

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~**(U) SEMIANNUAL REPORT TO THE CONGRESS**

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

(U) For the Period April 1, 2007 Through September 30, 2007**(U) Government Purchase Card Program; NSA/CSS IG; AU-06-0016; 12 April 2007**

~~(U//FOUO)~~ **Summary.** Our audit found that the Agency has successfully implemented a Government Purchase Card program and, for the most part, has effective controls over the [redacted] in annual purchases for FY2006. Unlike many agencies, NSA only issues credit cards to a small percentage of personnel; this limits financial exposure to wrongdoing and inadvertent misuse. Cardholders and certifying officials praised the program coordinators for their helpfulness and responsiveness. Nevertheless, the control environment needs strengthening in certain areas, including enforcement of requirements to get information technology purchases approved.

(U) Management Action. Management concurred with all recommendations to strengthen the control environment.

(U) Overall Report Classifications. SECRET//NOFORN

(U) Category. Acquisition Processes and Contract Management

(U) Oversight Review of Restaurant Fund, Civilian Welfare Fund, and Gift Shop; NSA/CSS IG; AU-07-0014; 15 May 2007

(U) 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 (CPA) firm who issued unqualified opinions. Our oversight review of the CPA audit found no problems in the conduct of the audit by the CPA firm. The two problems reported last year - the need for a new Nonappropriated Fund Instrumentality (NAFI) contract and the need for a high-speed Internet connection - have been addressed. Additional concerns identified in the current year's report are: 1) the restaurant contractor did not submit an annual audited profit and loss statement as required; 2) contracted CPAs were not on-site to observe the year-end closeout inventory; 3) records are not maintained and tracked in one dedicated database; and 4) NAFI management did not observe inventory counts to ensure adherence to prescribed procedures.

(U) Management Action. Management is in the process of implementing the audit recommendations.

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

(U) Category. Financial Management

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

Approved for Release by NSA on 07-01-2019, FOIA Case # 79825 (litigation)

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

(U) Chemical, Biological, Radiological, Nuclear Terrorism; NSA/CSS IG;
IN-06-0002; 24 May 2007

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

~~(S//REL)~~ **Summary.** As "the nexus between terrorism and weapons of mass destruction," the Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism mission is vital to national security. Our functional inspection of CBRN found that the CBRN workforce at NSA/CSS Washington (NSAW) and the Cryptologic Centers (CCs) is very talented and dedicated.

[Redacted]

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

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

(U) Category. Joint Warfighting and Readiness

(U) SIGINT Dissemination for Analytic Collaboration per USSID CR1611(P);
NSA/CSS IG; ST-06-0017; 25 May 2007

(U) Summary. Provisional United States Signals Intelligence Directive (USSID) CR1611, *SIGINT Dissemination for Analytic Collaboration*, implements policy for the dissemination of SIGINT, either as a product or service, or for analytic collaboration. The USSID has been provisional since 2004. Our special study found that it does not institute adequate internal controls and implementation procedures are unclear and inconsistent with NSA dissemination practices. As a result, NSA cannot account accurately for SIGINT disseminated under the USSID and there are inconsistent interpretations of what constitutes appropriate dissemination during collaboration activities. If SIGINT is disseminated before it is minimized for U.S. Person information, violations of Legal Compliance and Minimization Procedures (USSID SP0018) could occur.

(U) Management Action. The Signals Intelligence Directorate (SID) management concurred with the report's finding and recommendations. SID agreed to reissue the USSID, establish a plan to educate the workforce on USSID standards, and establish quality control of SIGINT disseminations during analytic collaboration. These actions will reduce, but not eliminate, the risk.

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

(U) Category. Joint Warfighting and Readiness

~~(U//FOUO)~~ **Mission Operations at the** [Redacted];
NSA/CSS IG; [Redacted]

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ **Summary.** The NSA/CSS OIG conducted this assessment of Mission Operations and Governance at the [Redacted] concurrent with the U.S. Army Intelligence and Security [Redacted]

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

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

Command (INSCOM) inspection of the [redacted]. Overall, the [redacted] is performing at an exceptional level given its limited resources. However, the success of the [redacted] transition and the site's ability to take on additional mission responsibility hinges on clearly defined authorities, responsibilities, and sufficient resources. Our inspection also found that the lack of a clearly defined and documented management structure within [redacted] is causing confusion for the workforce and thereby negatively impacting current operations; reporting deficiencies were noted due to gaps in reporting expertise at the site; and critical programming and manpower actions must be completed in the near term for [redacted] to attain and sustain the [redacted] Center mission requirements as set forth in the concept plan.

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ Management Action. SID Management concurred with all findings; [redacted] management non-concurred with one of the findings; however, the site is already attempting to clarify the leadership roles to the workforce, as recommended.

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

(U) Category. Joint Warfighting and Readiness

(U) Advisory Report on the Research Project on Governance for Agency Programs; NSA/CSS IG; AU-07-0003; 22 June 2007

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

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ Summary. At the request of NSA's Deputy Chief of Staff, the OIG performed this review to determine what acquisition oversight is being performed over the [redacted] in FY 2007 Research, Development, Test & Evaluation funds. We concluded that almost all of the funds received some degree of oversight by the Directorate of Acquisition (DA) and that the Agency improved this oversight by: 1) increasing the number of Program Executive Offices (PEOs) in the new DA organizational structure from [redacted] 2) creating the Tier 1 list of programs (major investment programs that are critical to NSA's transformation and are directly managed by the PEOs); and 3) implementing new acquisition guidance.

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

(U) Category. Acquisition Processes and Contract Management

~~(U//FOUO)~~ Satellite Modernization - [redacted] Program Management; NSA/CSS IG; [redacted]

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ Summary. The Program Management Office (PMO) for Satellite Modernization - [redacted] has demonstrated effective leadership, strong communication with the partners, and innovative, cost-effective solutions to technical issues in managing this critical program, valued at approximately [redacted]. However, our audit found that collaboration with the [redacted] partners is impeded by the conflicting standards and requirements of each participating partner, which the PMO is responsible for resolving. Additionally, based on two of the dollar thresholds specified in Department of Defense Instruction 5000.2, *Operation of the*

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

Defense Acquisition System, as implemented by NSA/CSS Policy 8-1, the SV program

~~(U//FOUO)~~ **Management Action.** The actions taken by the Senior Acquisition Executive meet the intent of the recommendations on the acquisition issues. The Office of the Director of National Intelligence will not include the SV Program on the Major System Acquisition list because it is too far along in the acquisition cycle. NSA's Office of Policy & Records provided an alternate recommendation addressing partnership concerns. Therefore, the OIG is referring this recommendation to the Chief Technology Officer for action.

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

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

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

(U) **FY2007 Report on Compliance with the Federal Information Security Management Act at NSA/CSS;** NSA/CSS IG; AU-07-0009; 31 July 2007

~~(C//REL TO USA, AUS, CAN, GBR, NZL)~~ **Summary.** Our FY2007 report on compliance with the Federal Information Security Management Act at NSA/CSS concluded that the Agency is making steady improvements to the security posture of its systems and networks. However, much more work must be done to

(U) **Management Action.** Management concurred with the recommendations and continues to take corrective action.

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

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

(U) **Mission Alignment and Build Out;** NSA/CSS IG, ST-07-0005; 6 August 2007

~~(U//FOUO)~~ **Summary.** The IG team began its special study of Mission Alignment and Build Out in April 2007. The special study was undertaken, in part, because information gathered from field and HQ inspections pointed to some human resource, mission delegation, and roles, responsibilities, and authorities issues of vital importance to Agency transformation. Shortly after the study was initiated, the Signals Intelligence Directorate (SID) reapportionment discussions were made public. As our review progressed, it became clear the SID reapportionment would significantly affect our results. Although we curtailed the study, we had gathered sufficient data to offer observations

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

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

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

highlighting some systemic governance and manpower issues. We found confusion about and inconsistencies between Enterprise governance policies and directorate-level implementing documents. Disciplined processes, an accurate mechanism to track and maintain data on human resources, and the commitment of leadership would enhance the Mission Alignment and Build Out initiative's ability to meet Transformation goals. While we did not make specific recommendations, we noted areas in need of leadership attention to help ensure a unified Global Enterprise.

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

(U) Category. Joint Warfighting and Readiness

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

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ [redacted]
NSA/CSS IG; AFISRA; NNWC; [redacted]

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ Summary. The IG organizations of the NSA/CSS IG, Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA), and the Naval Network Warfare Command (NNWC) performed the first joint inspection of

[redacted]

(U) Management Action. Management concurred with the findings of the joint inspection team and is taking corrective action.

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

(U) Category. Joint Warfighting and Readiness

(U) SIGINT Voice Processing System; NSA/CSS IG; AU-07-0015; 22 August 2007

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ Summary. [redacted]

[redacted]

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

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

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

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~



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

(U) **Acquisition Management;** NSA/CSS IG; AU-07-0002; 23 August 2007

(~~C~~//REL TO USA, AUS, CAN, GBR, NZL) **Summary.** The Directorate of Acquisition (DA) has a long history of



(U) **Management Action.** Management concurred with all recommendations and has initiated or planned actions in response to the audit findings.

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

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

(U) **Advisory Report on the Followup Research of Activities Associated with Expeditionary SIGINT Deployments to Hostile Areas;** NSA/CSS IG; ST-07-0015; 24 August 2007

(U//~~FOUO~~) **Summary.** This followup research continues the Office of the Inspector General's examination of the processes associated with the deployment of NSA/CSS personnel to hostile areas in the Central Command Area of Responsibility (CENTCOM AOR). A 2006 IG report (*Advisory Report on the Activities Associated with Expeditionary SIGINT Deployments to Hostile Areas*) highlighted the need to standardize processes related to candidate selection, pre-deployment mission training, Information Technology (IT) support and corporate resolution of issues. For the followup, we evaluated data

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

provided by interviews and a web survey with NSA/CSS personnel who deployed to [redacted]

In addition, we interviewed representatives of organizations involved in the deployment process. We found that, overall, major process improvements have been made, particularly administrative processes consolidated by the NSA Deployment and Readiness Center. However, several areas require continued monitoring: mission training; IT investment; P3 performance review, and oversight of time and attendance.

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

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

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

(U) **Menwith Hill Station; AFISRA IG; NNWC IG; INSCOM IG; NSA/CSS IG; Other IG;** JT-07-0003; 13 September 2007

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ **Summary.** The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA), Naval Network Warfare Command (NNWC), Intelligence and Security Command, NSA, and another IG visited Menwith Hill Station (MHS) in June 2007. The joint IG team found that MHS has demonstrated exceptional mission success and outstanding contributions to the SIGINT effort in [redacted]. Higher HQ and MHS leaders have taken remarkable steps since our last joint inspection in 2004 to effectively integrate and synchronize operations and support in a demanding environment. The following recommendations merit management's attention: [redacted]

(U//~~FOUO~~) **Management Action.** Management concurred with the findings of the joint inspection team and is taking corrective action.

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

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

(U) **Status of Agency Study on Information System Security; NSA/CSS IG;** AU-07-0001; 14 September 2007

~~(S)~~ **Summary.** The audit determined whether the Agency had taken steps to implement the [redacted] recommendations for strengthening the Agency's information system security posture. While our initial focus was to identify the status of the [redacted]

[redacted] Our review found that since 2000, numerous Agency studies, reports, and assessments of the [redacted]

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291129~~(b) (1)
(b) (3) - P.L. 86-36

vulnerability of Agency Information Systems have been conducted [REDACTED]

(U//FOUO) **Management Action.** The Information Technology and Information Assurance Directorates agreed to implement corrective action for all of the recommendations.

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

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

(U) **Labor Mischarging; NSA/CSS IG; IV-07-0052; 12 September 2007**

(U//FOUO) **Summary.** The NSA OIG substantiated an allegation that a contract employee mischarged an NSA Time and Materials contract between January 2006 and June 2007. We determined the contract employee mischarged 270 hours, amounting to approximately \$22,000 in false billings. The contractor reimbursed NSA that amount and dismissed the employee. The United States Attorney's Office, District of Maryland, declined prosecution due to the contractor's cooperation and reimbursement to NSA.

(U) **Management Action.** The matter was referred to the ADS&CI for possible security clearance action. The company made restitution in accordance with our findings.

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

(U) **Category.** Other (Contract Fraud)

(U) **Falsification of Crypto-Tape Testing Documents; NSA/CSS IG; IV-07-0036, 30 August 2007**

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

(U//FOUO) **Summary.** The NSA OIG conducted an investigation in response to an allegation that an Agency Cryptologic Fabrication worker forged the initials of two Agency officials responsible for conducting quality control tests on secure communications tapes ("crypto tapes"). According to the complainant, the subject employee forged the two officials' initials on quality control documents, but no quality control testing had been conducted. Our investigation substantiated the allegation. [REDACTED]

[REDACTED] The forged testing records were discovered prior to shipment, and we verified that this lot of tapes received appropriate quality control testing before it was released for distribution. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** The Report of Investigation in this matter was referred to the NSA Associate Directorate for Security and Counterintelligence (ADS & CI) for possible action on the employee's security clearance, and to NSA Employee Relations for administrative discipline.

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

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291129~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~**(U) Category. Other (Falsification)****(U) Falsification of Medical Center Document; NSA/CSS IG; IV-07-0028;**
15 June 2007

~~(U//FOUO)~~ **Summary.** The NSA OIG substantiated an allegation that an NSA employee falsified an official Government document in order to misrepresent her whereabouts to Agency management. The employee admitted she intentionally altered an Agency official's writing on an Occupational Health, Environmental & Safety Services document. The NSA OIG previously substantiated significant time and attendance violations against this particular employee.

(U) Management Action. The NSA OIG Report of Investigation on this matter was referred to the ADS & CI for possible action on the employee's security clearance and to NSA Employee Relations for administrative discipline.

(U) Overall Report Classification. UNCLASSIFIED//FOR OFFICIAL USE ONLY**(U) Category. Other (Falsification)****(U) Travel Voucher Fraud and Misuse of Government Charge Card; NSA/CSS IG;**
IV-07-0007; 30 August 2007

~~(U//FOUO)~~ **Summary.** The NSA OIG conducted an investigation in response to an allegation that an NSA Computer Scientist altered TDY itineraries and charged the Government for post-TDY "Rest and Relaxation" (R&R) trips to Thailand. Our investigation substantiated that the employee altered his official itineraries on four separate occasions to add a total of eight post-TDY R&R trips to Thailand. We determined the Government paid the employee's airfare for seven of these eight R&R trips, and that the employee inappropriately charged airfare for all eight trips to his Government travel charge card. In addition to the cost of the airfare for the Thailand trips, a review of 38 travel vouchers submitted by the employee between 2004 and 2007 determined that the employee was mistakenly reimbursed for other non-reimbursable TDY expenses. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) Management Action. Our Report of Investigation in this matter was referred to the ADS&CI for possible action on the employee's security clearance; to NSA Employee Relations for administrative discipline; and to the NSA Travel Card Program Office for initiation of a restitution action. The Agency has suspended the employee's Government travel charge card.

(U) Overall Report Classification. UNCLASSIFIED//FOR OFFICIAL USE ONLY**(U) Category. Other (Travel Voucher Fraud / Misuse of Resources)****(U) Time & Attendance Fraud, Travel Voucher Fraud, Misuse of Government Charge Card; NSA/CSS IG; IV-06-0057; 31 August 2007**

~~(U//FOUO)~~ **Summary.** The NSA OIG conducted an investigation based upon

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

allegations of voucher fraud against a GG-13 [REDACTED] We substantiated that the employee: 1) intentionally falsified her timesheets, for a total shortfall to the Government of 360.50 hours (approximately \$15, 580); 2) intentionally falsified a Government travel voucher, charging the Government \$1,001.40 for expenses in Hawaii when the trip was essentially a personal vacation; and 3) intentionally misused her Government travel charge card. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** The OIG Report of Investigation was referred to the ADS&CI, for possible security clearance action; to NSA Employee Relations for administrative discipline; and to the NSA Office of Finance for initiation of a restitution action.

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

(U) **Category.** Other (Fraud and Misuse)

(U) **Government Credit Card Misuse;** NSA/CSS IG; IV-07-0035; 17 September 2007

(U//~~FOUO~~) **Summary.** The NSA OIG substantiated an allegation that a former military assignee at NSA (now a contractor assigned to an NSA contract) knowingly misused his Government-issued travel charge card by charging over \$23,000 in personal expenses to the card, including a \$21,700 charge for on-line foreign currency trading, \$1,403.50 for cash advances and \$54.00 for cinema tickets. The former assignee failed to pay a balance of \$14,262.95 on the card prior to leaving Government service. The OIG verified that the former assignee is personally responsible for this debt, and therefore there is no potential pecuniary loss to the Government. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** The NSA OIG's Report of Investigation in this matter was referred to the ADS&CI for possible security clearance action.

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

(U) **Category.** Other (Misuse of Resources)

(U) **Misuse of Agency Software;** NSA/CSS IG; IV-07-0019; 23 July 2007

(U//~~FOUO~~) **Summary.** The NSA OIG substantiated an allegation that a GG-14 employee removed unused, unclassified Government-owned Commercial-Off-the-Shelf (COTS) software from Agency spaces, without authorization, and then installed the software on multiple personally owned computer systems. We also determined that, after installing the COTS software, the employee and/or a family member activated it, rendering it useless to the Agency. Finally, we concluded the employee failed to fully and truthfully respond to management inquiries about the COTS software.

(U) **Management Action.** The Report of Investigation in this matter was referred to the ADS&CI for possible security clearance action, and to NSA Employee Relations for administrative discipline. We also referred the matter to the Agency's Office of Finance for initiation of a restitution action.

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

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

(U) **Category.** Other (Misuse of Resources)

(U) **Misuse of NSA Computer Networks;** NSA/CSS IG; IV-07-0024;
10 September 2007

(b) (6)

(U//~~FOUO~~) **Summary.** The NSA OIG substantiated an allegation that a GG-13 Skills Community Director misused Government resources for private gain. Our investigation determined that the employee used the classified and unclassified computer networks to facilitate [REDACTED]

(U) **Management Action.** The matter was referred to NSA Employee Relations for administrative discipline.

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

(U) **Category.** Other (Misuse of Resources)

(U) **Misuse of NSA Unclassified Computer Network;** NSA/CSS IG; Various Control Numbers; 1 April 2007 to 30 September 2007

(U) **Summary.** During the past six months, the NSA OIG substantiated a total of 33 allegations that NSA affiliates misused Government resources by accessing adult-oriented material on the Agency's unclassified computer network. The 33 cases break down as follows: 18 contractor matters, 8 military assignee matters and 7 civilian matters.

(U) **Management Action.** Consequences for contractor employees ranged from company reprimand to dismissal from employment. Military assignee cases were referred to the appropriate service for military discipline. Civilian cases were referred to NSA Employee Relations for administrative discipline. All matters were referred to ADS&CI for possible security clearance action.

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

(U) **Category.** Other (Misuse of Resources)

(U) **Child Pornography;** NSA/CSS IG; CO-07-0279; 5 March 2007

(U//~~FOUO~~) **Summary.** The NSA OIG supported an FBI investigation into an NSA/CSS GG-15 civilian employee [REDACTED]. The FBI's investigation was part of Project Safe Childhood, a nationwide initiative designed to protect children from online exploitation and abuse. An FBI search of the civilian's Maryland residence and analysis of his home computer revealed that he used his home computer to receive more than [REDACTED] images of child pornography from the Internet. On [REDACTED] he was sentenced in Federal court to [REDACTED] years in prison followed by [REDACTED] years of supervised release for receipt of child pornography. He was also ordered to register as a sex offender.

(U) **Management Action.** The employee is no longer employed at the Agency and does not hold a security clearance.

(b) (6)

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

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

(U) **Category.** Other (Child Pornography)

(U) **Misrepresentation of Academic Credentials; NSA/CSS IG; IV-07-0003**
(8 August 2007); IV-07-0009 (30 April 2007); IV-07-0025 (8 August 2007)

(U) **Summary.** A Federal law enforcement Agency provided the NSA OIG with a list of individuals who obtained bogus degrees from diploma mills. Through a data interrogation process, we were able to determine that the list contained the names of three NSA civilian employees. We determined that each employee paid a fee for a bogus degree and represented that degree to the Agency as legitimate. We also determined that the employees provided the Agency with academic transcripts setting forth courses they did not actually take and grades they did not actually receive. In each case, we concluded the employees either knew or reasonably should have known their degrees were illegitimate, and that they intentionally misrepresented their credentials and qualifications to the NSA.

(U) **Management Action.** The OIG's Reports of Investigation were referred to the ADS&CI for possible security clearance action; to NSA Employee Relations for administrative discipline; and to NSA Human Resources for any necessary grade and pay adjustments.

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

(U) **Category.** Other (Misrepresentation)

(U) **Hostile Work Environment; NSA/CSS IG; IV-07-0027; 6 June 2007**

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that a GG-15 manager at an Agency field site created a hostile work environment for one of the military assignees. Our investigation determined that the GG-15's performance frustrations with the military assignee caused him to make statements and gestures toward the military member that were abusive in nature. We concluded that the GG-15 violated applicable NSA Policy by using intimidating language and gestures, and failing to exercise courtesy and respect in dealing with a coworker.

(U) **Management Action.** The OIG Report of Investigation in this matter was referred to NSA Employee Relations for administrative discipline.

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

(U) **Category.** Other (Hostile Work Environment)

(U) **Time and Attendance Fraud; NSA/CSS IG; IV-07-0011; 05 May 2007**

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that, between 1 February 2006 and 19 January 2007, a GG-13 Facilities Project Manager intentionally submitted false and inaccurate timesheets, for a total shortfall to the Government of 646 hours (approximately \$28,824). The employee asserted that he regularly conducted NSA business from inside his car in the NSA parking lot (outside the NSA CONFIRM

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

(b) (6)

system), because [redacted] Our investigation determined this explanation was implausible. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** The OIG Report of Investigation was referred to the ADS&CI for possible security clearance action; to NSA Employee Relations for administrative discipline; and to the NSA Office of Finance for initiation of a restitution action.

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

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

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

(U//FOUO) **Financial Accountability** [redacted] NSA/CSS IG;
[redacted]

(C//REL TO USA, AUS, CAN, GBR, NZL) **Summary** [redacted]

[redacted]

(U) **Management Action.** Responsible contractor made restitution in accordance with OIG findings.

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

(U) **Category.** Other (Financial Accountability)

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

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

**(U) NSA/CSS OIG ACTIVITIES RELATED TO
COUNTERTERRORISM**

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

(U) Inspection of the Geospatial Exploitation Office; NSA/CSS IG; IN-06-0005

~~(C//REL TO USA, FVEY)~~ **Background.** The Geospatial Exploitation Office (GEO) began operations [REDACTED]

[REDACTED] The primary objectives of the inspection were to assess GEO's mission effectiveness, GEO's ability to satisfy requirements and information needs levied on the organization, and GEO mission management. Prior to publication of the draft report, the SIGINT Directorate's Deputy Director for Analysis and Production realigned the S2 organization. The realignment resulted in [REDACTED]

[REDACTED] Several findings and recommendations were identified in the draft inspection report that apply to the GEO mission as a whole and not the GEO organization in particular. Depending on the outcome of the draft report review process, these mission topics may need to be addressed at the SID level.

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

(U) Special Studies of Counterterrorism Programs; NSA/CSS IG

~~(U//FOUO)~~ **Background.** In January 2007, all Counterterrorism programs previously operated under Presidential authority began operating under the authority of Foreign Intelligence Surveillance Court orders. For these new orders, the OIG performed reviews in accordance with their terms, which specified that an initial review would be done to ensure that minimization procedures were adequate. The FISC orders imposed strict time limits, but when possible, these reviews included testing. The OIG completed two such reviews in the past six months. In addition, we published a report on a special inquiry performed to answer concerns raised about activities under one of the FISC orders.

**(U) Assistance to ODNI IG for the Terrorist Watchlist Project; NSA/CSS IG;
JT-07-0006**

(U) Background. The Terrorist Screening Center (TSC) maintains a consolidated terrorism watchlist that is populated by information from the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI). Agencies that possess or acquire terrorism and counterterrorism information, with the exception of purely domestic counterterrorism information, are required by Executive Order 13354 to promptly give access to such information to the NCTC. The NCTC provides a subset of that information to the TSC for inclusion on the consolidated watchlist. The Intelligence Community Inspectors General (ICIG) Forum agreed to coordinate a review of the processes for nominating individuals to the consolidated terrorist watchlist. The Offices of the Inspector General of the Office of the Director for National Intelligence (ODNI), Central Intelligence Agency (CIA), Department of Justice (DOJ), Defense Intelligence Agency (DIA), National

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), Department of State (State), Department of Homeland Security (DHS), Department of Energy, and Department of Treasury (Treasury) are participating in the joint review. While other IC agencies performed internal reviews within their respective agencies, ODNI and NSA inspectors jointly reviewed NSA's participation in the watchlisting nomination process. The joint inspection team focused on the provision of terrorist-related SIGINT information to the NCTC for the purpose of watchlisting. Cross-community findings and observations from the individual agency reports will be incorporated in the overall IC IG report.

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~