(U) SEMIANNUAL REPORT TO THE CONGRESS

For the Period April 1, 2005 Through September 30, 2005

(U) **Kunia Regional Security Operations Center**; NSA/CSS IG; INSCOM IG; AIA IG; NSG IG; JT-05-0001; 31 March 2005

Summary. (U~~//FOUO~~) A team of inspectors from the Service Cryptologic Elements and NSA conducted a joint inspection of the Kunia Regional Security Operations Center (KRSOC). KRSOC is the first Regional Security Operations Center to be inspected by the Joint IG Team since the issuance of NSA/CSS Policy 1-3, *NSA/CSS Governance*, and the announcement of the NSA/CSS Build-Out. We found the site Headquarters relationship to be generally positive; some costly site-directed initiatives had not been coordinated with Higher Headquarters; and communication between KRSOC leadership and the SIGINT Analysis and Production Directorate needs attention, especially in light of the NSA/CSS Build-Out, which will require close collaboration in order to succeed.

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

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

Category. (U) Joint Warfighting and Readiness

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

(U) **Attack Sensing and Warning Program (Followup)**; NSA/CSS IG; ST-05-0014; 28 April 2005

Summary. (U~~//FOUO~~) The purpose of the Attack Sensing and Warning (AS&W) Program is to protect [redacted] The 2004 audit report found that the AS&W program had not undergone the type of independent review required by DoD and NSA regulations for high-dollar programs. As a result of our followup review, we were able to close out four of the six recommendations made in the 2004 final report. We found two recommendations that management had not addressed: The Defensive Information Operations Group has not developed the documentation required by DoD and NSA acquisition regulations and the same Group did not assign a qualified acquisition manager to the program as required by DoD and NSA acquisition regulations.

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

Category. (U) Infrastructure and Environment

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: ~~20291123~~

(U) **Cryptologic Mission Management Program**; NSA/CSS IG; AU-04-0005; 3 May 2005

Summary. (U~~//FOUO)~~ We found the Cryptologic Mission Management (CMM) Program Management Office was staffed by qualified and experienced acquisition and engineering personnel focused on program results and compliance with DoD and Agency acquisition management requirements. However, a recent review by an Integrated Process Team (IPT), led by the Agency's Chief Systems Engineer, made recommendations to help reduce technical and other program risks. Carrying out the IPT recommendations will postpone the Milestone B decision for CMM Increment 1 from the end of September 2004 to May 2005. Specifically, our audit found problems with the CMM risk reduction efforts known as the Focused Demonstration Operational Capability in the following areas: Award Fee determination; Deliverables; and Unverified Costs.

Management Action. (U//~~FOUO~~) Management is acting on all but one of our recommendations. The SAE nonconcurred with our recommendation to establish a process to resolve major disagreements on the award fee. Our recommendation is necessary to prevent future arbitrary award fee decisions as well as fraud or wrongdoing. Therefore, we are requesting that SAE reconsider his nonconcurrence.

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

Category. (U) Acquisition Processes and Contract Management

(U//~~FOUO~~) **Nuclear Weapons Personnel Reliability Program**; NSA/CSS IG; AU-04-0010A; 26 May 2005

Summary. (U~~//FOUO)~~ The purpose of the Nuclear Weapons Personnel Reliability Program (NWPRP) is to ensure that everyone who performs Nuclear Command and Control (NC2) duties meets the highest standards of reliability. Our audit found that the [redacted] strengthened the NWPRP control environment by implementing the recommendations from our 2002 review, but the following issues need attention: [redacted]

Management Action. (U~~//FOUO)~~ Management agreed to implement a formal training program for NWPRP management and support personnel designate the Staff Security Officer as the official responsible for advising the program on security eligibility; establish formal procedures for NWPRP drug testing; and formally determine the status of [redacted] (b)(3)-P.L. 86-36

Overall Report Classification. (U) CONFIDENTIAL//MR

Category. (U) Joint Warfighting and Readiness

(U) **Office of Equal Employment Opportunity;** NSA/CSS IG; ST-05-0002; 1 June 2005

Summary. (U) The study found that mandated timelines related to the investigation of formal Equal Employment Opportunity (EEO) complaints are not being met. In addition, data related to EEO complaints, which must be posted on the Agency's public website, was incomplete and inaccurate, and NSA's FY2004 EEO Program Status Report, due by 31 January 2005, was not submitted to the Equal Employment Opportunity Commission until late April.

Management Action. (U) Management concurred with the recommendations to correct the issues described above.

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

Category. (U) Human Capital

(U) **Classified Material Destruction;** NSA/CSS IG; ST-05-0022; 7 June 2005

Summary. (U~~//FOUO)~~ An anonymous complaint sent to the Director, NSA and the Office of Inspector General (OIG) alleged that Eagle Alliance (EA) was utilizing government resources and processes to dispose of EA computer equipment. The GROUNDBREAKER contract stipulates that EA is responsible for disposal of EA computer equipment. The complaint also stated that EA did not have standard operating procedures (SOPs) for disposing of computer equipment. Our special study found no evidence that EA was using government resources to dispose of EA-owned computer equipment. However, EA has not instituted two elements required by the contract: written SOPs covering its disposal process and a process for disposing of hard drives after removal from EA-owned computers. We also found that EA is storing approximately [redacted] We recommended an immediate decision to either have the Agency take over the disposal function (amending the contract accordingly) or require EA to comply with the contract terms.

Management Action. (U) EA will provide its position in writing to the Maryland Procurement Office. Senior officials will then present the Agency's approach in writing to the OIG.

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

Category. (U) Acquisition Processes and Contract Management

(U) **Contract Rates for Office Space;** NSA/CSS IG; AU-04-0019; 8 June 2005

Summary. (U) NSA has operated under a model that collocates contractors with the

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

missions they serve. Our audit found that Contracting Officer's Representatives (CORs) were not validating on- and off-site costs charged for the contracts in our sample. Since overhead rates for work done at contractor facilities are usually higher than for government facilities, NSA could be paying off-site rates for contractors who are actually working on-site.

Management Action. (U) The Maryland Procurement Office agreed to issue guidance that requires contractors to provide a breakout of on- and off-site rates and hours on invoices and to require CORs to check the on- and off-site rates and hours.

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

Category. (U) Acquisition Processes and Contract Management (b)(3)-P.L. 86-36

(U//~~FOUO~~) **Followup Inspection: Special U.S. Liaison** [redacted]
NSA/CSS IG; INSCOM IG; NSG IG; AIA IG; [redacted]

Summary. (U//~~FOUO~~) A followup joint inspection of the Special U.S. Liaison [redacted] NSA/CSS found significant progress from the April 2004 joint IG inspection in the areas of training, intelligence oversight, security, communications, and information assurance. Civilian employee recruitment has improved, albeit slowly; however, several findings remain open, pending action by NSA Headquarters.

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

Overall Report Classification. (U) SECRET//COMINT//REL TO USA, CAN, GBR, and NZL//20291123

Category. (U) Joint Warfighting and Readiness

(U) **Tailored Access Operations;** NSA/CSS IG; ST-04-022C; 19 July 2005

Summary. (U//~~FOUO~~) This study, the third in a series of three reports on the Agency's Tailored Access Operations (TAO) office, focused on the control environment. We found that: 1) [redacted]

Management Action. (U) TAO management concurred with all OIG recommendations and plans to take corrective action by 1 October 2005. The Finance Directorate will move the reimbursement process to the Disbursing Office to [redacted]

Overall Report Classification. (U) TOP SECRET//COMINT//NOFORN//220291123

Category. (U) Joint Warfighting and Readiness

(U) **FY2005 Report on Compliance With The Federal Information Security Management Act at NSA/CSS;** NSA/CSS IG; AU-05-0004; 5 August 2005

Summary. ~~(C)~~ NSA is making a concerted effort to address the weaknesses identified in our FY2004 audit of compliance with The Federal Information Security Management Act (FISMA). Although impediments still exist to achieving the Agency's certification and accreditation (C&A) goals, the Chief Information Officer (CIO) has made progress. NSA continued to maintain and track a Plan of Action and Milestone to address the inadequate C&A of Agency systems, identified as a material weakness in FY2002. However, we discovered several weaknesses in the Agency's IT security posture during our FY2005 FISMA review. We found that NSA has [redacted]

Management Action. (U~~//FOUO~~) The CIO has made a concerted effort to address FISMA requirements. This includes holding regular FISMA working group meetings, providing a data call to all responsible organizations to address reporting requirements, and raising awareness of FISMA requirements. In addition, the CIO established labs to perform vulnerability testing and penetration testing and secured additional resources to help create the documents associated with certifying mission-critical systems.

Overall Report Classification. (U) TOP SECRET//COMINT//NOFORN//20291123

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

Category. (U) Information Technology Management

(U) **NSA/CSS Representative Pacific (NCPAC);** NSA/CSS IG; IN-05-0002; 16 August 2005

Summary. (U~~//FOUO~~) Our inspection found that the Agency is well represented by the NSA/CSS Representative (NCR) Pacific and his staff. Pacific Command (PACOM) officials we interviewed had a high opinion of the NCR and his staff and regard them as a "model" of effective NSA/CSS liaison. Innovative NCPAC initiatives include embedding over [redacted] of the NCPAC staff in PACOM activities. Increased levels of support in the information operations arena are also highly valued by the Command. Areas for improvement include the following: NSA/CSS Policy 1-3 on governance does not conform to actual practice in the Pacific Theater; the operational span of control for the NCR is unclear; [redacted] the Regional Communications Security Monitoring Center, does not have enough assignees to perform its mission; and NCPAC's representational efforts to PACOM sub-commands in regard to Information Assurance are insufficient.

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

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

Management Action. (U) Management concurred in all recommendations, nine of which are already closed.

Overall Report Classification. (U) SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

Category. (U) Joint Warfighting and Readiness

(U) NSA/CSS IG;

Summary. (U~~//FOUO~~) Our inspection of the organization found that major development programs, including have potential, but their ultimate success at the Directorate and Agency levels. The Signals Intelligence Directorate leadership must act quickly to manage the risks

Management Action. (U) The Director for Analysis and Production concurred with all of the recommendations and convened an Integrated Product Team to address them.

Overall Report Classification. (U) SECRET//REL TO USA, AUS, CAN GBR, and NZL//20291123

Category. (U) Joint Warfighting and Readiness

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

~~(S)~~ NSA/CSS IG

Summary. ~~(S)~~ We visited three sites selected on the basis of location, risk, and reported oversight issues. Based on our findings, a representative of SID is working with one of the sites to improve analysis and reporting on SIGINT collected there, while another site launched a comprehensive reassessment of its ability to contribute to the national SIGINT mission and satisfy the requirements of We also recommended that sites improve their emergency action procedures. To that end, has now clarified its emergency operations procedures, and agreed to conduct emergency drills.

Overall Report Classifications. (U) TOP SECRET//COMINT//20291123 (all three reports)

Category. (U) Joint Warfighting and Readiness

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

~~SECRET//20291123~~

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

(U) **Electronic Intelligence (ELINT) Modernization Program;** NSA/CSS IG; AU-05-0001; 19 September 2005

Summary. ~~(S)~~ Budgeted to receive [redacted] from FY2004-11, the ELINT Modernization Program is intended to develop, integrate, and deploy the capabilities needed to fill the gaps identified in a study conducted at the behest of Congress. The audit identified two significant problems: [redacted]

Management Action. (U) Management concurred with all recommendations and corrective action is underway.

Overall Report Classification. (U) SECRET//TALENT KEYHOLE//20291123

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

Category. (U) Joint Warfighting and Readiness

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

(U) [redacted] NSA/CSS IG; INSCOM IG; AIA IG; NSG IG; [redacted]

Summary. ~~(C)~~ A team of inspectors [redacted]

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

Overall Report Classification. (U) SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

Category. (U) Joint Warfighting and Readiness

(U) **Precious Metals Recovery Program;** NSA/CSS IG; ST-05-0005; 19 September 2005.

Summary. (U~~//FOUO~~) The Precious Metals Recovery Program (PMRP) recycles film, circuit boards, and microchips for NSA, DoD, and other Intelligence Community customers. Our special study found that the PMRP [redacted] and no formal plan to spend the funds [redacted] generated from recycling microchips.

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

Additionally, the policy establishing the PMRP has not been updated since 1991, and internal controls are needed to safeguard the precious metals that are recovered when microchips are recycled.

Management Action. (U~~//FOUO)~~ Management nonconcurred with our recommendation to develop a plan to spend these funds rather than letting the money accumulate. Consequently, we are forwarding the report to the Comptroller.

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

Category. (U) Other

(U) [redacted] NSA/CSS IG; [redacted]

Summary. ~~(S)~~ Our functional inspection of NSA's program to [redacted] which is managed by the Signals Intelligence Directorate (SID), focused on analysis and training with the goal of determining whether SIGINT analysts [redacted] We found that Agency and SID leaders have not conducted a risk assessment to determine the appropriate level of effort for [redacted] and Agency policy does not adequately address the authorities and responsibilities for this function. Moreover, NSA's Implementation Plan for [redacted] does not address a key goal of the Director of Central Intelligence: [redacted]

Management Action. (U) Management concurred with our recommendations and is taking appropriate corrective action.

Overall Report Classification. (U) TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123

Category. (U) Joint Warfighting and Readiness

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

(U) **Information Technology Directorate Field Liaison Division;** NSA/CSS IG; IN-05-0005; 20 September 2005

Summary. (U~~//FOUO~~) The Information Technology Directorate's (ITD) Field Liaison Division is a [redacted] organization created in January 2003 as a direct response to recommendations from several Joint IG inspections. During the inspection, the Field Liaison Division's leadership changed and the ITD restructure began, resulting in a new focus for the Division. Nevertheless, the Director for IT asked that we proceed with the inspection to help identify problems or issues that need to be considered in ITD's restructuring and consolidation efforts. To this end, we issued a letter report advising the Director for IT of areas in need of attention as the ITD consolidation continues. Our inspection found that the Field Liaison Division has had a positive effect on the Extended

Enterprise; however, as ITD implements its concept of centralized management with decentralized execution, close attention should be given to the following: clearly delineating roles and responsibilities; implementing a mechanism for assessing the effectiveness of the new structure; and providing a dynamic, up-to-date, and useful NSANet presence.

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

Category. (U) Information Technology Management

(U) **Meade Operations Center;** NSA/CSS IG; INSCOM IG; AIA IG; NSG IG; JT-05-0006; 30 September 2005 (b)(3)-P.L. 86-36

Summary. (U~~//FOUO~~) The Joint IGs conducted an inspection of the [redacted] Meade Operations Center (MOC)) in 2002. A followup inspection in 2003 assessed progress in several areas, including Command Topics and Mission Operations. In keeping with the three-year inspection cycle for major field sites, the Joint IGs scheduled an inspection of the MOC to begin in August 2005. Our preparation for this inspection revealed that the predominant theme of the two previous inspections remains unresolved – the persistent lack of documented mission and an effective governance mechanism or chain-of-command. In a Joint IG Management Advisory Report, the Joint IGs suspended the on-site phase of the inspection until the Signals Intelligence Directorate (SID) clearly documents a mission and begins to exercise an effective governance approach for the organization. The Joint IGs concluded that the unresolved issues are unlikely to improve without a zero-based review to determine the missions, if any, that are best performed by the MOC, and 2) the implementation of effective governance from SID of those missions.

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

Category. (U) Joint Warfighting and Readiness

(U) **Inappropriate Representation Before the Government and Misuse of Resources;** NSA/CSS IG; IV-05-0005; September 2005

Summary. (U~~//FOUO~~) An NSA/CSS employee who established a software company inappropriately represented his company in a "pitch" meeting before the Government. This employee also misused Government resources to solicit and conduct private business. Furthermore, the employee and his business associate knowingly misused Government Information Systems to solicit business for their private company. Due to the potential Title 18 violation, the matter was referred to the DoJ for a prosecutive opinion.

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

Category. (U) Personnel/Standards of Conduct; Procurement and Contract Administration

(U) **Inappropriate Representation Before the Government;** NSA/CSS IG; IV-05-0011; June 2005

Summary. (U~~//FOUO~~) An NSA employee who "moonlighted" part-time for an Agency contractor inappropriately represented the contractor in a meeting before the Government, in a particular matter in which the United States was a party and had a direct interest. Due to the potential Title 18 violation, our report was referred to the DoJ for a prosecutive opinion.

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

Category. (U) Personnel/Standards of Conduct

(U) **Time and Attendance Investigations**; NSA/CSS IG; IV-04-0040 (31 May 2005); IV-05-0008 (23 May 2005); IV-05-0023 (9 September 2005); IV-05-0032 (9 September 2005)

Summary. (U~~//FOUO~~) The OIG substantiated four allegations of Time and Attendance abuse, wherein employees claimed hours in excess of those they were determined to have actually worked. In the aggregate, these cases will result in the recovery of approximately $46,500.00 in funds paid to employees for hours falsely claimed.

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

Category. (U) Other (Fraud)