a written reprimand and was directed to reimburse the U.S. Treasury for all costs associated with the unnecessary TDY that was charged to the Agency, and the Agency will recoup the salary paid to the spouse in accordance with applicable laws.

~~SECRET//NOFORN//X1~~

UNITED STATES GOVERNMENT

memorandum

IG-9296-99

DATE: 26 October 1999

REPLY TO ATTN OF: Inspector General

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

TO: DDI, DDO, DDCM, DDS, DDT

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 1999 - 30 September 1999. For your information, I am providing you with a copy of this report.

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

[redacted]

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

ETHAN L. BAUMAN
Inspector General

[redacted]

(b)(6)

Encl:
a/s

cc: DIR
D/DIR
EXEC DIR
EXREG
LAO

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

~~SECRET//NOFORN//X1~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD
1 APRIL 1999 - 30 SEPTEMBER 1999

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1, X3, X5, X6, X7, X8~~

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

~~SECRET//NOFORN//X1~~

SEMIANNUAL REPORT
FOR THE PERIOD 1 APRIL 1999 – 30 SEPTEMBER 1999

1. (S) [redacted] SUPPORT, [redacted]

Summary. (S) This audit assessed the effectiveness and efficiency of contracting and financial practices at the [redacted] Both NSA and CIA assign contracting officers to [redacted] The auditors found several areas that require improvement: there is a higher percentage of sole-source contracting at [redacted] than at CIA or NSA (about 30 percent higher than NSA); CIA's delegation of contracting authority to an [redacted] division chief violated good internal control practices; and the [redacted] disbursing office maintained excessive amounts of cash even though the monthly requirement was only about one-fourth of this amount.

Recommendations: (S) The [redacted] NSA's Office of Contracting, and CIA's Office of Finance and Logistics (OFL) managers agreed to undertake new initiatives to improve competition and ensure that contracting regulations are followed. [redacted] and OFL agreed to reduce the cash but did not agree to the recommendation to rescind the contracting authority of the [redacted] division chief; the CIA IG will handle this issue.

2. (S) [redacted] MISSION, [redacted]

Summary. (S//NF) This is the second of two joint audits conducted by the CIA IG and NSA/CSS IG (OIG) offices. The first report concentrated on contractual and financial responsibilities and the second audit focused on [redacted] support to law enforcement agency (LEA) personnel at [redacted] sites. It also examined the adequacy of emergency planning and response, training, equipment, and compliance with NSA directives. The audit found that the [redacted] sites have a close, productive working relationship with LEA personnel, but the sites had infrequent to no relations with LEA personnel. This was partly due to a lack of formal policy guidance on when and how to establish such relationships. The auditors also found that [redacted] sites have not always prepared or updated their Emergency Action Plans (EAPs) as required by NSA/CSS Regulation Number 25-14.

Recommendations. (S) [redacted] management concurred with all audit recommendations and plans to initiate formal procedures for establishing relations with LEA personnel at field sites. In addition, [redacted] management has established followup procedures to

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

ensure that field sites implement recommendations to correct EAP deficiencies during periodic [redacted] security reviews. Finally, [redacted] management has agreed to update EAP field instructions and establish a coordinator to manage the EAP program.

3. (U) SURVEY OF INFORMATION TECHNOLOGY INFRASTRUCTURE, IN-99-0007, 30 April 1999

Summary. ~~(C)~~ The inspection survey team reported that the Agency's Information Technology Infrastructure (ITI) – upon which it depends for mission success and routine tasks – [redacted] the cost to modernize it is not currently included in Agency budgets. The survey identified issues that warrant immediate attention by Agency leadership, particularly achieving corporate management of the ITI and addressing ITI planning at all levels as an integral part of corporate business planning. There are few metrics to gauge ITI performance, [redacted]

Recommendations. ~~(U//FOUO)~~ The survey made no formal recommendations but identified key issues for NSA Leadership to address. The charter establishing the Agency's Chief Information Officer (CIO) has been revised to give the new CIO management responsibility over corporate IT resources. Based on the survey, the NSA OIG conducted inspections of two organizations that are key role players in ITI readiness and modernization; the reports will be issued during the first quarter of FY 2000.

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

4. (U) SIGINT REPORTING FOR A PRODUCTION DIVISION, IN-99-0008, 30 April 1999

Summary. ~~(C)~~ This Intelligence Oversight (I.O.) inspection of SIGINT reporting for a production division found that personnel were keenly aware of their I.O. responsibilities, but did not have a formal program to make sure everyone is familiar with the basic I.O. documents: Executive Order 12333 and its implementing directives and regulations. Coincidental with the inspection, one of the division's offices launched an I.O. training initiative that will be implemented throughout the organization. In addition, the division appointed a Point of Contact (POC) for I.O. who will share the responsibility for familiarization and training with another POC.

~~SECRET//NOFORN//X1~~

5. (U//~~FOUO~~) JOINT INSPECTION OF THE DENVER FIELD STATION, JT-99-0003, 6 May 1999

Summary. (U//~~FOUO~~) This joint inspection by the IGs of the Service Cryptologic Elements (SCEs) and NSA/CSS assessed three interest items noted by the Director, NSA/Chief, CSS: mission integration, reliability of mission, and military member support. Other areas inspected included site command, operations, and support functions. The site recognizes and has taken direct action to integrate operational processes within its purview. Despite the limitations of various stovepipe systems that were delivered during the past few years, site initiatives have made mission integration more of a reality. More difficult integration issues exist, such as solving a problem of multiple management information systems. Regarding reliability of mission, most of the critical infrastructure elements that are required to sustain the site's operations have built-in redundancies that allow site operations to continue with minimal interruption. The inspectors found that good efforts have been made in the past several years by all appropriate commanders at the site to improve active duty military support. However, to improve morale and operational effectiveness, more work is required to provide full-service dining facilities, expanded fitness and recreational opportunities, and emergency services on a 24 hour, 7 days per week basis.

Recommendations. (U) The inspection report contained numerous recommendations for improvement. Management agreed with these recommendations and has taken, or plans to take, corrective action.

6. (U) Y2K EFFORTS CONCERNING COMMERCIAL OFF-THE-SHELF PRODUCTS, AU-98-0013, 21 May 1999

Summary. ~~(C)~~ The Year 2000 (Y2K) problem is rooted in the way automated information systems record and compute dates. This audit found that many of NSA's most critical systems have components that were not developed or supported in house but are commercial off-the-shelf (COTS) products purchased from vendors. [redacted] any COTS components that are not Y2K compliant could adversely affect the Agency's mission. The auditors also noted that [redacted]

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

~~SECRET//NOFORN//X1~~

Recommendations. ~~(C)~~ Management concurred with all recommendations and took the following actions: 1) included end-to-end system interface information identifying NSA's highest priority systems in an upgraded Information Technology Inventory Database; 2) added the "vendor's definition of compliance" and "vendor's compliance testing" to the COTS database for those products for which the vendor provided the information; and 3) started making use of the DOD Joint Integration and Test Facility test information on COTS products. These actions will reduce the risk of Y2K disruptions to NSA's most critical missions.

7. (U) SYSTEMS AND NETWORK OPERATIONAL EVALUATIONS, ST-99-0001, 28 May 1999

Summary. (U~~//FOUO~~) During this special study, a systematic review of the Systems and Network Center (SNC) activities was conducted to determine the extent and adequacy of policies, procedures, and internal controls governing the Center's operations, and whether existing policies and internal controls provided reasonable assurance that these activities were carried out with due regard for legal, operational, and other risks. The study found the SNC to be control conscious and personnel at all levels demonstrated personal and professional integrity; the Memorandum of Understanding (MOU) with the National Institute of Standards and Technology (NIST) had not been reviewed since 1989 and did not address reimbursement for SNC services; the process for approving requests for services had not been formalized; and written procedures for conducting operational evaluations did not address the provision of technical assistance to law enforcement agencies.

Recommendations. (U~~//FOUO~~) Management concurred with all recommendations and agreed to update and finalize policy and procedures for all SNC requirements, approvals and services. The SNC further agreed to institute procedures to ensure testing personnel are aware of the legal protocols. The Associate General Counsel for Information Systems Security will review and update the MOU with NIST and coordinate with appropriate offices to update and finalize NSA/CSS Regulation Number 130-3.

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

~~SECRET//NOFORN//X1~~

8. (U) FOLLOWUP INSPECTION ON NUCLEAR COMMAND AND CONTROL, AU-99-0009, 20 July 1999

Summary. ~~(S//NF)~~ [redacted] This followup review focused on these recommendations to determine whether management had implemented the recommendations or taken alternative actions that satisfied their intent. Overall, the inspection found that NC2 management had implemented most of the recommendations. Improvements were made in key areas: [redacted]

Recommendations. ~~(U//FOUO)~~ Management has agreed to designate NC2 positions for priority staffing and to establish an NC2 entry-level hiring program. Management also plans to complete a comprehensive vulnerability assessment by 31 December 1999, while the Office of Security will conduct [redacted] polygraphs of PRP personnel.

9. ~~(C)~~ JOINT INSPECTION OF MENWITH HILL STATION, JT-99-0004, 10 September 1999

Summary. ~~(C)~~ The inspection, conducted jointly by the IGs of the SCEs and NSA/CSS, found that overall the Menwith Hill Station (MHS) command climate is healthy; policy and guidance from higher headquarters is effective but there are deficiencies with respect to an overall lack of formal, written guidance; a dedicated MHS work force carries out a dynamic, [redacted] the communications and network division is competently run and professionally staffed; and MHS is establishing strong environmental safety and health programs.

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

Recommendations. (U) The inspection report contained recommendations for improvement. Management agreed with these recommendations and has instituted a formal process for tracking all of its corrective actions.

10.

(U) SPOUSAL ACCOMMODATIONS, ST-99-0006, 17 September 1999

Summary. (U//~~FOUO~~) This review was initiated in response to a request from the Inspector General, Department of Defense (IG DoD) to the Director, NSA/Chief, CSS to review the overseas spouse hiring program at NSA. The IG DoD was concerned that NSA's spouse hiring program appeared to give spouses of NSA employees undue employment advantages that are generally not available to other DoD family members overseas. As a result, the Director was asked to review the program to ensure its compliance with applicable regulations and avoids the perception of favoritism. This review determined that a vast majority of spouse hires (67 of 73) at field sites in FY 1997-1998 were accomplished in accordance with Merit System Principles and applicable regulations. In these hires, competitive procedures were followed in selecting spouses of NSA employees for vacant part-time indefinite positions. The OIG concluded that on six occasions in FY 1997-1998 spouses were placed in newly created positions, without competitive procedures, contrary to Merit System Principles. Furthermore, when competitive procedures were utilized, the spouses of NSA employees were not given employment preference. By contrast, within the DoD community outside of NSA, spouses and family members of DoD military and civilian personnel receive employment preference under DoD regulations that do not apply to NSA.

Recommendations. (U//~~FOUO~~) To avoid a recurrence of the occasions where non-Agency spouses were hired contrary to the Merit System Principles, the OIG recommended that the Deputy Director for Support Services ensure that appropriate corrective actions are taken in coordination with the NSA Office of General Counsel. These corrective actions include educating the work force and Agency senior officials about Merit System Principles and restrictions under the nepotism laws and regulations, and advising employees that Agency policy prohibits employees from making employment for their spouse a contingency for their accepting a PCS assignment.

(U) OFFICE OF SECURITY SERVICES MANAGEMENT REVIEW - MISSION, AU-99-0011, 20 September 1999

Summary. (U//~~FOUO~~) This audit is the second and final phase of a management review of the Office of Security Services (OSS). The first phase placed special emphasis on management controls in the support area. For a summary of this review, please refer to the Semiannual Report as of 31 March 1999. Phase II, the subject of this report, focused on compliance with investigative authorities, policies, and procedures. The phase II audit report found that, with the exception of two cases, the OSS' Reports of Investigation (ROIs) and Memoranda for the Record (MFRs) did not disclose any actions by Special Agents that were not in compliance with investigative authorities, policies, and procedures; the OSS did not have a record of adjudicative actions taken on [redacted] of the [redacted] ROIs and MFRs reviewed; about [redacted] percent of the automated information systems (AISs) did not have the certifications and accreditations required for operation; and approximately [redacted] percent of the data in the case control system was not accurate or complete.

Recommendations. (U//~~FOUO~~) Management agreed with our recommendations to document the new procedure for recording adjudicative dispositions; develop a Certification and Accreditation Plan (with milestones) to secure all AISs; and establish quality control measures for entering data in the new case control system, which is currently under development.

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

~~SECRET//X1~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/

CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD

1 OCTOBER 1999 - 31 MARCH 2000

~~SECRET//X1~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

FOR THE PERIOD OCTOBER 1, 1999 THROUGH MARCH 31, 2000

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

(U) **NSA's Y2K Efforts Regarding Continuity of Operations,** AU-99-0005, 30 November 1999

Summary. (U//~~FOUO~~) Contingency planning provides insurance against Year 2000 (Y2K) disruptions by instituting procedures to restore any affected systems and to continue the Agency mission in the interim. The Office of Inspector General (OIG) audit [redacted] however, at the time of the audit, the Operations Directorate (DO) was reducing the risk through efforts associated with its Y2K SIGINT Operations Plan.

Management Action. (U) The Agency Chief Information Officer (CIO) acted to ensure that contingency plans were complete and executable, and the DO validated its Y2K SIGINT Operation Plan. In the event, no significant disruptions took place.

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

(U) **Information Technology Infrastructure Division (Q57),** IN-99-0001, 1 December 1999

Summary. (U) Q57's mission is to provide tools and techniques to automate information technology infrastructure (ITI) management and monitoring at the National Security Agency/Central Security Service (NSA/CSS). The inspection found Q57 facing a dilemma between its two assigned responsibilities: readiness and modernization. Lacking the resources to perform both jobs well, the division needs clearer strategic direction in prioritizing its projects and functions. The inspectors were concerned about the large gap between what it will take to modernize the ITI and what Q57 is able to deliver with limited resources. The division also needed a process to manage requirements from diverse sources and a methodology for evaluating new tools and products.

Management Action. (U) Management directed Q57 to maintain existing systems first and use any remaining resources to modernize. Subsequently, however, on 3 January 2000, the DIRNSA set a new course, giving modernization first priority. Q57 has agreed to develop an automated requirements management process and a standard approach to product evaluation.

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

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

(U) Foreign Intelligence Liaison Relationships, AU-98-0011, 16 December 1999

Summary. (~~S~~) Conducted under the auspices of the Intelligence Community IG Forum, this joint review focused on processes established under Director of Central Intelligence Directives (DCIDs) to coordinate U.S. intelligence liaison activities with foreign governments.

Management Action. (~~C~~) The responsible parties agreed to establish a formal coordination process between the two agencies, and NSA has agreed to align Agency policy and practices

Overall Report Classification. (U) "~~TOP SECRET//COMINT//TALENT KEYHOLE//NOFORN.~~"

(U) Intelligence Oversight Inspection of the Conventional Remote Operations Facility (G62), IN-99-0003, 20 December 1999

Summary. (~~C~~) G62, the Conventional Remote Operations Facility, Its effectiveness in fostering intelligence oversight awareness and compliance is evidenced by the fact that G62 has not had a single violation in 5 years. The inspection identified some uncertainty as to the responsibility for giving intelligence oversight training to contract linguists who, for security reasons, are kept unaware of the fact that they work for NSA.

Management Action. (U//~~FOUO~~) G62 will meet with contractor representatives to devise a plan to give contract linguists the requisite intelligence oversight training. The Office of General Counsel (OGC) has offered to help develop an appropriate briefing.

Overall Report Classification. (U) "~~TOP SECRET//COMINT.~~"

(U) NSA's Implementation of the Defense Acquisition Workforce Improvement Act (DAWIA), AU-99-0001, 30 December 1999

Summary. (U//~~FOUO~~) To raise the professional knowledge, skills, and abilities of the government's acquisition workforce, the DAWIA sets mandatory education, training, and experience requirements. After benchmarking other Defense agencies, the auditors found

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

Management Action. (U) On 28 February 2000, the Director, NSA (DIRNSA) named a DAWIA-certified senior technical director in the Directorate of Technology and Systems (DT) to be NSA's senior oversight authority for ensuring compliance with DAWIA. She has already developed an action plan to accomplish the remaining corrective actions.

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

(U) **Joint Inspection of Kunia Regional Security Operations Center (KRSOC)**, JT-00-0001, 8 January 2000

Summary. (U//~~FOUO~~) The inspection, conducted jointly by the Inspectors General (IGs) of the Service Cryptologic Elements and NSA/CSS, found a critical impediment to KRSOC effectiveness and efficiency: the higher Headquarters requirement that Kunia operate as a joint site.

Management Action. (U) On 8 March 2000, the DIRNSA asked the Deputy Chief, CSS, to lead the Commanders of the Service Cryptologic Elements in a review of military-civilian structures and premises in the field and at NSA Headquarters (HQ). The Deputy Chief, CSS will report the group's recommendations to optimize the development and use of military cryptologists by June 2000.

Overall Report Classification. (U) "~~SECRET//COMINT~~."

(U) **SIGINT Processing and Dissemination** [redacted] **(M14)**, ST-99-0008, 3 January 2000

Summary. (U//~~FOUO~~) This was one in a series of OIG testable policy base reviews of high-risk Agency operations requested by the NSA Oversight Board. The study found that the policy that governs reporting [redacted] analysts to report possible [redacted]

Management Action. (U//~~FOUO~~) Management agreed to change the policy to require immediate reporting to [redacted] analysts understand what to do when they encounter an [redacted]

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

(U) **Signals Processing and Cryptologic Telecommunications Division**, IN-99-0002, 2 February 2000

Summary. (U//~~FOUO~~) J64 runs two critical round-the-clock operations: the Cryptologic Telecommunications Operations Center (CTOC) and the National Signals Processing Center. The inspection found that J64 was suffering from reductions in experienced technical support staff; expected manpower savings from new software tools had not materialized. Nevertheless, J64 had not gathered the data needed to make a business case that maps resource deficiencies against

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

requirements and assesses the resultant risk to the Agency mission. In addition, the Agencywide [redacted] installation was not being corporately managed.

Management Action. (U) J64 is developing a business case, including a risk assessment. The Agency's CIO has accepted corporate responsibility for resolving the [redacted] issue Agencywide. It is being addressed as part of the Agency's response to the January 2000 [redacted]

Overall Report Classification. (U) ~~"SECRET//COMINT."~~

(U) **Followup on Emergency Action Planning, AU-99-0010, 14 February 2000**

Summary. (U) In a 1997 audit report on Emergency Action Plans (EAPs), the OIG found that field sites had not submitted EAPs and annual recertifications to HQ. Our followup review found that the NSA EAP regulation was appropriately revised, but it took field elements over a year to comply.

Management Action. (U) As a result of this followup work, management has taken aggressive action to ensure completion of EAPs by the delinquent sites. As of January, 2000, all field elements had either submitted their EAPs or otherwise complied with the NSA regulation. To ensure future compliance, it is critical that delinquent sites be reported to the DIRNSA for corrective action.

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

(U) **Defense Special Missile and Astronautic Center (DEFSMAC), IN-00-0009, 18 February 2000**

Summary. ~~(S)~~ Located at NSA Headquarters, DEFSMAC is a joint NSA and Defense Intelligence Agency (DIA) activity. The inspection identified major issues [redacted] In addition, senior DIA managers viewed the partnership as strained; the leadership style of the [redacted] was demoralizing DEFSMAC managers; and the Director, DEFSMAC position had been vacant for 6 months.

Management Action. ~~(S)~~ Agency management is working with the National SIGINT Committee to clarify [redacted] collection priorities. A new [redacted] has been appointed and will be dual-hatted as Chief, DEFSMAC.

Overall Report Classification. (U) ~~"SECRET."~~

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

(U) **NSA's Support Services Budget,** AU-00-0001, 1 March 2000

Summary. (U) In response to concerns of the Senate Select Committee on Intelligence, the OIG conducted an audit of Directorate of Support Services (DS) budgets for FY 1997-99. Our review found that NSA has traditionally underfunded the DS budget and relied on fallout funds to cover expenditure shortfalls. Although some mission funds were shifted to pay for support-type expenses, the auditors were not able to determine the true amount of mission funds used for support purposes for two reasons: deficiencies in the guidance (and implementation thereof) on paying for support costs and inadequacies in the Agency's finance and budget systems.

Recommendations. (U) The Agency has undertaken initiatives to improve its business and program build processes along with its financial management systems. In addition, the DIRNSA endorsed recommendations to address all the issues identified in the audit and to ensure that managers have the information needed to make sound business decisions.

Overall Report Classification. (U) ~~"SECRET//COMINT."~~

(U) **Oversight Review of the Restaurant Fund,** AU-00-0011, 7 March 2000

Summary. (U) The OIG Office of Audits reviewed the contract audit of the Restaurant Fund performed by the Certified Public Accounting firm, Rager, Lehman, and Houck. The contract audit was found to be in accordance with Government Auditing Standards.

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

(U) **Certification and Accreditation (C&A) of Agency Systems and Networks,** AU-99-0006, 8 March 2000

Summary. (U//~~FOUO~~) Accreditation is the official decision to permit an information system to operate in a specified environment. The decision must be based on a certification that the system's security features and other safeguards meet security requirements. Our audit

[redacted]

with DoD Instruction 5010.40, Management Control (MC) Program Procedures, Enclosure 3 - Guidance in Applying the Definition of Material Weakness. [redacted]

[redacted]

Management Action. (U//~~FOUO~~) Management agreed to reengineer the C&A process; develop a formal risk management program; and assess and evaluate the material weakness created by the C&A deficiencies identified in the audit.

Overall Report Classification. (U) "~~SECRET//COMINT~~."

[redacted]

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

(U) Intelligence Oversight Inspection [redacted] 23 March 2000

Summary. (U~~//FOUO~~) Z03 managers and employees demonstrated keen awareness of their responsibilities with respect to Executive Order 12333 and United States Signals Intelligence Directive 18. However, the division lacks a formal intelligence oversight training program for new employees.

Management Action. (U) Management is developing an intelligence oversight training module and, beginning this year, will conduct annual refresher training for all division employees.

Overall Report Classification. (U) "~~SECRET//COMINT~~."

(U) Unified Cryptologic Architecture (UCA) Implementation, AU-00-0004, 31 March 2000

Summary. (U~~//FOUO~~) This audit focused on the UCA, a fundamental redesign of the cryptologic system. The key ingredient of the redesign was a common information infrastructure that will give Intelligence Community partners and customers [redacted] The audit identified major issues that could adversely affect the successful transition to and implementation of the UCA. Management action is pending.

Overall Report Classification. (U) "~~SECRET//COMINT//NOFORN~~."

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

~~SECRET//X1~~

#75761

UNITED STATES GOVERNMENT

memorandum

IG-9511-00

DATE: 10 October 2000

REPLY TO ATTN OF: Inspector General

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

TO: DIR thru D/DIR, E/DIR (Eyes Only)

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 2000 - 30 September 2000. For your information, I am providing you with a copy of this report.

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

[redacted] (b)(6)

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

ETHAN L. BAUMAN
Inspector General

Encl:
a/s

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

~~SECRET//X1~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD
1 APRIL 2000 - 30 SEPTEMBER 2000

~~SECRET//X1~~

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

(U) SEMIANNUAL REPORT TO THE CONGRESS

FOR THE PERIOD APRIL 1, 2000 THROUGH SEPTEMBER 30, 2000

~~(S)~~ [redacted] ST-00-0005, 3 May 2000

Summary. ~~(S)~~ [redacted] the NSA/CSS Office of the Inspector General advised the NSA/CSS Oversight Board that [redacted] field sites had collected—without Attorney General authorization—communications of a U.S. person [redacted] overseas [redacted] This special study found that support requirements were not directed by local customers but were entered manually on site. Three factors may have contributed to the unauthorized collection: lack of resolution between the Target Office of Primary Interest and another organization as to where the Collection Management Authority (CMA) resided and how it should be carried out; lack of oversight to ensure that sites follow [redacted] and lack of intelligence oversight training.

Management Action. ~~(S)~~ Management has now assumed CMA responsibility and, in accordance with its [redacted] is ensuring that USSID 18 compliance checks are performed and [redacted] Management also agreed to establish controls to oversee procedures at field sites and to ensure that all personnel are trained in and aware of—prior to their tours—the procedures they must follow when they encounter information about U.S. persons. Finally, management initiated intelligence oversight training and USSID 18 awareness sessions for its managers and analysts.

Overall Report Classification. (U) "~~TOP SECRET COMINT EXCEPTIONALLY CONTROLLED INFORMATION~~."

(U) **Joint Inspection of RAINFALL**, JT-00-0002, 9 June 2000

Summary. ~~(U//FOUO)~~ The inspection, conducted jointly by the Inspectors General (IGs) of the Service Cryptologic Elements (SCEs) and NSA/CSS, found shortcomings in documentation in Operations training and position certification procedures, Operations Security, and Emergency Preparedness. Additionally, [redacted] for military members was found to be non-existent and poor communications between the site and the [redacted]

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

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

On the other hand, the site has done an excellent job of handling the plus-up in military assignees and in building a sound Operations-Engineering relationship, both significant issues in the previous inspection in 1997.

Management Action. (U//~~FOUO~~) Site management has begun a formal program to rectify shortcomings in the area of positional documentation, operations security, [redacted] Site is working with higher headquarters to identify resources required to prepare and implement a consolidated Emergency Action Plan. Additionally, this inspection, coupled with a follow-on inspection (in progress) of the [redacted] should result in improved communications and effectiveness in the [redacted]

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

(U) **Intelligence Oversight Inspection of** [redacted] IN-00-0006, 12 June 2000

Summary. (~~S~~) This intelligence oversight inspection of the [redacted] found that the organization was in basic compliance with the requirements of E.O. 12333 and its derivative documents. It has placed some of the basic intelligence oversight documentation on its web-based training page for all to use and review; however, some basic documents need to be added. The Division has excellent risk management practices, including wide pre-publication review of all reports and on-line reference files that list problematic names. The Office of General Counsel (OGC) has not vetted the hundreds of intelligence oversight working aids and sites on WebWorld; this could result in inaccurate or misleading guidance.

Management Action. (U) Management agreed to add documents to the WebWorld training page to make a complete package. Operations Directorate organizations have begun a cooperative effort with OGC to standardize and ensure the accuracy of all intelligence oversight information posted on WebWorld.

Overall Report Classification. (U) "~~SECRET//COMINT~~."

(U) **FIREBIRD Contract Oversight,** ST-00-0006, 14 June 2000

Summary. (U) This special study focused on allegations brought to the attention of the OIG which questioned procurement practices used to buy personal computers (PCs) that were temporarily stored at the Agency's [redacted] warehouse. The audit found that NSA purchased the PCs from [redacted] which had bought them under a subcontract with [redacted] rather than purchasing them directly. There was a lack of detail on the [redacted] invoices as well as a lack of documentary evidence regarding Contracting Officer Representative (COR) review and approval of contractor invoices for payment.

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

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

Management Action. (U) Regarding the lack of details on the [redacted] invoices, management provided a memorandum detailing corrective actions taken, including the requirement that [redacted] include a material invoice detail sheet with each invoice. To address the lack of documentary evidence regarding COR review and approval of contractor invoices for payment, management developed a COR checklist for each invoice; it lists the documents reviewed and includes COR comments.

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

(U) **Oversight Review of the Non-appropriated Fund Instrumentality Audit of the Civilian Welfare Fund,** AU-00-0016, 29 August 2000

Summary. (U) The OIG Office of Audits reviewed the contract audit of the Civilian Welfare Fund performed by the Certified Public Accounting firm, [redacted] The contract audit was found to be in accordance with Government Auditing Standards.

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

(U) **Joint Inspection of** [redacted] JT-00-0003, 6 September 2000

Summary. (U//~~FOUO~~) The inspection, conducted jointly by the IGs of the SCE and NSA/CSS, found a command climate where a certain amount of discord exists between senior leadership at the site resulting in poor definition of the roles and responsibilities of the Vice Director and the Chief of Staff. Additionally, little progress has been made on several findings from the last (1997) inspection in the area of electronics maintenance and safety, particularly the fire alarm and fire suppression systems. There has been tremendous improvement, however, in the conduct of mission. The Joint IG team found Operations Directorate personnel to be fully engaged and dedicated to the mission.

Management Action. (U//~~FOUO~~) Senior SCE management has directly engaged the [redacted] Commander and Vice Commander regarding the command climate. Site management is working to rectify issues in the electronics maintenance area and is dealing with host base and higher headquarters management and technical personnel to address fire alarm and fire suppression system shortcomings.

Overall Report Classification. (U) "~~SECRET//COMINT~~."

(U) **Followup Audit on Certification and Accreditation of Information Systems,** AU-00-0015, 7 September 2000

Summary. (U//~~FOUO~~) This followup audit assessed progress to date in imple-

menting the six recommendations in our March 2000 (AU-99-0006) audit, which [redacted] While progress has been made on some of the recommendations, the audit followup found that the Agency's Chief Information Officer (CIO) and the Deputy Director for Information Systems Security (DDI) are at an impasse as to who should assume responsibility as NSA's Certifying Authority (CA).

Management Action. (U) The OIG elevated the followup findings to the DIRNSA to: 1) designate an Agency CA and; 2) determine whether to report, [redacted] to the OSD, [redacted]

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

(U) **Special Study of COMSEC Monitoring,** ST-99-0002, 29 September 2000

Summary. (U//~~FOUO~~) This special study of the Joint COMSEC Monitoring Activity (JCMA) found Agency directives and regulations regarding COMSEC monitoring are outdated; the Memorandum of Agreement (MOA) establishing the JCMA is also outdated; the JCMA lacks detailed written procedures for obtaining approval to conduct COMSEC monitoring; and the JCMA has not standardized procedures for conducting and documenting periodic Intelligence Oversight training at Headquarters and its Regional COMSEC Monitoring Centers.

Management Action. (U) The Defensive Information Operations Organization and JCMA, in consultation with the Associate General Counsel for Information Systems Security, agreed to update Agency directives and regulations in regard to COMSEC monitoring, along with the JCMA. JCMA further agreed to institute procedures to ensure monitoring personnel are aware of the legal protocols related to COMSEC monitoring .

Overall Report Classification. (U) "~~SECRET.~~"

(U) **Followup on Official Representation and Confidential Military Funds,** AU-00-0009, 29 September 2000

Summary. (U) This followup review of the 1998 audit report (AU-97-0016) found that in 1998 the Comptroller issued a policy change to the Resources Management Manual which states that cash accounts are subject to independent review every two years (biennially) or when the position of Chief, Special Operations changes hands. An independent review team performed a review in the January/February 2000 timeframe but did not issue its final report until September 2000.

Management Action. (U) Action taken by management fulfilled the requirement for a change in policy regarding the independent review; however, implementation was not timely based on the date of the independent review team's final report.

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

(U) **Favoritism and Preferential Treatment,** IV-99-0040, 4 February 2000

Summary. (U) An OIG investigation found that an Agency senior official engaged in a personal intimate relationship with a direct subordinate and that he showed favoritism and preferential treatment toward her. Additionally, the investigation found that the senior official and the subordinate misused government resources, including computer systems, cell phones, and credit cards, in furtherance of the relationship. They made false statements under oath to OIG investigators and failed to cooperate with an official investigation by their repeated obfuscation, denials, false statements and refusal to answer questions. The senior official also used threatening conduct and statements towards OIG investigators, and the subordinate destroyed and/or withheld records requested by the OIG. Both employees retired while Agency administrative actions were pending.

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

(U) **Inappropriate Conduct in the Work Place,** IV-00-0007/15, 5 July 2000

Summary. (U) An OIG investigation found that an Agency senior official yelled at a subordinate while administering a verbal reprimand in a manner which was personally degrading and belittling. The investigation also found that, on a separate occasion, the senior official grabbed another junior employee's arm, pulled a folder from the employee's hand, and admonished the individual with a raised voice in front of co-workers. During the course of the investigation, the OIG was informed of other alleged incidents involving the senior official's uncontrolled outbursts with subordinates over a period of approximately ten years. The report has been provided to management for appropriate action.

Overall Report Classification. (U) ~~"SECRET//COMINT"~~

(U) **Misappropriation of Funds,** IV-00-0030, 24 July 2000

Summary. (U) This investigation was conducted based on a complaint to the OIG Hotline that an Agency senior official had misappropriated Congressional plus-up funds intended for training and had used the funds to finance an unrelated project of low priority. An OIG investigation found that the Agency Senior Official

did not misappropriate Congressional plus-up funds and that the funds were used for their intended purpose, not to finance an unrelated project, as alleged.

Overall Report Classification. (U) **~~"TOP SECRET."~~**

UNITED STATES GOVERNMENT

memorandum

IG-9707-01

April 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 October 2000 - 31 March 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] on 963-3544s.

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

[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."

~~SECRET//NOFORN//X1~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD
1 OCTOBER 2000 - 31 MARCH 2001

~~SECRET//NOFORN//X1~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

FOR THE PERIOD October 1, 2000 THROUGH March 31, 2001

(U) **Freedom of Information Act (FOIA) Related Activities;** NSA/CSS IG, IN-00-0010, 27 October 2000

Summary. (U) At the request of Senior Leadership, the NSA/CSS Office of the Inspector General (OIG) conducted a functional inspection of agency activities related to FOIA requests. This inspection evaluated the effectiveness of the existing processes; the experience and training of those involved in the processes; workload and resource factors; and the impact on NSA's public image. The following improvements to FOIA processes are needed to make NSA function more effectively in this area: FOIA and Privacy Act Services needs to take a more proactive, strategic approach to developing and implementing FOIA-related policy; NSA is not fully compliant with the Electronic FOIA (E-FOIA) amendments of 1996 that require posting frequently requested material on the internet; and more training for FOIA case officers and Key Component personnel with FOIA responsibilities.

Management Action. (U//~~FOUO~~) Management concurred with all recommendations and actions have either been completed or are ongoing. We noted, however, that the FOIA release process is inextricably connected to the classification process. Improvements in the process will require leadership from the policy organization - to whom many of our recommendations are directed - but also full compliance by the Key Components to the policy organization's-generated policies.

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

(U) **Overhead Collection Management Center (OCMC);** NSA/CSS IG, IN-00-0011, 21 November 2000

Summary. (U//~~FOUO~~) This inspection of the OCMC found that, despite dramatic changes in the target set and overhead missions, the Memorandum of Agreement establishing the OCMC has not been updated since 1984. Failure to define new authorities, responsibilities, and roles has produced an extremely complicated and expensive system that operates without the formal direction needed to optimize its activities and to ensure that it will perform well in a crisis.

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

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

The position of Chief, OCMC, is now used as a developmental assignment, diminishing its effectiveness in dealing with high-ranking OCMC partners. Although most tasks, once executed, are successful, inefficient practices characterize the complex tasking process. Finally, OCMC work spaces are extremely dilapidated.

Management Action. ~~(C)~~ The new Chief, OCMC, will review the charter and begin drafting a document that codifies the complex overhead tasking process. The Collection Management Office will start documenting the extent to which resource constraints degrade the OCMC mission.

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

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

~~(S)~~ [redacted] **Supplemental Fund;** NSA/CSS IG, [redacted]

Summary. ~~(S)~~ At the request of the Office of Global Response, the OIG performed this audit of [redacted] supplemental funds shortly after the Office of Global Response assumed management of these funds. There were two concerns regarding the Crisis Management Office (CMO), from where the transfer occurred: 1) possible inadequate documentation and controls over the use of travel funds; and 2) possible diversion to [redacted] We found no evidence that anyone misused travel funds or diverted SIGINT equipment. However, we found that the CMO had not instituted robust controls in two major areas.

Management Action. (U) Management agreed to improve the internal controls over the use of supplemental funds during contingency operations. Additionally, management will also supplement the Crisis Action Management System Concept of Operations to document the requirements and budget processes and will include a standard checklist of expenses common to contingency operations.

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

(U) **NSA's Implementation of DoD 5000 Series;** NSA/CSS IG, AU-00-0002, 5 January 2001

Summary. (U) This audit focused on NSA/CSS Circular 5000, *Acquisition Management*, which implements DoD Directive (DoDD) 5000.1 and its accompanying regulation. It establishes a structured process for reviewing major acquisitions at specific milestones and making an informed decision on whether to proceed. The audit found problems in Agency implementation of DoDD 5000.1, including: 1) NSA had not finalized and implemented a formal plan to implement NSA 5000, due to the

Cryptologic Acquisition Program Board's failure to perform its assigned role; and 2) the process prescribed by NSA 5000 was not rigorously followed, as funding for [redacted] programs we reviewed was released before a Mission Needs Statement was developed.

Management Action. (U) Management agreed with our recommendations to designate, by charter, the Senior Acquisition Executive (SAE) as the responsible authority for oversight of NSA's acquisition management system and to develop a policy and a formal process that require SAE approval of acquisition documentation before program funding is released

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

(U) **Intelligence Community Coordination of Foreign Liaison Intelligence Relationships and Intelligence Disclosures to Other Countries;** NSA/CSS IG, AU-00-0013, 22 January 2001

Summary. (U) This interagency review, conducted with representatives who comprise the Intelligence Community Inspectors General Forum, determined the effectiveness of the mechanisms and administrative processes established under the Director of Central Intelligence Directives (DCIDs) for coordination of US espionage, counterintelligence, and related intelligence liaison activities with foreign governments and international organizations. [redacted]

Another finding pertained to the Special Assistant to the DCI for Foreign Intelligence Relationships (SA/DCI/FIR). Since 1991, the SA/DCI/FIR has advised and assisted the DCI in the discharge of his duties and responsibilities with respect to foreign intelligence relationships [redacted]

Management Action. ~~(S//NF)~~ Management officials from the participating [redacted]

(b)(3) - 50 USC 403g Section 6 of the CIA Act of 1949
(b)(3)-50 USC 3024 National Security Act of 1947 Section 102A(i)(1)
OGA

(b)(1)
(b)(3) - 10 USC 424
(b)(3) - 50 USC 403g Section 6 of the CIA Act of 1949
(b)(3)-50 USC 3024 National Security Act of 1947 Section 102A(i)(1)
OGA

[redacted]

Overall Report Classification: (U) SECRET//NOFORN

(U) **Intelligence Oversight Inspection of the Global Network Management Division;** NSA/CSS IG, IN-01-0004, 24 January 2001

Summary. (U~~//FOUO~~) This Intelligence Oversight (IO) inspection of the Global Network Management Division evaluated the office's program to comply with Executive Order (E.O.) 12333 and its implementing directives and regulations. The inspection found the Global Network Management Division was in basic compliance with E.O. 12333 and derivative documents, managers and employees demonstrated a keenawareness of their individual IO responsibilities, and several office elements had best practices, including online IO working aids and training verification. However, the office needs to formalize IO training for new employees and refresher training for its entire work force, and there is no formal procedure for reporting or logging potential violations.

Management Action. (U) During an interim status briefing, management immediately instituted process and program improvements to address the office's IO shortcomings. As a result, the Global Network Management Division now has an excellent IO web site, an official has been named to standardize training for new employees and annual refresher training, and a procedure to report and log incidents is in development.

Overall Report Classification: (U) SECRET//COMINT

(U) **Office of Facilities Engineering**; NSA/CSS IG, IN-00-0012, 25 January 2001

Summary. ~~(C)~~ This organizational inspection of the Office of Facilities Engineering evaluated their ability to perform their mission and identify any impediments to success. The inspection found the office's employees to be customer-focused, dedicated, and have introduced several innovative "best practices" into their daily routines. Nevertheless, we identified two concerns that could jeopardize the office's ability to perform its mission in the near future: substantial cuts in funding and an eroding skills base. [redacted]

[redacted]

estimate of the impact of the upgrade; NSA and the Service Cryptologic Elements

(SCEs) do not have Memorandums of Agreement (MOAs) on the responsibility for field support; and Technical Security Countermeasure (TSCM) inspections are not routinely performed on newly renovated OPS 1 cores.

Management Action. ~~(C)~~ Management concurred with most of the recommendations. The office of physical security routinely completes informal assessments of the technical security risk to mission after renovations [redacted] plan and will establish MOAs that assign funding responsibilities for facilities support at field sites.

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

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

(U) **Time Sensitive and Field Support Division**; NSA/CSS IG, IN-00-0013, 13 February 2001

Summary. ~~(C)~~ The Time Sensitive and Field Support Division has two missions: providing end-to-end support to the National Time Sensitive System (NTSS) and serving as the Program Manager for Information Technology Infrastructure (ITI) modernization for the extended Enterprise. This organizational inspection found a major impediment to a critical mission: lack of an Agency program to implement the Chief Information Officer's policy of [redacted] Other findings include key Division processes have not been documented, which impede NSA's effort to privatize delivery of ITI support services; the Division has an enviable record of maintaining NTSS availability but needs to gather performance data in order to identify improvements; and employees are anxious to find out how GROUNDBREAKER will affect them.

Management Action. (U) The OIG recommended that the Director of Information Technology Infrastructure Services (ITIS) implement a program to transition automated analysis and reporting tools and applications so that [redacted] etc., can run on [redacted] operating systems. Other recommendations include the Division documenting their processes; develop standard operating procedures; and utilize performance data to foster a continuous improvement mentality. Finally, the Director, ITIS, needs to give the work force concrete answers about how GROUNDBREAKER will affect their jobs.

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

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

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

~~SECRET//NOFORN//X1~~

(U//~~FOUO~~) Followup on the Joint Inspection of [redacted] NSA/CSS IG, [redacted]

Summary. (U//~~FOUO~~) This joint followup inspection, conducted jointly by the Inspectors General (IGs) of the Service Cryptologic Elements (SCEs) and NSA/CSS, focused on the serious electronic maintenance and life safety deficiencies observed during the original joint inspection in June 2000. Regarding electronic maintenance, the inspection found that [redacted] has taken all of the right steps to solve immediate deficiencies and to establish credible processes that ensure the sustainability of all maintenance programs. Accordingly, all of the findings have been closed. Regarding safety and fire protection, the inspection found that, where possible, interim controls and work-arounds have been instituted. [redacted] These existing deficiencies do not pose a serious threat to personnel, but continue to place mission equipment at [redacted] risk. Site management will continue long-term monitoring of the [redacted] project status to ensure continued action on the fire protection deficiencies.

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

(U) **Joint Inspection of Medina Regional Security Operations Center (MRSOC);** NSA/CSS IG, JT-01-0001, 20 February 2001

Summary. (U//~~FOUO~~) The inspection, conducted jointly by the IGs of the SCEs and NSA/CSS, found the site's responsibility for [redacted] has increased; [redacted] as well as space, parking, and facility issues; and a centralized focal point at NSA to serve as a one-stop-shop for MRSQC concerns and questions, has not been successfully addressed since the last inspection about two years ago. Despite the positive command climate, several issues demand immediate attention [redacted]

Management Action. (~~S~~) Management stated that the report validates the best practices of the MRSOC, provides a road map for management to improve the site, and recommendations are already being implemented. Management continues to provide periodic status updates on actions taken to correct the deficiencies noted in the report. The inspection produced several recommendations directed to higher headquarters and the site [redacted]

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

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

~~SECRET//NOFORN//X1~~

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

[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~~

~~CONFIDENTIAL//X1~~

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~~

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

~~CONFIDENTIAL//X1~~

~~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~~

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

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

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] 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~~

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

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,

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.

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

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~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE

SEMIANNUAL REPORT FOR THE PERIOD 1 OCTOBER 2001 - 31 MARCH 2002

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

~~SECRET//X1~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

FOR THE PERIOD October 1, 2001 THROUGH March 31, 2002

(U) **Integrated Financial Management System**; NSA/CSS IG, AU-01-0003, 4 October 2001

Summary. (U) One of the Director's initiatives under the 100 Days of Change was to transform the Agency's financial management processes and systems. In 1999, the Director hired a Chief Financial Manager (CFM) from private industry to lead the Agency's financial management transformation. An NSA/CSS Office of the Inspector General (OIG) audit found problems in two areas: (1) NSA does not have a documented plan, as required by DoD and Office of Management and Budget guidance, for its financial management transformation and (2) NSA has not established an organizational structure to oversee and manage its business systems, e.g., budget and finance, supply chain management, human resources, acquisition, and property systems.

Management Action. (U) The CFM agreed with the audit recommendations to: (1) develop a corporate strategy and plan for transforming its financial management systems and (2) establish a central organization to oversee the integration and configuration management for a single, integrated financial management system (including all business systems). These actions were progressing until the DoD decided to implement its Enterprise-wide effort to standardize and improve their many financial management systems. Current DoD timelines call for architecture development by second quarter FY03 followed by solution deployment in the third quarter of FY05.

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

(U~~//FOUO~~) **Bad Aibling Station Mission Transfer;** NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-01-0005, 30 October 2001

Summary. ~~(S)~~ The purpose of this joint inspection was twofold - to verify that procedures were in place to ensure a seamless transfer of the [redacted] mission from Bad Aibling Station (BAS) to the Medina Regional Security Operations Center (MRSOC), and to account for the cessation and mitigation processes

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

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

associated with the closure of BAS. The [redacted] transfer is on track, but some serious problems need resolution. These include: shortfalls in the training of linguists for MRSOC positions; systems administration and technical support manning shortfalls; and unclear lines of responsibility for [redacted] collection equipment. Shortly after this inspection concluded, the closure of BAS was postponed to September 2004. Thus, some of the findings of this report must be viewed in a different light.

Management Action. ~~(S)~~ Management should develop their strategy for Signals Intelligence development in the post-BAS period. Army's Intelligence and Security Command needs to develop its [redacted] training pipeline, and additional IT/system administration resources must be provided to the MRSOC.

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

(U) **Integrated Logistics Management System**; NSA/CSS IG, AU-01-0002, 11 December 2001

Summary. (U) The Agency's Supply Chain Management (SCM) process manages the flow of materiel and related information between customer and supplier. The audit objectives were to determine whether the Agency is moving toward a centralized logistics process and if plans for the Agency's financial management system (FMS) take into account the need to integrate and have interoperability with the automated SCM system that must feed into it. An OIG audit found that NSA does not have a written plan to ensure that the SCM System is integrated and interoperable with the Agency FMS currently in development. The audit was unable to determine the accuracy of actual cost reductions and avoidances attributed to the new SCM process. However, the auditors found the methodology employed to establish cost baselines to be acceptable and consistent.

Management Action. (U) The Chief Financial Manager (CFM) agreed with the audit recommendation that the FMS integrator should evaluate the SCM system to ascertain whether it can be integrated into the new FMS or whether it should be replaced.

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

(U) **Office of Russia**; NSA/CSS IG, IN-01-0010, 13 December 2001

Summary. (U) The Office of Russia provides intelligence gained from Russian communications. An inspection found that missions, roles, and authorities of the [redacted] divisions are not clearly delineated, and office level management has not resolved a serious conflict between the two that interferes with mission accomplishment. The organization's work force does not feel well informed about the

Agency, the Signals Intelligence Directorate, or the organization's Transformation efforts.

Management Action. (U) Management concurred with all recommendations and will act to clearly delineate roles, responsibilities, expectations, and authorities; resolve the internal conflict between the [redacted] divisions; and develop and implement a strategy to make Transformation relevant to all levels of the organization's work force.

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

(U) **Strategic Assessment of Intelligence Oversight**; NSA/CSS IG, ST-00-0001, 14 December 2001

Summary. (U) In order to protect the rights of U.S. persons during the conduct of NSA's missions, DoD Regulation 5240.1-R, and NSA/CSS Directive 10-30 require NSA , through intelligence oversight awareness training, to familiarize its personnel with Executive Order 12333 - the Intelligence Community's charter - and the laws, directives, and regulations that implement it. In response to ongoing concerns about the consistency and adequacy of intelligence oversight (I/O) awareness at the Agency, the OIG conducted a comprehensive study of this issue. The results indicated broad non-compliance with DoD and Agency requirements for providing I/O awareness training, which was nonexistent or inadequate in [redacted] of the organizations we reviewed. Fortunately, although training has not been up to par, the Agency has many other controls and procedures in place to ensure that the rights of U.S. persons are protected.

Management Action. (U) Management agreed to implement our recommendations, including production of a videotaped version of basic I/O awareness training, development of tailored I/O training for high-risk organizations, and revision of NSA/CSS Directive 10-30 with more detailed guidance about I/O training and quarterly reporting requirements. Additionally, management is providing interim I/O awareness training programs that meet minimum DoD requirements.

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

(U) **Advisory of Information Technology Outsourcing**; NSA/CSS IG, ST-01-0004, 16 January 2002

Summary. (U) Based on lessons learned by other public and private sector organizations that outsourced Information Technology (IT) services, the OIG concluded that success is closely tied to: strong management commitment; well-

documented planning; experience with performance based contracting (PBC); effective service level agreements (SLAs); and contract monitoring aimed at continuous improvement rather than compliance. An OIG study indicated that GROUNDBREAKER (GB) is likely to experience many of the aforementioned obstacles. Applying the lessons learned in the study to the GB transition environment, the OIG concluded that success probably hinges on: demonstrable commitment to GB success by top-level management; documented transition and implementation plans; SLAs that accurately reflect customer expectations; appropriate metrics; and performance standards. For the long term, the Agency needs to develop training in all aspects of PBC: writing performance objectives and measures; learning new contract monitoring techniques; and using incentives to optimize performance.

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

(U) **Fort Gordon Regional Security Operations Center (GRSOC)**; NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-01-0003, 24 January 2002

Summary. (U) A joint inspection found the command climate to be excellent, and the work force is dedicated and professional. However, the GRSOC is stretched thin, almost to the breaking point, by a growing mission and continual shortages of experienced personnel. The inspection also included the effectiveness of the Joint-like Testbed initiatives: the Common Workforce Training and Executive Training Council have had a positive impact and are highly effective; the Combatant Cryptologic Support Center has improved national-tactical partnering, but needs increased resources to reach full effectiveness. The Joint Rating Scheme was assessed to be effective with the Regional Security Operations Center Commander rating the local Service Cryptologic Element unit commanders but having minimal positive impact when extended throughout the junior ranks. The Joint J1 Organization Testbed was effective but requires further evaluation following planned changes in functions.

Management Action. (U) Headquarters management should give immediate attention to three areas affecting the GRSOC: mission overload, manpower, and the requirements process. DIRgram-212 of 7 December 2001 implemented the Joint IG recommendations on the Joint-like Testbed initiatives.

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

(U) **Special Study on NSA Support to Law Enforcement;** NSA/CSS IG, ST-02-0001, 7 March 2002

Summary. (U) In January 2002, the Intelligence Community Inspector General (IG) Forum undertook a project to identify the support to law enforcement provided by each member's agency. The impetus for the project was twofold: (1) in response to a desire, expressed by the Congress and others, to increase information sharing between the intelligence and law enforcement communities and (2) in anticipation of possible future taskings related to events from 11 September 2001 from the Congress regarding this issue. As NSA's contribution to this project, the NSA OIG solicited input from its Directorates and Associate Directorates based on their interaction with the law enforcement community. This and other information was used in the compilation of a special study regarding NSA's support to law enforcement. This study found that NSA interacts with a broad spectrum of law enforcement entities, including organizations within the Departments of Justice, Treasury, and Transportation; the military law enforcement community; and local and state police departments. Under Executive Order 12333 and National Security Directive 42, NSA interacts with law enforcement in the course of conducting Signals Intelligence, Information Assurance, Security, and Education and Training missions, and by providing assistance in the form of knowledge, equipment, and personnel.

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

(U) **Office of Foreign Relations**; NSA/CSS IG, IN-01-0005, 15 March 2002

Summary. ~~(S)~~ As part of the Agency's transformation, the Director charged NSA's Director of Foreign Relations with "orchestrating and improving all of our foreign relationship activities, processes, and decisions." The OIG evaluated the Office of Foreign Relations (OFR) for effectiveness and efficiency, as well as the degree to which transformation is taking hold within the organization and associated foreign relations activities. Findings of the inspection include the following: there is a need for an up-to-date charter that defines the current roles and responsibilities of all Agency organizations involved in foreign relations; the [redacted] program budget execution and accommodation purchase function, inadequately retained in the Agency reorganization, needs to be reconstituted and; a decision-making process for SIGINT foreign relations initiatives—including an expeditious approval process and a formal risk management component—is needed.

Management Action. ~~(S)~~ Management has already completed several actions; however, some recommendations require "cooperative actions." For these, the OFR was designated as the lead, responsible for a consolidated OFR/SIGINT Directorate (SID)/Information Assurance Directorate (IAD) response. OFR and IAD

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

concurred in all actions. The SID Director non-concurred in the recommendation related to the [redacted] Program budget execution and accommodation purchase function. We have requested that the Director, NSA clarify to the Director of Foreign Relations and the SID Director the "model" for the corporate Foreign Relations Program, and direct them to address the issues raised.

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

(U) **Continuity of Operations and Contingency Planning for** [redacted] NSA/CSS IG, AU-02-0002, 27 March 2002

Summary. ~~(S)~~ In response to the terrorist attacks of 11 September 2001, the Deputy Director, NSA established a Mission Assurance Task Force (MATF). The audit found that the MATF had developed a three-phase strategy [redacted]

Management Action. (U) The CIO agreed with our recommendation to revise NSA Regulation 25-1 and to develop a Mission Assurance Policy by mid-summer.

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

(U) **Continuity of Operations -** [redacted] NSA/CSS IG, AU-02-0004, 27 March 2002

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

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

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

[redacted]

Management Action. (U) Management concurred with all recommendations to revise and test the EAP; establish emergency destruction procedures and capability; and establish accountability for mitigating any risks and vulnerabilities identified in ARM recommendations.

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

(U) **Review of Transformation Progress in the Signals Intelligence Directorate**; NSA/CSS IG, IN-01-0011, 29 March 2002

Summary. (U) An OIG review of the progress in transforming the Signals Intelligence Directorate (SID) found SID to be about at the 1-year mark of a 5-year transition, despite the exigencies of responding to 11 September. Strategic direction for key business lines is set, with customer-focused initiatives underway and technological innovations for reporters and analysts under development or coming on line. Nevertheless, we noted the following concerns: SID leadership focus was more tactical than strategic at the time of the review, and the control environment in place to guide transformation was inadequate – there are few schedules that articulate next steps, milestones are non-existent; and senior managers were not sure of their next deliverables in support of transformation. The report recommends a planning process that sets strategic direction for the SID and establishes action plans with milestones. SID leadership also needs to clarify roles, responsibilities, processes, and decision-making authorities for key executives with key transformation responsibilities.

Management Action. (U) SID leadership concurred with all recommendations and has reset its focus on the strategic aspects of transformation. Actions have been taken to tighten the control environment and work is underway to define further measures to gauge progress towards SID goals in this area.

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

(U) **Follow-up Inspection of the Overhead Collection Management Center (OCMC)**; NSA/CSS IG, IN-02-0003, 28 March 2002

Summary. (U)) The primary purpose of this follow-up to the FY 2000 organizational inspection of the OCMC was to identify impediments to the implementation of the prior recommendation to "validate the role of a central tasking authority for overhead collection and write a charter detailing the updated authorities and responsibilities." A secondary goal was to determine whether the overhead tasking process had benefited from the inspection's other

recommendations. The follow-up found that progress on updating the charter is being impeded by uncertainty about the future of the SIGINT Overhead Requirements Subcommittee and the role of the SIGINT Committee in managing overhead collection activities. The follow-up also found that improvements in overhead tasking have resulted from the 2000 inspection.

Management Action. (U) The follow-up found that the issues surfaced regarding the OCMC charter are well recognized and are being actively addressed by appropriate authorities.

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

(U) **Inherently Governmental Functions and Contract Administration Improprieties**; NSA/CSS IG, IV-00-0041, 11 January 2002

Summary. (U) An OIG investigation found that an Agency Program Manager and Contracting Officer's Representative (PM/COR) engaged in a series of improper practices in violation of the Federal Acquisition Regulation and Agency procurement policies, including making a series of unauthorized commitments; interfering with contractor performance; and allowing a contractor employee to engage in inherently governmental functions. In addition, the PM/COR engaged in a pattern of harassment and intimidation of those who reported the contractor employee's improprieties to management or attempted to take corrective action themselves. Management removed the individuals as the PM/COR and the Office of Employee Relations issued a written reprimand. The former PM/COR donated 24 hours of annual leave to the Leave Bank and agreed to prepare a research paper on the "Proper Management of Contracted Personnel." The Contracting Group is reviewing the current contracts used by this program and has indicated further action may be forthcoming.

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

(U) **Senior Official Investigation**; NSA/CSS IG, IV-02-0001, 24 January 2002

Summary. (U) An OIG investigation found that an Agency senior official used contractor employees as if they were personal staff and improperly administered the contract as a personal services contract. The contractor employees received routine direction and taskings from the senior official, including how the tasks were to be accomplished and the deadlines for accomplishing them, and reported directly to the senior official on the status of the tasks. The increased reliance on the contractor employees by the senior official and other groups within NSA resulted in the scope and associated costs of the contract significantly

expanding – from [redacted] in 1998 to [redacted] as of 31 October 2001. Prior to the OIG investigation, the senior official was unaware of the government rules regarding personal services contracts. We recommended that the Senior Acquisition Executive take appropriate corrective actions to ensure that the current contract is administered properly.

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

(U) **Senior Official Investigation**; NSA/CSS IG, IV-01-0047, 5 February 2002

Summary. (U) An OIG investigation found that an Agency senior official, who works part-time for an NSA contractor, represented this employer at a meeting with NSA representatives. The purpose of the meeting was to discuss matters related to a contract with the Agency. We concluded that he engaged in outside employment activity that conflicted with his official duties. This same senior official was investigated by the OIG a year earlier, and was found to have represented his contractor employer at a meeting with NSA employees. The Agency's Office of Employee Relations subsequently counseled him concerning his responsibilities. In addition, after the first investigation, the senior official's NSA management advised the OIG that he would avoid any future contact with government employees while working in his capacity as a contractor. The senior official failed to adhere to this guidance. Administrative actions are pending.

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

~~SECRET//X1~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

FOR THE PERIOD April 1, 2002 THROUGH September 30, 2002

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

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

(U) **Menwith Hill Station**; NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-02-0001, 22 May 2002

Summary. ~~(S)~~ A joint team of inspectors from the Service Cryptologic Elements (SCEs) and NSA conducted an inspection at Menwith Hill Station (MHS) from [redacted] On the positive side, MHS is doing an outstanding job of supporting [redacted] due to the collective efforts of the workforce. However, the Joint IG found that NSA's Signals Intelligence Directorate needs to provide more definitive guidance and a formal architecture for [redacted]

Management Action. (U) Since the inspection, Executive Agency responsibility has changed from Army INSCOM to Air Force AIA and the transition activities associated with this change are proceeding.

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

(U) **Methodology for Certification and Accreditation and Risk Management**; NSA/CSS IG, ST-02-0012, 31 May 2002

Summary. (U) This review describes the Certification, Accreditation, and Risk Management (CARM) methodology. It synthesizes extensive training, certification, and "hands-on" use of capability maturity models (CMMs), frameworks, and assessment methodologies dating back to 1991. The models and frameworks contain the essential elements of effective processes for numerous and varied disciplines. The CARM methodology was developed to (1) reduce the number of questions to a small set of "breakpoint" questions; (2) add structure to the team composition; and (3) facilitate

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

implementation of a quick but repeatable evaluation methodology. It is easy to learn and apply, and it produces reliable results. Extensible by design, it can be used by a wide variety of organizations for different purposes. It is currently being considered for further development into an automated version and for use throughout the Intelligence and DoD communities to provide a standard and repeatable process to support annual assessments of national security systems and collateral systems by a variety of organizations.

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

(U) **Personal Property Accountability**; NSA/CSS IG, AU-02-0012, 13 June 2002

Summary. (U//~~FOUO~~) After the annual inventory for 2000, the former Operations Directorate (now the SIGINT Directorate (SID)) had to [redacted] As a result, the Director, NSA, asked the OIG to review SID's property accountability process and procedures. The audit found that SID's control environment needed improvement, especially since SID managers are not sufficiently involved in the property accountability process, and system administrators often fail to report the movement of information technology (IT) equipment. We also found that NSA needs to address three corporate policy issues: conducting financial liability investigations, assigning accountability for laptop inventories, and including the Associate Directorate for Security in the write-off process.

Management Action. (U//~~FOUO~~) Management concurred with our recommendations to improve controls, [redacted] They also plan to institute policy to improve the Agency's control environment, such as assigning individual responsibility for tracking property, reporting losses, and acting on the results. [redacted] financial liability investigations are already underway.

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

(U) **Personnel Reliability Program**; NSA/CSS IG, AU-02-0001, 19 June 2002

Summary. (U//~~FOUO~~) The Agency is not in full compliance with the DoD Nuclear Weapons Personnel Reliability Program (NWPRP) requirements. [redacted] personnel performing NC2 duties must meet high standards of individual reliability. An audit found that the revised NSA Regulation 30-24, *Nuclear Weapon Personnel Reliability Program*, does not incorporate the most recent DoD requirements, particularly formal designation of a Competent Medical Authority (CMA). This Program lacks some of the controls needed to

ensure that NWPRP-certified personnel have met, and continue to meet, DoD reliability standards. Program officials could only document that [redacted] percent of the [redacted] employees actually met all of the requirements for entering the NWPRP.

Management Action. (U) Management concurred with our recommendations to amend NSA Regulation 30-24 to incorporate requirements for a designated CMA and training for program officials; develop standards for documenting key aspects of the NWPRP process; automate the program tracking system; and improve drug-testing procedures. Management has already implemented actions to address most of the recommendations.

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

(U) **Service Level Support Agreements**; NSA/CSS IG, IN-02-0002, 11 July 2002

Summary. (U//~~FOUO~~) Internal Service Level Agreements (SLAs) at NSA were intended to normalize the relationships between service providers and customers, especially those that were disrupted during the FY2001 Agency reorganization. At that time, many support functions were removed from the directorates and consolidated elsewhere. The "losing" mission organizations needed assurance that they would continue to receive these services. At the Director's request, the OIG reviewed the quality of finalized SLAs; determined the status of draft or unsigned SLAs; and evaluated associated processes at NSA. We found no formal (policy/directive) requirements to develop SLAs and no standards that service providers could use to write SLAs. As a result, most SLAs tracked by the Chief of Staff have not been finalized; those that were are of marginal quality and may not achieve their intended purpose. We also believe the number of SLAs to be excessive; many may be unnecessary.

Management Action. (U) The Director has decided to retain the use of SLAs. Management concurred with all aspects of our recommendation. The Chief of Staff will publish a policy and establish a program, including standards and guidelines written in layman's language, for drafting and evaluating such agreements.

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

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

(U//~~FOUO~~) **Aerospace Data Facility - Denver;** NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-02-0002, 16 July 2002

Summary. (~~S~~) A joint team of inspectors from the SCEs and NSA conducted an inspection at the Aerospace Data Facility (ADF), Denver, [redacted] The primary drivers for most of the findings during this joint inspection were the efforts to [redacted] Considerable progress towards implementation has been made in the last year. However, especially in the areas of Command Topics, Mission Operations and Mission Systems, previous Higher Headquarters principles regarding relationships, responsibilities, chain-of-command and the resulting organizational structures are no longer applicable. The Joint IGs found that a comprehensive review of those principles of governance, specifically as they are applied to leadership structures and responsibilities, is needed. [redacted] In the area of programs and resources, ADF managers are to be complimented, especially for their efforts to consolidate human resources service for military and civilian personnel.

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

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

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

(U) **Followup Inspection of Defense Special Missile and Astronautics Center;** NSA/CSS IG, IN-02-0004, 19 July 2002

Summary. (U) The OIG conducted a followup inspection of DEFSMAC and evaluated the outcome of management actions taken in response to four recommendations from our FY2000 inspection (IN-00-0009).This inspection found that major improvement has occurred in all four focus areas: updating the charter, authorities of the subcommittees, clarity of expectations, and morale of watch personnel. We also found that some military personnel in DEFSMAC believe civilian supervisors should not be part of the military performance rating process. The extent to which NSA supervisors—civilian or military—play in a member's evaluation varies from service to service. Consequently, DEFSMAC needs a policy regarding military performance evaluations that is applied uniformly throughout the Center and is consistent with local SCE policy and practice.

Management Action. (U) Management concurred with the finding and action has already been completed. In conjunction with this matter, the inspectors

reviewed NSA Personnel Management Manual (PMM) 30-2, Chapter 235, *Performance Reports and Counseling*, dated 14 June 2001. We found that the PMM contains inaccurate data regarding evaluations of Navy enlisted personnel assigned to NSA. This issue is being addressed separately with the Office of Military Personnel.

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

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

(U) **NSA Certification Process;** NSA/CSS IG, AU-02-0003, 2 August 2002

Summary. ~~(S)~~ This audit determined the degree to which [redacted] mission-critical and mission-essential Agency systems met specific DoD and DCI certification requirements. [redacted]

Management Action. (U~~//FOUO~~) Management agreed to issue a new NSA Directive to resolve conflicting DoD and DCI guidance and to seek DoD and DCI approval for it; [redacted]

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

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

(U) **Intelligence Oversight Review of the SIGINT Forensics Laboratory**; NSA/CSS IG, ST-02-0009, 26 June 2002

Summary. ~~(C)~~ At the request of the Deputy Director for Data Acquisition post 11 September 2001, the OIG reviewed this high-risk operation, [redacted] The OIG found the Lab needs formal policies for providing technical assistance to external customers, including law enforcement agencies, and for SIGINT lead purposes; documented SOPs approved by senior management; and stronger internal controls for partitioning and reporting on incoming datasets. Other findings of this special

study include the following: SID policy needs to reflect the Lab's evolving mission—conducting forensics analysis for SIGINT lead purposes—and to provide guidance on handling technical assistance to external agencies; and the [redacted] staff needs to publish written procedures and to conduct a periodic inventory of physical media provided for forensics analysis.

Management Action. (U) The Signals Intelligence Directorate agreed to all of the OIG findings and recommendations; corrective action is underway.

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

(U) **NSA's Senior Hire Program**; NSA/CSS IG, ST-02-0010, 16 August 2002

Summary. (U//~~FOUO~~) This special study examined the processes, practices and results of NSA's initiatives to hire senior executives from outside of the Agency. The study covered [redacted] senior executives who were hired during the period December 1999 to June 2002. Patriotism, a strong support for NSA's mission; and a desire to contribute to transforming the Agency were reasons most frequently cited for accepting employment offers. The allure of working for NSA outweighed federal salary limitations for many of the newly hired senior executives. The study also found that Agency personnel at the front end of the hiring process are doing an excellent job of helping new executives through recruitment and security clearance processes. For logistical and cultural reasons however, the Agency does a poor job of welcoming and absorbing newly hired executives, especially those recruited for newly created assignments in support of transforming processes having to do with the business of running the enterprise. Study results also prompt Agency management to pay more attention to diversity as it continues to hire senior executives.

Management Action. (U) Agency leadership welcomed the results of the study and commissioned a working group to address the suggested improvements included in the study.

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

(U) **Followup Inspection of the Time Sensitive and Field Support Division**; NSA/CSS IG, IN-02-0006, 12 September 2002

Summary. (U//~~FOUO~~) The primary purpose of this follow-up to the FY 2001 organizational inspection of the Time Sensitive and Field Support Division was to evaluate why two recommendations regarding transitioning [redacted] reporting and analysis tools to run on the [redacted] had not been completed. Lack

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

of progress regarding these recommendations resulted in the Chief Information Officer (CIO) granting a waiver to the Information Technology Infrastructure Services (ITIS) to permit the purchase of [redacted] to upgrade field sites that had [redacted] The [redacted] We found that little progress was made on the recommendations because it was a low priority for SID and ITIS management, there was a lack of financial resources, and key personnel who had agreed to implement the recommendations were reassigned due to reorganizations or otherwise departed. We identified promising developments that indicate that the recommendations will be completed in the coming year.

Management Action. ~~(S)~~ Funds amounting to [redacted] have been identified for the [redacted] migration effort and are in the CBJB for FY 2003. Also, in June 2002 the SID Systems Engineering Office accepted responsibility, pending sufficient funding, for managing the overall migration program. As a result, the OIG has transferred action on the recommendations in question to the Signals Intelligence Architecture Office, which has accepted responsibility for the recommendations.

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

(U) **Report on Government Information Security Reform;** NSA/CSS IG, AU-02-0009, 12 September 2002

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

Summary. ~~(S)~~ GISRA requires all government agencies to assess the information security risk associated with their operations and assets; determine the level of security needed to mitigate that risk; and periodically test and evaluate security controls and techniques. All of these actions must be part of an agency-wide security policy implemented throughout the organization and backed up by the training needed to support these activities. [redacted] The OIG has the benefit of detailed knowledge of NSA's IT security activities, and has done sufficient audit work to formulate the opinion [redacted]

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

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

(U) **Followup Inspection of Menwith Hill Station**; NSA/CSS IG, AIA IG, INSCOM IG, NSG IG, JT-02-0005, 20 September 2002

Summary. (U//~~FOUO~~) From [redacted] a joint inspection team revisited Menwith Hill Station to assess progress the Station is making in correcting problems found during the March 2002 Joint IG Inspection in the Command Topics, Mission Systems, Communications and Computers, and Base Operations areas. The Station's command climate has improved slightly since March, but continued attention is needed. Inspectors found that the 'victim mentality' prevalent during the March inspection is abating. Morale is beginning to improve despite the fact that the myriad of problems found in the quality of life area remain unaddressed except for improvements noted in medical services. In the area of Mission Systems, considerable progress was noted in responding to findings from the March inspection. Significant improvements were also found in information systems accreditation, development of local standard operating procedures, preventative maintenance programs, and within the Telecommunications Operations Center. Under Base Operations, sufficient progress was found to warrant closing [redacted] findings documented in this area during the March 2002 inspection. However, inspectors found that the Station's plans for resolving most of the remaining findings are contingent on the transfer of the base operations support mission from the Army to the Air Force and the establishment of an Air Base Squadron with commensurate levels of USAF services. Inspectors remain concerned that quality of life and morale will suffer further if Station leadership does not aggressively pursue interim fixes to the findings that remain open in this area.

Management Action. (U) Station management continues to work on resolving findings from the March 2002 inspection.

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

(U) **Kunia Regional Security Operations Center**; NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-02-0003, 24 September 2002

Summary. (U//~~FOUO~~) A joint team of inspectors from the SCEs and NSA conducted an inspection at the Kunia Regional Security Operations Center (KRSOC) from [redacted] The inspectors found a site successfully prosecuting a set of targets that are very diverse, both technically and geographically; however, the team also found some problems that are impacting the site's effectiveness. It was noted that about [redacted] Additionally, there are concerns about assigning personnel with the required skills, experience, and leadership to key positions. A rigorous qualifications-based

selection process is needed. [redacted]

there are two findings related to jointness. The KRSOC needs to make more progress in certain jointness issues relating to its J1 and common workforce training, and the Central Security Service needs to identify a more definitive end-state. Overall, the KRSOC is best described as "consolidated" rather than "joint." More Senior Noncommissioned Officer leadership is needed on the watch floor, and most Operations sections are still Service-specific.

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

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

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

(U) **Allegation of Contract Fraud**; NSA/CSS IG, IV-00-0032, 10 April 2002

Summary: (U) An OIG Investigation was conducted into potential false claims by a contractor for computer software, installation and training totaling [redacted] which were never received by the Agency. The investigation found that an Agency employee received and lost the software and was careless when he mistakenly authorized a [redacted] payment for installation and training prior to those services being received. Additionally, the investigation found that the Agency employee failed to protect Government property by not developing, implementing, and utilizing an effective property accountability system for the software under his control -- resulting in the loss of [redacted] in software. Lastly, the investigation found the terms of the contract required installation of the software. The software was not installed; there was no performance under the contract and no final acceptance of services and materials. The Agency employee was given a verbal reprimand; and an action to terminate the contract for default and recovery of approximately [redacted] paid on behalf of three Federal Agencies, is pending against the contractor.

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

(U) **Alleged Unauthorized Commitments**; NSA/CSS IG, IV-01-0051, 19 August 2002

Summary. (U) An OIG Investigation found that an Agency employee engaged in a series of unauthorized contractual commitments by knowingly directing a contractor to perform as a general contractor to procure [redacted] in goods and services outside the scope of the contract. It was also found that the Agency

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

~~SECRET//X1~~

employee failed to fulfill his assigned duties as the Contracting Officers Representative (COR) by signing receipts for deliveries of items he did not verify were received: such as [redacted] for self defense classes; [redacted] for twenty 2-way radios and [redacted] for 12 pair of Ocean Wave sunglasses. The Agency employee also willfully submitted false documents intended to limit the CO's knowledge of what was actually acquired under the contract for items such as the unauthorized installation of an [redacted] trailer and the unauthorized construction of an [redacted] building. We recommended that: 1) action be taken against the CO for his supervisory failures; 2) the Agency employee be permanently barred from serving as a COR; and 3) additional action be taken to recover [redacted] for unauthorized and unaccounted for purchases. Finally, the investigation revealed multiple indicators of fraud involving the contractor and possibly Government personnel. Evidence indicating false claims, false documents and conspiracy to defraud the Government was provided to the Defense Criminal Investigative Service (DCIS) for further investigation. The DCIS investigation is on-going.

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

~~SECRET//X1~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

FOR THE PERIOD October 1, 2002 THROUGH March 31, 2003

(U) **Competition in Contracting**; NSA/CSS IG, AU-02-0010, 18 October 2002

Summary. (U) The Competition in Contracting Act (CICA) requires full and open competition, to the maximum extent possible, for all federal procurements. To this end, the Senior Acquisition Executive set a goal of competing 80 percent of Agency contracts for FY2001. This audit found that controls over the award of sole-source contract actions were strong, but the categorization of competitive and non-competitive awards needed improvement. After reviewing all awards of $1 million or more, we concluded that Agency metrics for FY2001 overstated the extent to which contracts were competed by about 7% of the number of contracts and about 14% of their dollar value. We attributed the overstatement to deficiencies in three areas: training, automated controls to prevent erroneous data entries, and quality assurance.

Management Action. (U) The [redacted] has initiated actions to improve the accuracy and reliability of data and metrics regarding procurement actions. Statistics regarding competition will be changed to reflect the most recent Defense Federal Acquisition Regulation Supplement guidance.

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

(U) **National SIGINT Collection Center**; NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-02-0004, 23 October 2002

Summary. (U) This joint inspection found the command climate in the National SIGINT Collection Center (NSCC) to be poor. [redacted]

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

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

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

Overall Report Classification: (U) ~~TOP SECRET//COMINT~~ (b)(3)-P.L. 86-36

(U) **Information Operations Technology Center**; NSA/CSS IG, IN-02-0001, 9 December 2002

Summary. (U//~~FOUO~~) The Information Operations Technology Center (IOTC) is a joint DoD and Intelligence Community organization. Our inspection found that, on the whole, Agency support to the IOTC is improving, [redacted] for this high-priority external customer. We also found that the Information Assurance Directorate (IAD) at NSA needs a more productive relationship with the IOTC. NSA is doing an adequate job of providing enabling and administrative support to the IOTC, [redacted]

Management Action. (U//~~FOUO~~) SID officials have agreed to establish policies and procedures to ensure appropriate collaboration between SID and IOTC managers, along with a plan to give authorized external customers better access to information. In addition, the IAD has assigned an account manager to the IOTC to strengthen the relationship, and acquisition officials are working to determine the necessary level of support.

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

(U) **Acquisition Reform Initiatives**; NSA/CSS IG, AU-02-0006, 27 January 2003

Summary. ~~(S)~~ As part of the FY2002 planning process, NSA's then Senior Acquisition Executive (SAE) asked the OIG to review two acquisition reform initiatives: the appointment of acquisition program managers (APMs) and full implementation of the Defense Acquisition Workforce Improvement Act (DAWIA). A particular focus was the effectiveness of APMs in executing the [redacted] in supplemental counterterrorism (CT) funds that NSA received after 11 September. Our review found that APMs are doing a good job with supplemental funds but are impeded by resource shortfalls. [redacted]

Management Action. (U) We discussed these issues with the new SAE who is committed to acquisition process and workforce improvement. His organization is working with Agency leadership to identify the funds and staff necessary to carry

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

out its mission. They also have drafted a revised DAWIA regulation that requires DAWIA position audits, a workforce plan, and performance metrics.

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

(U) **Advanced Research and Development Activity**; NSA/CSS IG, AU-02-0008, 13 February 2003

Summary. (U//~~FOUO~~) The Advanced Research and Development Activity (ARDA) was created in FY1999 and placed under NSA management to give the Intelligence Community a world-class research facility focused on operational problems involving information technology. With ARDA's budget slated to double in FY2003, the OIG conducted an audit to evaluate ARDA's stewardship of these funds. Our review found that ARDA has made admirable progress since its inception but must improve program management in order to achieve the results envisioned by the Director for Central Intelligence. Specifically, ARDA is not adequately staffed to direct and oversee its complex portfolio of programs; while interacting closely with the DCI, ARDA does not have a formal process to link its activities to the Defense Science and Technology Strategy; and ARDA does not have a written policy promoting use of a competitive, merit-based process for awarding funds.

Management Action. (U) Management agreed with the audit recommendations to determine appropriate program staffing through a study and establish an oversight board to review the direction and quality of ARDA's research program. The ARDA Director also plans to enhance measurements of program progress and effectiveness and has already developed a written policy promoting a competitive, merit-based process for awarding funds.

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

(U) **Threat Analysis Division of the National Security Incident Response Center;** NSA/CSS IG, JT-03-0001, 24 March 2003

Summary. (U//~~FOUO~~) The Threat Analysis Division of the National Security Incident Response Center produces all-source intelligence analyses of adversarial threats to vital U.S. information networks. Its primary customers are tactical military users. Our organizational inspection found that this is a well-managed organization with high morale and an enviable record of customer satisfaction. At the time of our inspection, the contractor for an analysis effort

[redacted]

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

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

~~SECRET//X1~~

[redacted] In addition, customer satisfaction levels—already very high—could be optimized by systematically collecting and analyzing customer feedback.

Management Action. (U//~~FOUO~~) Since the publication of the draft inspection report, [redacted] The Information Assurance Directorate recently contracted for a strategic reassessment of the division's approach to threat analysis in light of emerging threats to information systems.

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

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

(U//~~FOUO~~) **RAINFALL;** NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-03-0001, 25 March 2003

Summary. (~~C~~) This joint inspection found a site that was successfully executing its mission; [redacted] the Application of Dislocation Allowance was not consistent among the U.S. military services at the site – a repeat finding from our 2000 joint inspection.

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

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

(U) **Morale, Welfare, and Recreation Fund at Menwith Hill Station;** NSA/CSS IG, AU-02-0013, 31 March 2003

Summary. (U) Morale, welfare, and recreation (MWR) programs help maintain mission readiness and productivity and build a strong sense of military community. However, the March 2002 Joint Inspectors General report on Menwith Hill Station (MHS) found that the site's underfunded MWR programs were a major source of dissatisfaction, contributing to serious morale problems. Our audit of MWR operations found that the lack of a central accounting system makes it impossible to determine if the level of appropriated fund (APF) support complied with DoD standards, but we estimate that it fell well short of the standard, particularly for Category C (revenue-generating) activities. Better internal controls

are needed in three areas, along with regular audit coverage of the MWR fund and a formal long-range plan for renovations and repairs to MWR facilities.

Management Action. (U) We recommended that the Chief Financial Manager and the MHS Commander find ways to ensure that APF support to MWR activities at the site meets DoD standards. Additionally, we recommended a central accounting system that tracks all APF support to MWR activities, along with better internal controls.

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

(U~~//FOUO~~) **NSA Travel Card Investigation**; IV-02-0043, 31 October 2002

Summary. (U~~//FOUO~~) An OIG investigation found that an NSA civilian failed to follow Code of Federal Regulations and Agency guidance by using his Government Travel Card (GTC) for personal purposes. From July 2001 through July 2002, the employee misused his GTC to obtain 98 cash advances totaling $30,230 for personal purposes unrelated to official travel-related expenses. The investigation also found that the employee was delinquent on payment of the GTC balance. The balance has since been satisfied and administrative actions are pending.

Overall Report Classification: (U) ~~SECRET//X1~~

(U~~//FOUO~~) **NSA Travel Card Investigation**; IV-02-0035, 01 November 2002

Summary. (U~~//FOUO~~) An OIG investigation found that an NSA civilian employee was unable to pay her Government Travel Card (GTC) bill because she used her TDY advances for family dining and entertainment expenses while she was between PCS assignments. In an attempt to keep a zero balance on her GTC, replace shortages in her checking account, and hide her financial irresponsibility from her husband, she obtained a pre-PCS advance and began taking unauthorized cash advances with her Government Travel Card. When confronted with a 60-day delinquency on her GTC, she secured a loan from her Thrift Savings Plan account and paid her GTC balance in full. Her GTC has been suspended. The employee was also suspended from duty for three days and has agreed to undergo financial and other counseling for a period of one year.

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

(U//~~FOUO~~) **NSA Contractor Labor Hour Investigation**; IV-02-0021, 8 November 2002

Summary. (U//~~FOUO~~) An OIG investigation into a complaint that an Agency contractor employee was claiming hours in excess of what he was actually working revealed that over the course of three years, NSA was improperly charged for 857 labor hours, amounting to [redacted] There was insufficient evidence to prove that the company knowingly presented a false claim to the government in this case. The company has agreed to repay the agency for the hours and the employee in question was terminated. The case was referred to the Defense Criminal Investigative Service (DCIS) for consideration of criminal charges against the former contractor employee.

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

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

~~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]

(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

~~SECRET//X1~~

Certification and Accreditation Reviews. [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

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