(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

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

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] for12 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~~