(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) ***For the Period October 1, 2007 Through March 31, 2008***

(U//~~FOUO~~) ; NSA/CSS IG;

(~~S//REL~~) **Summary.** During September and October 2007, the NSA/CSS Office of the Inspector General (OIG) conducted a special inquiry into an allegation that We found no violations of NSA's legal compliance and minimization procedures and issued no formal recommendation, but we observed that additional oversight familiarization training was needed.

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

(U) **Category.** Other (Operational Authorities)

(U) **Contract Warehouse Operations;** NSA/CSS IG; AU-07-0019; 14 November 2007

(~~C//REL~~) **Summary.** In support of the Information Technology Directorate (ITD), the Agency contracts for warehouse space to store more than pieces of information technology equipment and parts valued at These warehouse services cost the Agency about annually. We performed this audit to evaluate the effectiveness and efficiency of the storage facilities contract to satisfy the Agency's requirements and needs. Our audit found that the Contracting Officer Representative must develop and implement a sampling plan to verify the accuracy of the contractor's inventory records. Additionally, the Property Acquisition Support Office must tag all of the ITD's pilferable items destined for the contract warehouse and account for them in the Defense Property Accountability System as required by NSA/CSS *Financial Management Manual 7-2*. Finally, some deliveries are

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

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

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

(U) **Agency's Streaming Media Capability;** NSA/CSS IG; AU-07-0020; 4 December 2007

(U//~~FOUO~~) **Summary.** In April and July 2007, the OIG received similar hotline complaints about organizations duplicating streaming media and web services to the

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

Agency. In a 2006 Inspection Report, OIG found the same problem—Agency organizations use their own personnel or pay contractors to provide multimedia services instead of using the corporate authority (Office of Multimedia Solutions). Although the [redacted] has a legitimate role in providing operational streaming media in support of Signals Intelligence analysts, it has, on limited occasions, duplicated services offered by the Office of Multimedia Solutions. Although this office is responsible for web design and development of organizational and project websites on the NSA intranet as required by NSA/CSS Policy 10-7, other organizations are performing identical services. Duplication occurs because responsibilities of the Office of Multimedia Solutions and other Agency organizations are not clearly defined.

(U) **Management Action.** The Chief of Staff and Technology Directorate concurred with all recommendations and have initiated corrective actions.

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

(U) **Category.** Other (Information Technology) (b)(3)-P.L. 86-36

(U) **Laptop and Other Portable Computing Devices Accountability**; NSA/CSS IG; AU-07-0005; 4 December 2007

(U//~~FOUO~~) **Summary.** Since 2000, the Agency has focused on improving its accounting of portable computing devices (PCDs), such as laptop computers. Nonetheless, as of 29 June 2007 the Agency had not accounted for some [redacted] of the more than [redacted] PCDs in use at NSA over the period 2000-2007. Our audit found that, although improvements had been made in tracking and identifying PCDs at the Agency, the audit trail for PCDs was inefficient and, in some cases, non-existent, especially for the hand-receipt process for Agency-owned and contractor-provided PCDs. Despite adequate accountability procedures for incoming property through Central Receiving, Agency personnel could bypass that process. Consequently, PCDs were brought into the Agency and not properly accounted for in property records. Missing or unaccounted for PCDs were not always reported as soon as they were known to be lost. Meaningful investigations cannot be conducted when missing PCDs, [redacted] are not reported quickly.

(U//~~FOUO~~) **Management Action.** After issuance of the audit report in December 2007, the Director, NSA/CSS tasked the Agency's Senior Leadership Team (SLT) to address the persistent problem of unaccounted-for laptops within the Agency. From December 2007 until February 2008, under the leadership of the Chief of Staff, the Agency conducted an exhaustive search for laptops, significantly reducing the number of unaccounted-for laptops identified in our audit report; developed a new Standard Operating Procedure (SOP) for laptop controls and accountability; approved technical measures to protect data on PCDs and track laptops; and withheld performance bonuses for 2007 for most SLT members until the search had been concluded and the SOP developed.

(U//~~FOUO~~) In February 2008, the SLT directed a number of actions, including

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

the preparation of a written report on these issues. On 7 March 2008, the Deputy Chief of Staff submitted the required report to the SLT. It included a history of the laptop accountability issue at NSA since 2002, results of the recent intensive efforts, and major actions that lie ahead. Attachments to the report included detailed results of the search and the new accountability procedures prepared by the OIG, Office of General Counsel, Directorate of Security, and Directorate of Installations and Logistics.

(U) Overall, the Agency is seriously addressing the issue of laptop accountability and is well on its way to establishing a systemic solution to this challenge, incorporating procedures that could be considered for adoption elsewhere in the Intelligence Community.

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

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

(U) **Category.** Other (Information Technology)

(~~S//REL~~) NSA/CSS IG; (both reports)

(~~S//REL~~) **Summary.** We visited two sites selected on the basis of risk, location, and reported oversight issues. Our reviews assessed site operations, local customer support, and compliance with intelligence oversight requirements and instructions. At each site, we found some discrepancies between policy and the execution of Emergency Destruction Exercises. At one site, support to law enforcement was not fully coordinated.

(U) **Management Action.** management at the sites advised HQ that all employees had participated in Emergency Destruction Exercises after receiving clarification on procedures. Employees at one site have been reminded of the requirements of The other site will have a comprehensive environmental survey performed in 2008, and has confirmed receipt of a secure telephone.

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

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

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

(U) **Inquiry From Congress Concerning Possible USSID SP0018 Violations**; NSA/CSS IG; ST-08-0017; 17 December 2007

(U) **Summary.** In response to a request from the office of U.S. Senator Leahy of Vermont, we reviewed allegations of improper intelligence activities and violations of SIGINT authorities made by a citizen of Vermont, who had been a U.S. Army Reservist deployed to Fort Gordon, Georgia, in October 2001. We were unable to substantiate the allegations since the Reservist had never been assigned to NSA and had not performed an NSA mission while deployed.

(U) **Management Action.** We provided our findings for further action to the

Assistant to The Secretary Of Defense (Intelligence Oversight) and the Inspectors General of the Department of Defense, Department of the Army, and the U.S. Army Intelligence and Security Command.

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

(U) **Category**. Other (Operational Authorities)

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

(U) **Joint Inspection of NSA/CSS Europe;** NSA/CSS IG; AFISRA IG; INSCOM IG, NNWC IG; JT-07-0004; 18 December 2007

(~~C//REL~~) **Summary.** The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency, Naval Network Warfare Command, Intelligence and Security Command, and NSA conducted a joint inspection at Stuttgart [redacted] Germany, in September 2007. For at least two years, NSA/CSS Europe leadership (NCEUR) has focused on [redacted] The SIGINT Director has supported these initiatives and has adopted certain authorities. Under NSA/CSS Policy 1-3 on governance, the NCEUR transformation must be appropriately codified. Each Senior Functional Authority responsible for mission and enabling functions must formally delegate authorities in its management directives and allocate appropriate manpower and financial resources. Inspectors found many in the NCEUR workforce were unaware of or confused about their own and other organizational roles in the ongoing transformation. More effective communication of the NCEUR vision and the Director's intent is a major challenge. Joint inspection activities uncovered several areas where additional management oversight is needed, including safety, logistics, property accountability, training, Intelligence Oversight and cover travel.

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

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

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

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

(~~C//REL~~) **Retention of Domestic Communications Collected Under FISA Surveillances;** NSA/CSS IG; ST-06-0007; 21 December 2007

(~~C//REL~~) **Summary.** While conducting collection operations authorized under the Foreign Intelligence Surveillance Act (FISA) of 1978, as amended, NSA might incidentally collect domestic communications subject to limitations. Our evaluation, conducted from September 2006 through August 2007, showed that: 1) although NSA collection systems and raw traffic databases can be programmed to facilitate compliance with retention procedures, some processing and retention procedures had not been programmed; 2) appropriate training on how data repository systems can improve analyst compliance with retention rules should diminish the unintentional override of these features; and 3) developing an automated dissemination system could lower NSA's risk of noncompliance.

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

Corrective actions are underway on programming and training, and management is devising a plan to lower risks associated with dissemination.

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

(U) **Category.** Other (Operational Authorities)

(U//~~FOUO~~) NSA/CSS IG;

(~~S//REL~~) **Summary.** In FY2008, the OIG reported that . During the review, passage of the Protect America Act changed the overall authority under which surveillance directed at persons reasonably believed to be outside the United States could be conducted. That Act has now expired, but the conclusions of the OIG study are still valid. The OIG recommended changes in training and internal control procedures to avoid future collection incidents.

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

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

(U) **Category.** Other (Operational Authorities)

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

(U) **Inquiry Into Tasking Incidents in** NSA/CSS IG;

(~~S//REL~~) **Summary.** During August and September 2007, the OIG conducted a special inquiry into incidents that took place in limited period, but NSA could not verify whether The OIG recommended changes in internal control procedures to avoid future compromise of

(U) **Management Action.** The SIGINT Directorate concurred with the recommendations and has proposed plans to protect the data.

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

(U) **Category.** Other (Operational Authorities)

(U) **Information Technology Enterprise Management System;** NSA/CSS IG; AU-06-0018; 21 December 2007

(~~S//REL~~) **Summary.** In FY2002, Congress recognized the need for an Information Technology Enterprise Management System (ITEMS) program at NSA. Although the Agency has been slow to implement an Enterprise Management System (EMS) that will monitor the health, status, and security of the Agency's Information Technology (IT) Infrastructure, ITEMS is currently regarded as a key program in the Agency's IT modernization effort. As of 30 June 2007, the estimated cost of the ITEMS program Our audit found that program requirements are not well defined

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

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

because of inadequate stakeholder involvement, a weak governance process, and insufficient senior Agency management sponsorship. Without full funding and adequate staffing, ITEMS may not meet its goal of delivering a centralized EMS capability to NSA. As a result of recent budget cuts [redacted] Further, the program's small government staff creates the risk of inefficient program management and potentially puts too much reliance on contractor support for important program work and decision-making.

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

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

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

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

(U) **Quick Reaction Report** – [redacted] **Closeout**; NSA/CSS IG [redacted]

(~~C//REL~~) **Summary.** On 3 August 2007, the OIG received a complaint that alleged mismanagement of the [redacted] closeout. Our ongoing audit of the [redacted] Closeout disclosed a problem that warrants immediate attention by Agency leadership because valuable resources are being expended [redacted] The complaint specifically questioned [redacted] We found that the [redacted] had not conducted sufficient research to determine the most cost effective method for [redacted] This occurred because the Office was unaware that [redacted]

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

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

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

(U) **Follow-up Audit of the Special Study of Time Synchronization**; NSA/CSS IG; AU-07-0018; 23 January 2008

(~~U//FOUO~~) **Summary.** To accomplish its various missions, NSA must reliably affix accurate time-date stamps and, when available, geolocation information on all collected signals. However, NSA currently has no way to certify the accuracy of time-related information, even to the extent of accurately specifying the order of events. Key Agency organizations agree that synchronized time is crucial to the mission and must be established. To fix this long-standing Agency problem, the Time and Frequency Coordination Authority (TFCA) was established in May 2006. The objective of our audit

was to follow-up on the TFCA's progress to establish and implement an enterprise-wide time synchronization solution. Our follow-up audit found that, although TFCA has the authority, it does not have the organizational structure and resources necessary to direct and implement a time synchronization solution. The TFCA has not developed an acquisition plan, which would define user-timing requirements and include key performance goals, to eliminate the Agency's time synchronization deficiencies. Furthermore, the TFCA has not developed time standards and policies to ensure that consistent timing practices are applied across the Agency in support of the Signals Intelligence mission.

(U) **Management Action.** The Chief of Staff, Chief Technology Officer, and Senior Acquisition Executive agreed to implement corrective actions for the recommendations.

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

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

(U~~//FOUO~~) **Follow-Up Inspection of NSA/CSS Accuracy in Aligning Military Joint Duty Assignments with Billet Specifications**; NSA/CSS; IN-08-0003; 24 January 2008

(U~~//FOUO~~) **Summary.** The inspection, conducted in August 2007, was a follow-up review of an earlier OIG recommendation concerning NSA's compliance with a limited aspect of military joint duty assignment (JDA) regulations. The main areas for improvement cited in the inspection include: 1) establishing uniform expectations of Officer Assignment Managers' roles and responsibilities by setting verification frequency dates and assigning explicit JDA billet authorities; 2) adhering to the NSA Personnel Management Manual, Chapter 201, when reassigning JDA officers; and 3) finalizing the Certification Plan, which has been in draft since 2006.

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

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

(U) **Category.** Human Capital

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

(U) **Advisory Report on TURBULENCE Program Management**; NSA/CSS IG; AU-08-0007; 11 February 2008

(U~~//FOUO~~) **Summary.** A centerpiece for Agency transformation is the development of a series of mission modernization capabilities known as TURBULENCE. TURBULENCE focuses on the development and fielding of an architectural framework to modernize mission capabilities in a distributed, peer-to-peer, real-time environment. When TURBULENCE moved from research to development, it became part of the [redacted] On 9 January 2008, the first increment of [redacted], known as Increment I Passive, was granted approval by the Milestone Decision Authority to proceed to the next phase, system development and demonstration. Our advisory audit reported that the Agency must commit to full and timely TURBULENCE implementation through the [redacted] program. Although concrete steps have been taken to increase program

management rigor, only the initial [redacted] increment has been defined, and funding for a critically-related IT infrastructure project is in question. Program management is also [redacted] to support program operations. As a result of these findings, the OIG will begin a series of reviews for this fiscal year on selected areas of [redacted]

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

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

(U) **Signals Survey and Analysis Division Within the Office of Target Pursuit**; NSA/CSS IG; IN-07-0004; 6 March 2008 (b)(3)-P.L. 86-36

(U//~~FOUO~~) **Summary.** The inspection reviewed the Signals Survey and Analysis (SSA) Division for efficiency, effectiveness, and compliance, and to determine the relationship between SSA and the [redacted] and the functional boundaries between SSA and [redacted] Our inspection found a lack of strategic direction for the SSA workforce. Existing strategic plans do not address the role of signals analysis or SSA specifically. Since the inspection, SSA leadership has drafted a strategic plan that details specific objectives and measurements for the SSA workforce. Although SSA and [redacted] share compatible missions, their organizational separation hampers dialogue and limits operational collaboration. Finally, we found that SSA's relationship with [redacted] is inconsistent and collaboration is limited. While the relationship has improved with the division's renewed focus on the Centers, interaction is still based primarily on personal networks.

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

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

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

(U) **Oversight Review of Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop**; NSA/CSS IG; AU-08-0015; 7 March 2008

(U//~~FOUO~~) **Summary.** The financial statements of the Agency's Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop were audited by a Certified Public Accountant firm (CPA) who issued unqualified opinions. Our oversight review of the CPA audit found that the audit was conducted consistent with Government Auditing Standards. Last year, the CPA audit made four recommendations: (1) require contract auditors to be on-site to observe year-end inventory closeout, (2) require Sodexho to fulfill its contractual obligation to provide an annual audited profit and loss statement to the Restaurant Fund, (3) maintain and track fixed asset records in one database, and (4) require Nonappropriated Fund Instrumentality (NAFI) managers to supervise inventory counts and verify that inventory counting procedures are followed. NAFI management has addressed and corrected each of these recommendations. The CPAs did not identify any management concerns this year.

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

(U) **Category.** Financial Management

(U) **Agency's Transition to Internet Protocol Version 6**; NSA/CSS IG; AU-08-0004; 26 March 2008

(U//~~FOUO~~) **Summary.** The audit objective was to determine the Agency's progress in transitioning to Internet Protocol Version 6 (IPv6) and fulfilling the Information Assurance (IA) requirements established by the DoD and Director of National Intelligence. The Information Assurance Directorate has proven to be a valuable IA resource for the overall transition effort. However, NSA's transition status stands in contrast to the Office of Management and Budget's FY2007 assessment that more than half of the agencies are on track to meet the deadline. Our audit concluded that the Agency's transition to IPv6 has been stalled. The transition plan has not been approved by the Chief Technology Officer, and the Agency lacks a Program Management Office to manage and coordinate the transition to IPv6. We also found that recently acquired Information Technology (IT) devices may not process both IPv6 and its predecessor. By accepting the risk that IT devices may not process both, the Agency could delay implementation and incur increased costs.

(U) **Management Action.** The Technology Directorate (TD) concurred with our recommendations, and the IAD agreed to assist TD with information assurance support on IPv6 transition efforts.

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

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

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

(U) **Vehicle and Driver Services**; NSA/CSS IG; AU-08-0003; 31 March 2008

(U//~~FOUO~~) **Summary.** The audit objective was to determine whether the Agency operates an efficient and effective vehicle program. As of September 2007, the Agency owned [redacted] vehicles and transportation assets. In addition, the Agency leased [redacted] vehicles and assets. Our audit found that, with few exceptions, Commuter and Motorfleet Services does not operate an efficient vehicle program of almost [redacted] vehicles and assets. In FY2007 the Agency spent over [redacted] on vehicles and maintenance. However, more than half of the Agency vehicles reviewed had been used less than 50 percent of DoD's mileage guidelines. The Agency does not have a process for reviewing usage to determine whether or not a vehicle is needed or whether vehicles should be leased or purchased. Consequently, the Agency is leasing transportation assets that would be more cost-effective if purchased.

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

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

(U) **Category.** Other (Logistics Services)

(U) **Procurement Fraud Initiative**; NSA/CSS IG; Various Control Numbers; 1 October 2007 to 31 March 2008

(U//~~FOUO~~) **Summary.** In October 2007, we launched an initiative to identify fraudulent billings by NSA contractors. This initiative involves data interrogation of contractor

access records, coordination with contractor compliance officials, analysis of billing records, and investigation of access and billing anomalies.

(U//~~FOUO~~) After a six-month run, our initiative has produced significant results. To date, we have identified several hundred potential mischarging matters, opened 38 new mischarging investigations, and completed 14 mischarging investigations, in which we substantiated more than 4,400 mischarged hours, amounting to approximately $500,000 in potential recoveries.

(U//~~FOUO~~) We are closely coordinating this initiative with the Defense Criminal Investigative Service, Baltimore, and the Office of the United States Attorney for the District of Maryland.

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U) **Advisory Report on NSA Participation in the Terrorism Watchlisting Process;** NSA/CSS IG; ODNI IG; JT-07-0006; 4 December 2007

(U//~~FOUO~~) **Summary.** In December 2006, the Intelligence Community Inspectors General Forum agreed to coordinate a review of the processes for nominating individuals to the consolidated terrorist watchlist. This advisory report responds to the Forum's Memorandum of Understanding, 19 March 2007 (amended and restated as of 7 May 2007), that required the NSA Office of the Inspector General to participate in a joint review. A team of inspectors from the ODNI and NSA conducted a joint review of NSA's participation in the terrorist watchlist nomination process from March to September 2007. The advisory report highlighted that: 1) no formal process exists for the review of [redacted] 2) no standardized format exists for submitting watchlist nominations; and 3) no Intelligence Community-wide training is available on the watchlist nomination process. These observations were included in the ODNI's inspection report, *Intelligence Community-Wide Review of the Terrorist Watchlist Nomination Process: Findings and Recommendations for Action*, 28 February 2008.

(U) **Management Action.** Management has initiated action in several areas highlighted by the joint IG team.

(U) **Overall Report Classification.** SECRET//NOFORN (b)(3)-P.L. 86-36

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

(U) **Geospatial Exploitation Office**; NSA/CSS IG; IN-06-0005; 22 January 2008

(U//~~FOUO~~) **Summary.** During an OIG organizational inspection, the Geospatial Exploitation Office [redacted] Nevertheless, the recommendations in the final report still apply to the GEO mission. Our inspection found that Signals Intelligence Directorate (SID) leadership concurs with the need to define and disseminate a clear division of effort across the Extended Enterprise. Since the on-site phase of the inspection, SID's Office of Analysis and Production's [redacted] of the GEO mission addressed many problems. However, throughout the inspection, SID was unable or unwilling to exercise any authority over the geospatial exploitation mission conducted in [redacted] GEO training, particularly for [redacted] must be relevant and formalized.

(U) **Management Action.** SID Management concurred with the recommendations. Although SID did not provide final action plans on several recommendations made in the draft report, the IG published the final report, including estimated completion dates, and will address those recommendations during the follow-up phase.

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

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