U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED

Robert C. Tapella
Public Printer

December 2, 2010

The Honorable Charles E. Schumer
Chairman
Joint Committee on Printing
318 Russell Senate Office Building
Washington, DC 20510

Dear Mr. Chairman:

In accordance with 44 U.S.C. 3903 and the relevant provisions of the Inspector General Act of 1978, as amended, I am transmitting to Congress the Semiannual Report of the Office of the Inspector General (OIG) for the U.S. Government Printing Office (GPO), covering the 6-month period of April 1 through September 30, 2010, along with the following information as required by law. This letter meets my statutory obligation to provide comments on the OIG's report and highlights management actions taken on the OIG's recommendations, which may relate to more than one reporting period.

General Comments

As provided for by law, this section offers my general comments on the OIG's semiannual report and operations.

I. **Management Challenges**. In my view, the organizational and technological transformation that GPO began implementing in 2003 remains critical to the future of GPO. To carry out that transformation successfully, in this and previous reports the OIG has identified several challenges facing GPO's management that we are at various stages of addressing.

1. *Human Capital Operations and Management:* Human Capital (HC) operations and management continue to be top priorities at GPO. During the past year, HC at GPO has undergone major changes in an effort to streamline, improve, and build in accountability and quality control. In addition to the reorganization of the department, we have tackled major changes to Federal hiring as mandated by the Office of Personnel Management (OPM). We have successfully complied with the elements of the hiring reform that apply to GPO, including use of category rating, allowing resume and cover letter only as an initial application, and we have trained all of our supervisors and managers.

732 North Capitol Street, NW Washington, DC 20401 202-512-1000 rtapella@gpo.gov

We continue to automate our processes in order to improve timeliness, reduce errors, and improve our quality control processes. These initiatives are designed to better support GPO's mission and to improve our customers' experience. We are currently beginning the implementation of manager self-service, a key EmpowHR module that will move GPO away from paper SF-52s to an all-electronic system of HC processing. We believe that these improvements to the hiring process are a crucial step in overall improvement to HC management at GPO.

Additionally, we are continuing planning at the strategic level. We started this year with a comprehensive workforce analysis followed by a series of presentations and one-on-one meetings with business unit leadership on workforce planning. We have established new HC consultant positions that provide direct support to GPO managers to plan for upcoming recruitment, and both our policy office and GPO University are working together to issue an updated position management directive and in-depth position management training course as a new addition to the already robust supervisor series. These efforts will also improve overall HC management at GPO.

GPO's Chief Operating Officer, acting Chief of Staff and the acting Chief Management Officer meet weekly with the Chief HC Officer and staff to review key HC activities. HC issues are also regularly discussed at the weekly meeting of all GPO senior leaders. Senior managers have effectively used the recently revised performance management system to achieve significant results across GPO.

We continue to be dedicated to continuous improvement. To that end, building on the FY10 performance metrics, and looking forward to FY11, all HC employees and managers will have specific measures of accuracy and timeliness as well as customer service as part of their performance plans. We are committed to furthering GPO's goals through strategic HC management, building on the success and leveraging the talent of our organization as well as critically evaluating and fixing areas in need of improvement.

2. *Information Technology Management and Security:*

    a. *Compliance with the Federal Information Management Security Act (FISMA):* GPO continues to make progress and improve controls related to FISMA requirements. A total of 14 open OIG recommendations pertaining to FISMA were closed

in the reporting period and GPO is tracking potential changes to FISMA that may occur based on draft legislative proposals that have been made recently to ensure technology and budget request plans and other resources are aligned with any changes that may be enacted.

b. *Implementation of the Federal Digital System:* In the April 2010 FDsys program review, management indicated that the sunset of *GPO Acc*ess would take place in a phased manner, starting with the final development release of FDsys. The actual sunset activities for *GPO Access* will take 3 months, completing the technical activities in late December 2010. From a technical perspective FDsys was ready to be considered the system of record on September 30, 2010. However, there were and continue to be non-technical factors that GPO leadership is considering prior to the sunset of *GPO Access*. These mainly consist of communication activities to the end users of the system and assisting them in the transition that will likely extend into January. A detailed plan is being developed for these critical activities.

GPO has instituted a rigorous change management and configuration process for information technology projects to help ensure that issues are being resolved and that we have a documented baseline of the code used in production. Issues identified through Program Tracking Reports (PTRs) are reported and corrected based on the severity of the issue. The Change Control Board (CCB) assesses the severity of issues and designates them as such. This level of severity determines the priority. Historically, GPO has found that new collections being introduced into the system result in a large number of PTRs. This seems to be largely a result of inconsistencies in the legacy data set. GPO uses very high quality standards for data migration, which has been a contributor to the PTR count since any issue found during the migrations process was logged as a PTR.

Management concurs that testing is an area that needs additional attention. Over the past three years GPO has made great strides in improving test and configuration management areas, with the formation of the IT Quality organization. Additionally, GPO has recognized that system performance modeling and testing are a gap and have made good progress in

closing this gap. In the past 6 months, in anticipation of enabling GPO's Continuity of Access (COA) instance, IT has conducted performance testing on the COA instance as well as the production instance. Both of these instances performed well under this stress testing and revealed areas in the design and configuration where some changes will benefit the overall system performance. One of these areas is in the application server section of the system. This has been a known issue, and validated by the solution provider, Oracle. As such, IT is now upgrading to a new Oracle application server (WebLogics). GPO held off on this upgrade until Oracle was comfortable that WebLogics was ready to support FDsys.

Additionally, during enhanced testing of system performance, GPO uncovered areas outside of FDsys that required some enhancements. For example, with FDsys having a public-facing component at the legislative branch alternate computer facility (the first public facing system to be operated at the ACF), IT learned of a need to improve GPO's network configuration at the ACF. These enhancements have been made and the bandwidth leading to the ACF is being increased to mirror the performance of the service coming to the GPO main facility.

3. *Security and Intelligent Documents:* As the Federal Government's leading provider of secure credentials and identity documents, Security and Intelligent Documents (SID) is a business unit that exemplifies GPO's transformation to high-technology production. During the OIG's reporting period, SID reported the successful manufacture of more than 7.7 million electronic passports for the State Department. The Washington DC facility produced over 5.4 million passports while the Secure Production Facility (SPF) at the Stennis Space Center, MS, produced more than 2.3 million passports. During FY10, total passport production volume was 13,275,300.

   SID operates the Washington, DC-based Secure Credential Center (SCC) to support the Department of Homeland Security's Customs and Border Protection (DHS/CBP) Trusted Traveler Program (TTP), as well as other Federal secure ID card requirements. The SCC produced 199,477 Trusted Traveler cards during FY10, as well as the Department of Health and Human Services Center for Medicare and Medicaid Service's identification cards to citizens of Puerto Rico.

In a significant accomplishment during the reporting period, SID completed the certification process for the SCC to become a General Services Administration-certified and fully qualified secure card graphical personalization facility. The SCC is now officially certified to handle, graphically personalize, and distribute HSPD-12 PIV cards. The audits for this certification were completed in May 2010; the GSA completed their assessment and certified GPO in November. This certification allows the GPO's SCC to more comprehensively serve Federal agency requirements for HSPD-12 cards and other secure credentials.

During the reporting period, SID initiated new secure credential programs in support of other Federal agencies, including the State Department's Office of Foreign Missions and the Department of Homeland Security. Additionally, the secure credential product line of leather-bound secure flash badges for Federal law enforcement officers and Inspectors General is growing. SID now supplies more than 30 Federal agencies with their leather bound badges.

SID continued to conduct 5S Audits at both plant locations. 5S is a series of defined steps and audits that are intended to improve efficiencies in manufacturing process flows, equipment usage and placement, and environmental housekeeping standards.

A major milestone was accomplished in July 2010 when the Stennis secure facility and SID personnel successfully completed the required audits and earned their ISO9001 certification. This globally-recognized certification for world class production, quality, and process improvement methodologies is a substantial and well-respected qualification. During the reporting period, the Washington DC secure facilities and SID personnel underwent the rigorous ISO9001 audits. In November 2010, SID was informed that they had received a strong positive recommendation from the auditors to award ISO9001 certification to the Washington DC secure operations (passport production, secure card operations, and new product development) as well. Formal certification was received in late November.

Additionally during the reporting period, SID completed the formal training of its entire workforce at both facilities in the subjects and concepts that are foundations of OHSAS (Occupational Health and Safety Systems) 18001. The OHSAS 18001 standards promote

industry best-practices for occupational health and safety standards and programs in a production environment.

SID is also working to develop the capability to manufacture secure blank card bodies through the procurement of card lamination and punch equipment and technologies that will result in more secure and controlled card production as well as lower costs and better service to our agency customers. Card lamination and punch equipment was delivered to SID in September 2010 and the process of installation, standard operating procedure development, and operator training is underway. SID capability to manufacture secure blank card bodies is expected to be operational in FY11.

SID is working closely with Plant Operations to establish a Secure Credential Testing Laboratory to conduct regular performance, durability, and quality tests of passports and credential products. The lab will eliminate costly third party commercial test laboratory expenses for these required product evaluations and provide an environment of greater governmental control and security for these activities. The secure facilities are presently under construction, equipment is on order, and personnel are being trained to support this crucial secure product testing environment. The Secure Credential Testing Laboratory is expected to be operational in FY11.

GPO, in cooperation with the State Department's Bureau of Consular Affairs, issued a Request for Proposal in June 2010 for the procurement of eCovers used in the manufacturing of passports. The proposed eCovers will be compatible with existing GPO manufacturing and DOS passport personalization processes, and will be required to meet various external requirements and standards, including those of the International Civil Aviation Organization (ICAO) and the ISO.

4. *Internal Controls:* Management concurred with KPMG's FY09 financial statement audit findings and continues to recognize the importance of internal control over financial reporting. Specific monthly measures have been implemented to properly record and review property, plant and equipment records, and new Oracle-based reports are near completion which will enable a more timely and accurate reconciliation of both accounts payable and GPO's deposit accounts. Supervisory review procedures are now in effect to help reduce the risk of any further cash flow statement misclassifications.

During the reporting period, SID and associated organizations implemented actions to address the recommendations of the OIG's review of GPO's e-passport supply chain security.

GPO's Oracle financial system (GBIS) went live in May 2009. At that time, GPO decided to standardize its reporting environment using the business intelligence tool Business Objects. Since that time, approximately 118 reports have been developed to bring visibility to all aspects of the data stored in GBIS. These reports, readily available in public folders, are being used to ensure a consistent look at the financial data and provide the ability to evaluate and address deficiencies.

During the past year, GPO has added processes to address IT general and application controls. Security access controls have been addressed by examining all roles and responsibilities and bringing them under configuration management oversight. Assignmen*t of personnel to roles has been put under the control of IT Security and officers within Financial Management. Developers' access to the Production instance of GBIS has been removed. All new development, modifications, and testing are being controlled by the GPO Configuration Management section. To address contingency planning, a secure VPN has been established at GPO's COOP site with the hosted Oracle On Demand environment in Austin, TX.

5. *Protection of Sensitive Information:* As recommended in a February 2009 Management Implication Report, a senior manager was appointed as Privacy Officer (PO). Subsequently, GPO hired a Privacy Program Manager (PPM) to implement rules of conduct and appropriate administrative, technical, and physical safeguards to ensure personally identifiable information (PII) is identified and protected within all GPO business units and with GPO contractors as well. The PPM structured a Privacy Incident Response Team (PIRT) and incident reporting process to investigate and respond to incidents containing PII. These actions were completed by the end of FY 2010.

   GPO's Privacy Program fosters transparency and individual participation regarding how GPO uses PII responsibly to fulfill its mission. Working with GPO's business units, the PPM is targeting for completion, by the end of calendar year 2010, privacy threshold analyses (PTAs), which will provide an overview of PII collection and retention practices, as well as behaviors in handling of PII. The PPM is currently working with GPO business units to implement behavior

changes and privacy protections to ensure that the collection and use of PII is limited to the scope of the authorized activities, and that PII functions integrate all relevant privacy protections. The PPM is implementing Privacy Impact Assessments (PIAs) and, if required, System of Records Notices (SORNs) that embody the collaborative efforts of program management, technical, legal, and appropriate IT security safeguards to reduce and/or remove PII usage to minimum required levels. The completion of the compliance documentation is critical and requires analysis, recommendations, and approvals. These activities are to be completed by all business units by middle of the third quarter of FY 2011.

In addition, the PPM is working with GPO Employee Communications Office on developing a full communication strategy and with GPO University to develop a training curriculum for all GPO employees and contractors on their responsibilities for protecting PII and complying with established guidelines. These steps are to be completed by the end of FY 2011. The PPM also submitted a request GPO's IT services to provide an evaluation of a privacy online incident reporting website to be completed by the second quarter of FY 2011.

GPO's IT area provides technical support and analysis to the PII protection effort, including input on GPO's PII directive and technical assessments, (using software tools, of all GPO network attached storage systems for unprotected PII. IT plans to continue the periodic assessments of GPO IT systems to detect unprotected PII data going forward, in accordance with GPO policies and procedures.

6. *Acquisitions and Print Procurement:* The acquisition function assessment report is still ongoing in Acquisitions. We have contracted with the Procurement Strategy Board to assist us with the assessment. The goal was to have the assessment completed by the end of the reporting period, however, while developing the assessment procedures more time was required to fully develop. The assessment objectives are being finalized and should be launched and completed by second quarter FY 2011. In addition, the issue of contract file information required by the Materials Management Acquisition Regulation (MMAR) was addressed in the responses to the e-Passport audit and we continue to place emphasis on effective contract administration of all contracts. Finally, GPO's financial area is reviewing the provisions of the Improper Payments Elimination Improvement Act as signed into law on July 22, 2010, to determined actions to be taken by GPO.

7. *Financial Management and Performance:* GPO's GBIS Oracle financial system went live in May 2009. At that time, GPO decided to standardize its reporting environment using the business intelligence tool Business Objects. Since that time, approximately 118 reports have been developed to bring visibility to all aspects of the data stored in GBIS. These reports, readily available in public folders, are being used to ensure a consistent look at the financial data and provide the ability to evaluate and address deficiencies. Deficiencies with the design and/or operations of GPO's IT general and application controls were noted in security management, access controls, configuration management, and contingency planning.

8. *Continuity of Operations:* In September 2010, GPO's Business Continuity Office completed a COOP multi-year strategic plan outlining the agency's goals and objectives to ensure complete support of its mission essential functions. The three main goals of the plan are to establish all-hazards mobile capabilities, complete business unit COOP plans, and establish, update and implement COOP policies and directives. The plan was presented to and approved by the GPO operating committee. It was then presented to staff of the Committee on House Administration. The COOP multi-year strategic plan serves as a roadmap for COOP planning, tests, training, and exercises. The following represent significant COOP capability improvements and exercises during FY 2010:

   In another development, GPO assembled House and Senate fly-away kits to support the Enrolled Bill process. The kits are to support enrolled and engrossed printing at an alternate chamber and are composed of cases, printers, paper, cables, and other supplies. There is a kit for Senate and a kit for the House; each kit consists of three cases. The kits can be used at ad hoc COOP sites as needed.

   GPO is also completing Continuity of Access (COA) activities to ensure uninterrupted public access to gpo.gov and FDsys.

   During the reporting period, GPO conducted two successful exercises. The July 2010 House alternate chamber exercise completed all objectives to test notification systems for key staff, demonstrate onsite printing of enrolled/engrossed bills, validate fly-away kit contents, manuscript scanning conducted with file transfer via air card, simulate high-volume delivery of product to alternate site, simulate manuscript pick up from the alternate site, and receive electronic transfer of introduced Bill via FTP at the ACF. The October 2010 congressional

products exercise tested composition (across 3 shifts) for the *Congressional Record*, committee report with graphics, bills, and calendar. It also tested OCR scanning, public access posting to FDsys, printing procurement using GPO contracts, and file Transfer to the LOC and commercial vendors.

9. *Strategic Vision and Customer Service*: Business units across GPO continue to align to changing customer requirements in support of new technologies and transparency initiatives throughout the Government. E-book publishing services in the Publications and Information Sales unit, new security card products in the Security and Intelligent Documents unit, and continuously expanded digital content offered on the FDsys platform are some of many examples. In keeping with elements of the May 2010 draft update to the *Strategic Vision*, GPO is making significant strides to improve a customer service and new business development culture. In Print Procurement, a simplified SF-1 form was introduced along with a system to automatically notify customers of order receipt via email. Simplified and automated workflows have dramatically reduced errors and process time as well. Newly-0appointed directors of sales and marketing have gained traction in the new Agency Accounts and Marketing business unit, as evidenced by over $16 million of new business generated over the past 12 months by the National Account Manager team. During this time the marketing team organized and held over 50 presentations throughout the United States to introduce GPO services to Federal agency customers.

10. *Sustainable Environmental Stewardship:* GPO's goal of environmental sustainability and stewardship is a continuous improvement initiative throughout the agency. GPO's Environmental Advisory Committee is continually evaluating and identifying creative ways to improve sustainability efforts in recycling, procurement, and energy efficiency that ultimately reduce GHG emissions. In calendar year 2009, the most recent period for which complete figures are available, GPO's waste reduction activities successfully diverted 4,702 tons of waste from the landfill, representing recyclables directed to recycling, reuse, and compost facilities.

    Internally, GPO's office recycling programs collect mixed paper, cans, and bottles for recycling, and all paper, chemical, and metal waste from operations is evaluated and recycled if possible. In 2009, GPO redirected 87.5% of the waste steam to non-landfill uses. In conjunction with the Architect of the Capitol, GPO began feasibility

and cost studies for composting cafeteria waste and use of compostable containers and utensils. GPO is testing and evaluating a comprehensive group of office and off-set paper options with higher recycled content, more sustainable manufacturing processes, and lower chemical environmental impact to offer to its customers. GPO's roof replacement project, which was completed in spring 2010, contracted for approximately 100,000 square feet of Energy Star-rated and bio-based products. The contract also required recycling of old materials removed from the roof when possible.

GPO continues to recognize economies of scale in purchasing and working with legislative branch partners. GPO's Environmental Services is developing chemical inventory systems and working with Acquisitions to review waste hauling contracts to benefits to the Agency. GPO is also improving infrastructure performance by retrofitting the steam system to improve efficiency and prioritize projects identified in a 2008 PEPCO Energy Survey Report to reduce energy consumption and improve equipment and infrastructure to reduce energy costs. GPO will continue working on environmental stewardship and energy efficiency projects to improve the results.

II. **Audits and Inspections**. During the reporting period, the OIG issued 3 new audit and assessment reports, with recommendations to help improve operational performance:

- *Federal Digital System (FDsys) Independent Verification and Validation – Eleventh Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 10-07, June 18, 2010).* This assessment continued the ongoing independent verification and validation (IV&V) evaluation associated with the development of FDsys. The evaluation provides quarterly observations and recommendations on the FDsys program's technical, schedule, and cost risks, as well as related issues. This IV&V did not identify any new technical, cost, or schedule risks. The report discusses issues and concerns addressed in previous quarterly reports.

- *Federal Digital System (FDsys) Independent Verification and Validation – Twelfth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 10-08, September 16, 2010).* This evaluation also did not identify any new technical, cost, or schedule risks, and did not include any new recommendations. However, the evaluation discusses a number of issues worth noting as GPO implements the remaining efforts to complete Release 1 of FDsys.

- *WebTrust Assessment of GPO's Public Key Infrastructure Certification Authority – Attestation Report (Assessment Report 10-09, September 2010).* This was an annual compliance review of GPO's Public Key Infrastructure Certification Authority. The assessment resulted in an attestation report expressing its unqualified opinion that management's assertion related to the adequacy and effectiveness of controls over its certification authority operations was, in all material respects, fairly stated based on the American Institute of Certified Public Accountants WebTrust for Certification Authority Criteria.

In addition, the OIG serves as the Contracting Officer's Technical Representative for the audit of GPO's FY 2010 financial statements, which was begun by KPMG during the reporting period. Title 44, U.S.C., requires that GPO obtain an annual audit of its financial statements. The audit of GPO's FY 2009 financial statements was conducted by KPMG. KPMG issued an unqualified opinion on the statements, asserting that they were fairly presented, in all material respects, and in conformity with generally accepted accounting principles. KPMG identified 2 significant deficiencies: financial reporting controls and information technology general and application controls. As the OIG;s Semiannual Report for the period October 1, 2009, through March 31, 2010, noted, KPMG made recommendations for each condition; management concurred with those recommendations and has either planned or initiated responsive corrective action.

Prior Period Outstanding Recommendations. As required by law, this section summarizes management's actions to address OIG recommendations still outstanding from previous reporting periods:

- *GPO Network Vulnerability Assessment (Assessment Report 06-02, March 28, 2006).* One recommendation made in this report remains open.

- *Assessment of GPO's Transition Planning for Internet Protocol Version 6 (IPv6) (Assessment Report 08-12, September 30, 2008).* One recommendation remains open pending completion of GPO's ongoing infrastructure refresh.

- *Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Fourth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 09-01, November 4, 2008).* Two recommendations remain open.

- *Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Fifth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 09-03, December 24, 2008).* Three recommendations remain open.

- *Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Sixth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 09-07, March 20, 2009).* Three recommendations remain open.

- *Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Seventh Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 09-12, September 30, 2009).* At the end of the reporting period, 17 recommendations remain open.

- *Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Ninth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 10-01, December 2, 2009).* Four recommendations remain open.

- *GPO's Compliance with the Federal Information Security Management Act (Assessment Report 10-03, January 12, 2010).* As the OIG report states, management continues to work with the OIG to implement corrective actions on the remaining 14 open recommendations.

- *Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Tenth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 10-05, March 24, 2010).* Three recommendations remain open.

III. Investigations. During the reporting period, the OIG performed investigative work on procurement fraud, workers' compensation fraud, employee misconduct, and other matters including theft, illegal hacking, or other matters, as detailed in the OIG's report. In some cases this work resulted in evaluation for possible civil or criminal action by the Justice Department, and in others in proposals for GPO internal corrective action. These activities demonstrated the value of OIG investigators in protecting GPO from waste, fraud, and abuse.

IV. Statistical Tables.

Statistical tables as required by law are enclosed.

If you need additional information with respect to this report, please do not hesitate to contact Mr. Andrew M. Sherman, Director of Congressional Relations, on 202-512-1991, or by e-mail at asherman@gpo.gov.

Sincerely,

ROBERT C. TAPELLA
Public Printer

Enclosures

cc: The Honorable Robert Brady, Vice Chairman
The Honorable Dan Lungren, Ranking Minority Member
The Honorable Patty Murray
The Honorable Tom Udall
The Honorable Robert Bennett
The Honorable Saxby Chambliss
The Honorable Michael Capuano
The Honorable Susan A. Davis
The Honorable Kevin McCarthy

ENCLOSURE I

STATISTICAL TABLE FOR SECTION 5(b)(2) – DISALLOWED COSTS

		Number of Audit Reports	Disallowed Costs Questioned	Disallowed Costs Unsupported
A.	Audit reports for which final action[1] had not been taken by the commencement of the reporting period	0	0	0
	Audit reports issued during the period with potential disallowed costs	0	0	0
	Total Costs	0	0	0
B.	Audit reports on which management decisions[2] were made during the reporting period			
	(i.) Dollar value of disallowed costs	0	0	0
	(ii.) Dollar value of allowed costs	0	0	0
C.	Audit reports for which final action was taken during the period, including:			
	(i.) Dollar value of disallowed costs that were recovered by management through offsets against other contractor invoices or nonpayment	0	0	0
	(ii.) Dollar value of disallowed costs that were written off by management	0	0	0
D.	Audit reports for which no final action has been taken by the end of the reporting period	0	0	0

[1] As defined by law, the term "final action" means the completion of all actions that the management of an establishment has concluded, in its management decision, are necessary with respect to the findings and recommendations included in an audit report, and in the event that the management concludes no action is necessary, final action occurs when a management decision has been made.

[2] As defined by law, the term "management decision" means the evaluation by management of the findings and recommendations included in an audit report and the issuance of a final decision by management concerning its response to such findings and recommendations, including actions concluded to be necessary.

ENCLOSURE II

STATISTICAL TABLE FOR SECTION 5(b)(3) – FUNDS PUT TO BETTER USE AGREED TO IN A MANAGEMENT DECISION

		Number of Audit Reports	Dollar Value of Recommendations
A.	Audit reports for which final action[3] had not been taken by the commencement of the reporting period	0	0
	Audit reports for which final action had not been taken for new reports issued during the reporting period with potential funds put to better use	0	0
B.	Audit reports on which management decisions[4] were made during the reporting period	0	0
C.	Audit reports for which final action was taken during the reporting, including:		
	(i.) Dollar value of recommendations that were actually completed	0	0
	(ii.) Dollar value of recommendations that management has subsequently concluded should not or could not be implemented or completed	0	0
D.	Audit reports for which no final action has been taken by the end of the reporting period	0	0

[3] Same definition as in Enclosure I.
[4] Same definition as in Enclosure I.