~~SECRET//REL TO USA, FVEY~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) ***For the Period April 1, 2008 through September 30, 2008***

(U) Assessment of Management Controls to Implement the Protect America Act of 2007**; NSA/CSS IG; ST-08-0001; 3 April 2008**

(U//~~FOUO~~) Summary. NSA has implemented procedures to comply with the provisions with the Protect America Act of 2007 (PAA), which modified the Foreign Intelligence Surveillance Act (FISA) and was signed into law on 5 August 2007. To protect the privacy rights of U.S. persons, the new legislation required NSA to implement and follow procedures established by the Director, NSA, to ensure its adherence to three requirements: that targets are located overseas, that the foreign intelligence purpose is significant, and that personnel follow applicable minimization procedures. Our findings included: 1) NSA immediately implemented DIRNSA-directed procedures on compliance with PAA and strong controls to determine that targets are located outside of the U.S; 2) PAA tasking needs additional controls, in particular to verify that only authorized selectors are on collection and that the information acquired relates to the foreign intelligence target; and 3) more rigorous controls will increase the reliability of spot checks for PAA compliance.

(U) Management Action. **Management concurred with the recommendations.**

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

(U) Category**. Significantly Improve Intelligence Capabilities**

(U) NSA/CSS Hawaii; **NSA/CSS IG; AFISRA IG; INSCOM IG, NNWC IG; INSCOM; JT-08-0001; 23 April 2008**

(U//~~FOUO~~) Summary. **The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency; Naval Network Warfare Command; Intelligence and Security Command; and NSA conducted the inspection at Kunia, Hawaii, in January and February 2008. The transformation challenges identified during the inspection of mission operations at NSA/CSS Hawaii (NSAH) are a microcosm of those facing the Extended Enterprise: the requirement to maintain legacy capabilities on critical enduring target sets and, at the same time, develop a workforce that can take on the challenges of the networked world. We found that** [redacted] **With the completion of the new NSAH building years away, the likelihood that personnel will have to remain in the tunnel past FY13 has emerged. An engineering and safety study of the tunnel has revealed several health and safety problems that must be addressed in the near term. Funding for these repairs must be identified as well. Finally, the inspection team identified fourteen commendable achievements across all elements of NSAH, reflecting solid leadership at all levels.**

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

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~20320108~~

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

(U) Overall Report Classification. **TOP SECRET//COMINT//REL TO USA, FVEY**

(U) Category. **Joint Warfighting and Readiness**

(U) Official Representation and Confidential Military Funds**; NSA/CSS IG; AU-08-0017; 23 April 2008**

(U//~~FOUO~~) Summary. **We conducted this audit to determine whether Official Representation and Confidential Military Funds are managed consistent with laws and regulations and to follow-up on our previous audit recommendations. We found that NSA organizations, such as the Internal Review Group and Operations Risk Management, have conducted adequate internal-control reviews of the Official Representation and Confidential Military Funds. Therefore, we discontinued our audit. We will periodically review the Internal Review Group's accounting practices to ensure that adequate oversight continues.**

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

(U) Category. **Financial Management**

(U) Advisory Report on NSA/CSS Extended Hours Operations**; NSA/CSS IG; ST-08-0003; 30 May 2008**

(U//~~FOUO~~) Summary. **Extended-hours areas include watch/operation centers, production areas, and support offices. We reviewed the consolidation achieved and efforts currently underway by the National Security Operations Center, Signals Intelligence Directorate, Technology Directorate, Information Assurance Directorate, and other Agency organizations. Our special study found that over the past 12-18 months significant progress in reducing and consolidating extended- hours organizations has been achieved. An interview of the Director of Installations and Logistics and the Special Executive for Power, Space, and Cooling revealed that recent consolidation efforts have produced available space for other uses and that extended-hours operations areas have minimal effect on power consumption. We also found that there is no single authority for establishing extended-hours operations, nor is there official policy or guidance for setting up or maintaining extended-hours areas or functions. Finally, NSAW does not maintain a consolidated list of extended-hours operations areas.**

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

(U) Category. **Joint Warfighting and Readiness**

(U) NSA/CSS Colorado; **NSA/CSS IG; AFISRA IG; INSCOM IG; JT-08-0002; 18 June 2008**

(U//~~FOUO~~) Summary. **The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency; Intelligence and Security Command; and NSA conducted the inspection at NSA/CSS Colorado (NSAC). This was the first inspection of NSAC. The**

inspectors found that confusion surrounding the NSAC mission, functional realignment, and implementation timing has created dissention and distrust that has diverted mid- and upper-level management's focus from the mission. We found a number of compliance problems typical of a site undergoing its first inspection. For example,

Finally, the inspection team identified three commendable achievements across all elements of NSAC.

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

(U) Overall Report Classifications. SECRET//COMINT//TALENT KEYHOLE//REL TO USA, FVEY

(U) Category. Joint Warfighting and Readiness

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

(U) Closeout; NSA/CSS IG;

(U//~~FOUO~~) Summary. In May 2002, the Director, NSA notified the Assistant Secretary of Defense, Command Control, Communications and Intelligence, that the

Our audit found that; overall, the Microelectronics Solutions organization has made little progress in the closeout of in accordance with applicable DoD and NSA/CSS regulations, especially in regard to the

has done little to prepare the building for reutilization or to reduce its power consumption. This failure to act persists even though the operations ended and Microelectronics Solutions management has had to prepare for the shutdown. , the Agency has spent more than on this effort and,

(U//~~FOUO~~) Management Action. Management concurred with our recommendations, but advised us that power consumption was not a priority for the closure. Because of the Microelectronics Solutions management's inability to make any progress in the shutdown of we made a recommendation to the Information Assurance Director to restructure Microelectronics Solutions management that is responsible for the delay.

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

(U) Category. **Joint Warfighting and Readiness**

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

(U) NSA's Top Secret /Special Compartmented Information Public Key Management Infrastructure**; NSA/CSS IG; AU-08-0001; 27 June 2008**

(U//~~FOUO~~) Summary. **NSA Public Key Infrastructure (PKI) protects NSA communications and networks by providing authentication of users, encryption, and digital signing. NSA PKI ensures that security restrictions on classified data and information are maintained when information is e-mailed or published on web pages. Our audit found that,**

[redacted]

(U) Management Action. **During the audit, the Chief Information Security Officer initiated actions to address the noted conditions.**

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

(U) Category**. Joint Warfighting and Readiness**

(U) Nuclear Weapons Personnel Reliability Program; **NSA/CSS IG; AU-08-0006; 7 July 2008**

(U//~~FOUO~~) Summary. **One of the Agency's most important missions is** [redacted] **The purpose of the Nuclear Weapons Personnel Reliability Program (NWPRP) is to ensure that everyone who performs these duties meets the highest standards of reliability, including physical, psychological, and technical competence. The NSA/CSS Office of Inspector General, which is responsible for DoD oversight, has conducted periodic audits of the NWPRP since 2001. Our most recent audit found that the NWPRP has significantly improved the security, medical, and program management controls since our initial review in 2001. The program has established a systemic process to ensure and document that individuals accepted into the program meet, and continue to meet, DoD reliability standards. NSA policy requires that NWPRP employees be randomly drug tested at a higher rate than the rest of the Agency population. However, flaws in the selection methodology prevent the program from meeting its stated goals.**

(U) Management Action. **Management concurred with all recommendations and corrective actions are underway.**

(U) Overall Report Classification. **CONFIDENTIAL//REL TO USA, FVEY**

(U) Category. **Joint Warfighting and Readiness**

(U) RT-10 Initiative**; NSA/CSS IG; AU-07-0016; 11 July 2008**

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

~~(S//REL)~~ Summary. **To improve SIGINT support for the Joint Intelligence Operations Capability in Iraq, NSA developed a system called RT-10;** [redacted] **We performed this audit in response to an allegation that RT-10 had been developed without the programmatic oversight that NSA and DoD regulations require. We found this allegation** [redacted] **essential for an ongoing war. The Agency has recently made progress in establishing program structure for RT-10, an effort that should be reinforced as the system is** [redacted] **Our audit concluded that, since** [redacted] **the RT-10 program has operated without the oversight and documentation necessary to hold the Program Office accountable for cost, schedule, and performance. With DoD support, the program was expanded** [redacted] **although a Capability Production Document, the formal requirements specification, was not sent to DoD for validation until** [redacted]

(U) Management Action. **Management concurred with the recommendations.**

(U) Overall Report Classification. **TOP SECRET//COMINT-ECI RDV//NOFORN**

(U) Category. **Joint Warfighting and Readiness**

(U) [redacted] on the Agency's Unclassified Network; **NSA/CSS IG; AU-08-0005B; 14 July 2008**

~~(S//REL)~~ Summary. **In its current state, the Technology Directorate (TD)-developed** [redacted]

(U) Management Action. **The TD concurred with our recommendations, and the Signals Intelligence Directorate and NSA/CSS Threat Operations Center agreed to assist TD in the process. TD has started to take corrective actions.**

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

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Joint Warfighting and Readiness**

(U) Compliance with the Federal Information Security Management Act at NSA/CSS; **NSA/CSS IG; AU-08-0012; 31 July 2008**

(U//~~FOUO~~) Summary. **Our FY 2008 audit on compliance with the Federal Information Security Management Act found that, after another FISMA reporting cycle, the Agency has**

made some improvements to the security of its systems and networks. Information Technology (IT) security personnel are becoming more effective in [redacted] into major Agency initiatives. For example, [redacted] However, much more work must be done to correct the material weakness reported in August 2006 regarding IT security for systems within NSA's control. Weaknesses that have not been fully mitigated include:

[redacted]

(U) Management Action. **Management concurred with the recommendations and corrective actions are underway.**

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

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

(U) Category. **Information Security and Privacy**

(U//~~FOUO~~) Advisory Report on the [redacted] NSA/CSS IG;

~~(S//REL)~~ Summary. **To achieve its stated goal of [redacted] NSA has implemented a series of initiatives called Transformation 3.0. One initiative, [redacted] This advisory review focused on the Intelligence Oversight (IO) and internal controls implemented by [redacted] developers. Our review concluded that [redacted] developers are properly applying Signals Intelligence (SIGINT) rules to SIGINT activities and Information Assurance (IA) rules to IA-relevant activities and are implementing appropriate IO controls. However, not all IO controls have been documented or implemented because [redacted] is not yet fully operational under [redacted] Because [redacted] supports a new mission for NSA, and the risk is high if safeguards are not incorporated into procedures to ensure protection of U.S. persons information, an IO review of control mechanisms may be warranted when [redacted] becomes fully operational.**

(U) Overall Report Classifications. **TOP SECRET//COMINT//REL TO USA, FVEY**

(U) Category. **Significantly Improve Intelligence Capabilities**

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

~~(S//REL)~~ Summary. **Our audit found that [redacted] which provides [redacted] Transformation 3.0 programs, is not adequately funded. Without adequate funding, critical components of the [redacted] program will fail. [redacted] is included in a set of projects called [redacted]. Since the project began, [redacted] development costs have been [redacted] The [redacted]**

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

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

[redacted]

(U) Management Action. **Management agreed with our recommendations to improve the requirements and budget processes for the [redacted] projects.**

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Significantly Improve Intelligence Capabilities**

(U) Agency's System Security Plans; **NSA/CSS IG; AU-08-0005A; 8 September 2008**

~~(S//REL)~~ Summary. **Since 2002, the Agency OIG has reported that deficiencies in the Agency's System Security Plans (SSP) Program [redacted] .Contributing factors include a lack of Agency requirements, standards, and resources. Our audit found that, although currently implementing initiatives to improve the SSP Program, [redacted] We also determined that the Information Security Office did not establish a baseline level of evidence for all accreditation decisions.**

(U) Management Action. **The Technology Directorate concurred with our recommendations and has started to take corrective actions.**

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

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Information Security and Privacy**

(U) Utilization of Time and Material (T&M) Contracts; **NSA/CSS IG; AU-07-0006; 16 September 2008**

(U//~~FOUO~~) Summary. **We performed this audit as part of the Agency OIG's contract fraud initiative to determine whether controls are adequate for contractor oversight. Since 2005, NSA has collected or is in the process of collecting more than $1 million in contractor mischarging on service contracts, including T&M. Today the Agency has more than [redacted] T&M contracts valued at about [redacted] Our audit found that the Agency does not routinely perform the extensive oversight needed for T&M contracts, in spite of recent substantiated mischarging. Our review of [redacted] contract actions confirmed this appraisal, especially in regard to certifying contractor invoices and validating contractor education and experience. The underlying cause of the contracting problems has been long-term understaffing of the Contracting Group. A recently approved FY2008 staffing increase to Acquisition should improve the Group's ability to work with Agency organizations to avoid T&M contracts and provide necessary oversight.**

(U//~~FOUO~~) Management Action. **The Director, Business Management Integration (BMI), has not provided comments to Recommendation 2 that Acquisition develop a plan to convert long-term T&M contracts to fixed-price contracts (including performance-based). We have again asked the BMI Director to respond to this report. The Contracting Group has taken or started to take corrective actions in response to our other recommendations. The Technology Directorate (TD) concurred with our recommendations, and the Signals Intelligence Directorate and NSA/CSS Threat Operations Center agreed to assist TD in the process. TD has started to take corrective actions.**

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

(U) Category. **Acquisition Processes and Contract Management**

(U) Joint Duty Assignment Program - Civilian; **NSA/CSS IG; ST-08-0020; 29 September 2008**

(U//~~FOUO~~) Summary. **Our special study on NSA's implementation of the Joint Duty Assignment (JDA) Program found that NSA is implementing the JDA program as effectively as possible given the evolving state of the JDA program within the Intelligence Community. DoD implementing guidance was issued on 2 June 2008; NSA's implementing guidance is currently in draft and is expected to be published shortly. However, we did identify the following concerns that may impede the JDA program: 1) The requirement to keep an individual on the losing organization's billet for the duration of the JDA tour, which may result in denial of the assignment, is a contentious issue; 2) JDA vacancies are not attracting candidates; and 3) JDA credit and waiver decisions are delayed awaiting policy and guidance.**

(U//~~FOUO~~) Management Action. **The Associate Directorate for Human Resource Services concurred with the report, with minor administrative changes.**

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

(U) Category. **Human Capital**

(U) China and Korea Missions; **NSA/CSS IG; IN-08-0001; 30 September 2008**

~~(S//REL)~~ Summary. **Our inspection of the China and Korea Production Center found that, with few exceptions, mission delegation and execution are working well, internal and external partnerships are positive and productive, and customer satisfaction is high. However, the following concerns surfaced:**

[redacted]

(U//~~FOUO~~) Management Action. **Management concurred with the recommendation and is taking corrective action.**

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

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Joint Warfighting and Readiness**

(b) (6)

(U) Time & Attendance Fraud; **NSA/CSS IG; IV-07-0029**

(U//~~FOUO~~) Summary. **The OIG substantiated an allegation that, between March 2006 and March 2007, a GG-13 NSA employee intentionally submitted false and inaccurate timesheets for a total shortfall to the government of 786 hours. On [redacted] the employee pled guilty in United States District Court to a felony violation of Title 18, United States Code, Section 1001 (False Statements). On [redacted] the employee was sentenced to [redacted] years probation, [redacted] home confinement, and [redacted] hours community service. The court also ordered the employee to pay the government restitution in the amount of [redacted]**

(U) Management Action. **The employee resigned from the Agency in lieu of termination. In view of the criminal conviction, the matter was referred to the Associate Directorate for Security and Counterintelligence for security clearance action.**

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

(U) **Category**. **Other (Time and Attendance)**

(U) Procurement Fraud Initiative**; NSA/CSS IG; Various Control Numbers; 1 April 2008 to 30 September 2008.**

(U//~~FOUO~~) Summary**. In October 2007, we launched an initiative to identify fraudulent billings by NSA/CSS contractors. This initiative involves the interrogation of contractor access data, coordination with company compliance officials, analysis of billing records, and the investigation of access and billing anomalies.**

(U//~~FOUO~~) After twelve months, our initiative has produced significant results. To date, we have identified several hundred potential mischarging matters and completed more than 40 mischarging investigations. These investigations have revealed more than 9,000 hours charged by contractors for fraudulent billings or out-of-scope work. Recoveries for these hours will exceed $1.2 million. In most of the instances where fraud has been substantiatied, the company has terminated the offending employee. Some examples include:

(U//~~FOUO~~) IV-07-0055. **A subcontractor employee fraudulently billed the government 298 hours (approximately $56,000) for non-work activities. The company reimbursed the government the full amount.**

(U//~~FOUO~~) IV-07-0042. **A subcontractor employee fraudulently billed 374 hours (approximately $39,000) for time spent at lunch. The company reimbursed the government for the full amount.**

(U//~~FOUO~~) IV-08-0006. **A contractor employee fraudulently billed 910 hours (approximately $68,000). The employee admitted to billing the government for time spent taking college courses.**

(U//~~FOUO~~) IV-08-0014. **A subcontractor employee admitted to billing 582 hours (approximately $98,000) for contract work performed at home, which was specifically prohibited under the contract terms. The contractor has offered $250,000 to settle all claims for out-of-scope work performed by its employees on that contract.**

(U//~~FOUO~~) IV-08-0043. **A contractor employee fraudulently billed 751 hours (approximately $82,000) for time spent taking care of personal matters during the workday.**

The employee admitted to billing the government for personal matters.

(U) Special Inquiry: Employee Concerns – Yakima Research Station (YRS), WA; **NSA/CSS IG; ST-08-0023; September 2008**

(U//~~FOUO~~) Summary. **A spate of complaints from Yakima Research Stations (YRS) employees concerning work relationships prompted a quick reaction special study by the OIG. The study found that portions of the relatively small YRS workforce had become factionalized harming work relationships and creating discord. The new Chief of Station, YRS, who arrived only weeks prior to the OIG visit, has since restructured the site leadership team. This change appears to have substantially improved the situation. Additional recommendations regarding promotion administration and training for a specific work center were provided to the new Chief of Station.**

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

(U) Category. **Other (Intelligence Support/Standards of Conduct)**

(U) **OIG-Directed Management Inquiry: Hostile Work Environment Allegations – NSA/CSS Texas;** NSA/CSS IG; CO-08-0635; August 2008

(U//~~FOUO~~) **Summary.** The OIG tasked the NSA/CSS Texas command to conduct a management inquiry into actions by a mid-level manager who had been accused by several subordinates of hostile and abusive treatment. The management inquiry substantiated several instances during which the manager used abusive or profane language. The report has been forwarded to the NSA Office of Employee Relations for appropriate action.

(U) **Overall Report Classification.** U//FOUO

(U) **Category.** Other (Intelligence Support/Standards of Conduct)

(U) **Misuse of Government Resources**; NSA/CSS IG; CO-08-0384, CO-08-0403, CO-08-0453, CO-08-0454, CO-08-0455, CO-08-0517, CO-08-0525, CO-08-0526, CO-08-0563, CO-08-0673, CO-08-0674, CO-08-0723, CO-08-0724, CO-08-0771, CO-08-0791, 1 April 2008 to 24 September 2008.

(U//~~FOUO~~) **Summary.** The OIG substantiated 15 allegations of NSA affiliates' misuse of government resources (e.g., accessing adult-oriented material through the Agency's unclassified Internet network).

(U) **Management Action.** Subjects in these cases were civilian employees, military affiliates, and NSA contractor employees. Discipline ranged from a letter of warning to reduction in grade.

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

(U) **Category.** Other (Computer Misuse)

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U//~~FOUO~~) **Advisory Report on Decompartmentation Plans for Counterterrorism Special Programs**; NSA/CSS IG; ST-08-0018; 30 June 2008

(U//~~FOUO~~) Summary. Our advisory report found that the Program Management Office (PMO) was diligent and thorough in assessing the scope and complexity of removing data from the compartmented program while ensuring compliance with laws, regulations, and other mandates. The content, communication, and assignment of supporting plans were adequate to provide reasonable assurance of compliance and successful implementation. Although a solid foundation of planning was in place, supporting plans need fine tuning. We made no formal recommendations;however, management should consider the need for more detailed written plans and firm milestones in the areas of document preservation, reporting, and debriefing. Most importantly, because the Program Management Office has formally disbanded, former PMO members and NSA leadership must rigorously monitor remaining actions to ensure that the decompartmentation is successful.

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

(U) Category. **Joint Warfighting and Readiness**

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

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

~~(S//REL)~~ **Summary. The objectives of this inquiry were to identify authorities for the handling of data in [redacted] and to determine if policies and procedures are in place and followed to ensure compliance with those authorities. We also reviewed system security practices for [redacted] Information Systems. Our special study found that overall the Associate Directorate for Security and Counterintelligence (ADS&CI) [redacted] is compliant with NSA's authorities. [redacted] ADS&CI obtained required approvals for [redacted] certified and accredited by the Technology Directorate. ADS&CI management has minimized risk by limiting access to [redacted] data, reviewing queries of the data, and providing review results to the Office of General Counsel. Although ADS&CI management has established a good control environment, some [redacted] information systems improvements are needed, and the Technology Directorate must improve oversight of [redacted] system security practices.**

(U//~~FOUO~~) Management Action. ADS&CI management concurred with our findings Their planned actions, which will further reduce the risk associated with [redacted] operations, meet the intent of our recommendations.

(U) Overall Report Classifications. **SECRET//REL TO USA, FVEY**

(U) Category. **Joint Warfighting and Readiness**

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