U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED

Robert C. Tapella
Public Printer

June 7, 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 October 1, 2009, through March 31, 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:* Management concurs that Human Capital operations and management is and should be a top challenge not only in GPO but across the Federal Government.

   The process for hiring, as the Director of the Office of Personnel Management has often noted, is in serious need of improvement and the volume and complexity of required data elements for each Federal employee is excessive by any standard. The fact that the document that describes in very brief detail the form and format of all required data elements (*The Guide to Data Standards*) is 552 pages long shows the level of complexity.

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

However, we realize that within these constraints much can and is being done at GPO to improve Human Capital operations and management. In order to improve the efficiency and effectiveness of our operations we have undertaken a number of significant initiatives. At the outset of our change process we tasked GPO's organizational architects to conduct an independent review and analysis of our operations. We also involved our customers and employees in a thorough review of all aspects of our operations. We then used that information to begin a top-to-bottom redesign and restructuring of our operations. We have recently reorganized Human Capital with an emphasis on ensuring that all of our processes are designed around robust quality control measures, specific measures of accountability at both the employee and organizational level, and involvement and review from outside of Human Capital.

We now have ongoing weekly Financial and Human Capital vulnerability assessment meetings that involve key staff from both organizations. As part of this new process we have drafted a plan to regularly sample a significant portion of all key entries affecting employee data at the National Finance Center and within our time and attendance system (WebTA).

At the strategic level, earlier this year we conducted a business case presentation for all of our senior managers on the need for a comprehensive workforce planning process. Following those presentations we developed and distributed detailed workforce data and then conducted meetings with the senior management of each business unit within GPO to discuss and begin to plan for a GPO-wide Human Capital Strategic Plan.

To ensure that we stay on track with our Human Capital improvements we have committed to the establishment of regular customer service surveys and specific measures of accuracy and timeliness. These three metrics will be used as the basis for all Human Capital performance plans. We are also committed to the establishment of an internal quality assurance program that will allow us to evaluate programs and processes across Human Capital. Finally, we are continuing to work with the organizational architects to ensure that we can maximize our efficiencies through the use of continual process improvement approaches.

2. *Information Technology Management and Security:*

   a. *Compliance with the Federal Information Management Security Act (FISMA):* GPO has continued to make progress in complying with

FISMA. As the OIG report states, each of the 21 recommendations provided by the recent FISMA compliance assessment will remain open until fully implemented by management and evaluation by the OIG.

b. *Implementation of the Federal Digital System:* There have been numerous incremental production builds (sprints or increments) as part of our agile development methodology. These builds have been driven by the addition of collections, which in turn drives completion of Release 1.

GPO initially estimated that 55 collections were available on *GPO Access* to be migrated to FDsys. All content has been accounted for during the migration process. The differences in the current numbering and naming of content collections can be attributed to the way content is grouped and processed within FDsys, as has been detailed previously, most recently at the FDsys program review conducted in April. FDsys currently contains 29 of 41 FDsys collections, representing over 90% of the *GPO Access* content, and all collections will be in FDsys after the completion of the Group 5 collections development. The collections remaining represent smaller collections in volume and in usage, with the bulk of the collections and relevant *GPO Access* data currently available on FDsys.

GPO has developed a detailed task list and a schedule has been created for Release 1 completion activities. The tasks and schedule were developed with full support from the FDsys Chief Architect, FDsys Integration Manager, and the FDsys development team. The execution of this schedule will allow for the completion of Release 1 by the end of this fiscal year.

Our intent is to make FDsys GPO's system of record after all *GPO Access* content had been migrated to it, and when there is assured access capability in the event of system failure. Access will be assured through the stand up of a continuity-of-operations (COOP) capability. Through our ongoing Risk Review Process, we identified a timing risk with implementing a full failover capability (i.e., COOP), which will not be complete until late 2010. To mitigate this risk, we are building a Continuity of Access (COA) capability for FDsys at the legislative branch alternate computing facility (ACF). This capability will provide effective failover of the data access functionality of FDsys, meeting the requirements we have identified to establish FDsys as the system of record. The deployment of this COA site substantially reduces our risk while providing a high level of service to Congress and the public and allows GPO to begin sunsetting *GPO Access*.

Critical FDsys data, including content, metadata, source code, and documentation from the FDsys development, test, and production instances, are currently backed up offsite to the Alternate Computing Facility. Implementing continuity and failover for FDsys in this phased approach, consisting of the completion of COA followed by the completion of the full COOP failover instance in late 2010, provides continuity of access to historic and new content, with the ability to recreate the full system from backups. The COA capability will be operational in August 2010 and the full system failover capability will be operational in December 2010.

Issues identified through Program Tracking Reports (PTRs) are reported and corrected based on the severity of the issue. In terms of system quality, of the 1,284 PTRs reported since FDsys was launched, 62 represent issues that were determined to be "critical" to the operations of the system. All of these issues have been resolved. The vast majority of outstanding PTRs are a result of processing inconsistent data being migrated from *GPO Access*. As stated in the April program review, the data migration activities have been more complex than originally estimated. We also have adopted very high quality standards for the data migrating into FDsys. As such, any issue found in the migration process is logged as a PTR. This process is reviewed regularly at content migration design reviews as well as in our regular Change Control Board meetings.

Regarding the open recommendations from the Quarterly IV&V reports on FDsys, a process has been put in place to assist in the closure of these recommendations and is in use.

c. *Other Challenges:* There were two primary issues in the PURL system failure. One was an IT infrastructure failure and the other was a loss of the Persistent Uniform Resource Locator (PURL) database.

The PURL database is on the same infrastructure hardware that had supported Microcomp until we migrated this critical application to a new infrastructure called Itanium, which is now operational and replicated at the ACF. The PURL system had not yet been migrated off the old infrastructure. A component in the old infrastructure failed. We were able make a repair with parts that we maintain in inventory in 2-3 days. However, the infrastructure failure resulted in data loss from the PURL database that then needed to be restored. The database restoration process that had been documented years ago was flawed and did not allow GPO to effectively restore the database.

GPO contacted OCLC for assistance, which stepped in and helped restore the database. This process took several weeks.

There were a number of after-action tasks that resulted from this issue. First, a backup system was created for the infrastructure support for the PURL database. This system stays available at all times. In the event of an issue with the production infrastructure, the backup is invoked immediately. Second, the database backup process was corrected and documented, updating the old and erroneous procedure. Finally, a comprehensive project to replace the PURL datebase was initiated and is underway. This project will allow GPO to host the PURL application outside of GPO, providing a modernized application and complete failover capabilities by the host provider. The new capability is expected to be launched this summer, allowing us to sunset the existing PURL system. Additionally, GPO's library and IT areas have initiated a comprehensive review of all library program applications and have developed a plan to upgrade or replace all of them to ensure continued operational capability. These projects are now underway.

3. *Security and Intelligent Documents:* GPO's Security and Intelligent Documents (SID) business unit continued to be the Federal Government's leading provider of secure credentials and identity documents in two secure production facilities located in Washington, DC, and Stennis, MS.

   SID has made significant progress on the audit recommendations that were made. To date SID has made sure that all secure passport materials are properly segregated from any other GPO materials. All stock locations are now being monitored by camera and require a badge or code to enter the area. The access list is being monitored by Security and SID management to make sure that only members who have a need to enter the area are authorized to do so. Changes have been made to the SID's Manager of Product Security and Integrity position and the Secure Supply Chain Vendor Audit Program has been documented and formalized. The position was moved from oversight of the Operations Manager to the Managing Director of SID, with direct access to the Deputy Public Printer, to minimize any potential conflict of interest. A new Manager of Product Security and Integrity was hired and begins working in the position in June. The roll-out and implementation of this improved audit program will be accomplished during the months ahead as the new Manager of Product Security and Integrity conducts visits to our key vendor locations. In addition, a detailed process for all vendor security audits has been developed. This process includes vendor audit procedures, trip report

procedures, vendor risk analysis, long term calendar of supplier visits, and a trip approval procedure. Additional items will be addressed to ensure that GPO's Acquisitions, General Counsel staff, and Security continue to be involved with the overall vendor selection, audit requirements as part of the contracts, and formal security audits of our manufacturing facility.

Regarding the security personalization system (SECAPS), the audit of SECAPS is anticipated to be completed sometime in June 2010.

SIDS plans to obtain ISO certification for the Stennis, MS, facility in the summer of 2010; the same certification for the Washington, DC, passport production facility is planned for FY 2011. Additionally, 5S audits continue in both the facilities, with scores of above 90%.

GPO has been working to obtain certification as a producer of HSDP-12 identification cards. In May 2010, card samples passed all external laboratory tests. We are currently waiting scheduling from the General Services Administration's certifying body, and anticipate certification in June 2010.

A Request for Proposal was issued this spring for passport covers and associated materials. SID is reviewing the questions and is ready to receive samples from potential vendors for testing.

4. *Internal Controls:* As noted above, SID has made significant progress on the audit recommendations that were made regarding controls over passport supply chain security. To date SID has made sure that all secure passport material is properly segregated from any other GPO material. All stock locations are now being monitored by camera and require a badge or code to enter the area. The access list is being monitored by Security and SID management to make sure that only members who have a need to enter the area are authorized. Changes have been made to the SID Manager of Product Security and Integrity's position and the audit process has been formalized. The position was moved from oversight of the Operations Manager to the Director of Security and Intelligent Documents to eliminate any potential conflict of interest. In addition a detailed process for all vendor security audits has been developed. This process includes vendor audit procedures, trip report procedures, vendor risk analysis, long term calendar of supplier visits, and a trip approval procedure. Additional items will be addressed to ensure that GPO's Acquisitions, General Counsel staff, and Security continue to be involved with the overall vendor selection, audit requirements as part of the contracts, and formal security audits of our manufacturing facility.

Management concurred with KPMG's 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, 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, and finally supervisory review procedures are now in effect to help reduce the risk of any further cash flow statement misclassifications.

5. *Protection of Sensitive Information:* GPO adopted two directives to formalize a structure for the protection of sensitive information and to assign specific responsibilities.

   GPO has modified the forms used to procure printing to require agency customers to identify printing jobs that contain PII. GPO is in the process of rolling out the updated forms for use by all agency customers. Printing jobs identified as containing PII are subject to special handling to safeguard the PII. Print Procurement has developed and implemented a standard operating procedures governing PII effective May 2010. A PII standard operating procedure (SOP) has been distributed to Print Procurement employees and will be posted on the Intranet.

   GPO has prepared training to educate employees in how to identify and safeguard PII information. This course will become part of the recurring training requirement for appropriate employees to maintain focus in this important area.

   GPO has designated a Privacy Officer and is in the process of hiring a dedicated Program Manager for privacy. These individuals will carry out the initial requirements of the PII directive to complete an inventory of PII data in use at GPO, review individual business unit plans, and prepare a plan to reduce the use of Social Security numbers to the minimum level required.

6. *Acquisitions and Print Procurement:* Acquisition Services has contracted with an outside vendor to provide an independent assessment of the acquisitions function. The findings of the assessment should be available by September 30, 2010.

   Management concurs with the finding on contract administration and is addressing this concern through training provided by the Federal Acquisition Institute and quarterly Acquisition in-services training where

contract administration and other specific acquisition functions are addressed.

As contracts for various supplies for passports are being renewed, Acquisition Services will work with SID and the Office of the General Counsel to ensure that appropriate security language is incorporated. In addition, Acquisition Services will begin reviewing all supplier contracts to ensure that appropriate security language is incorporated.

Acquisition Services continues to work with various GPO business units to ensure that applicable contracts meet sustainability requirements and will aggressively identify other procurements where sustainable initiatives can be achieved.

7. *Financial Management and Performance:* As noted above, management concurred with KPMG's 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, 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, and finally supervisory review procedures are now in effect to help reduce the risk of any further cash flow statement misclassifications.

8. *Continuity of Operations:* Development of GPO's continuity of operations (COOP) capabilities continues as a top management priority.

   During the reporting period GPO conducted internal and external COOP exercises in accordance with an annual exercise plan. These exercises are designed to train GPO staff in the required processes and actions that would be needed during an actual event as well as identify further areas for improvement. During the reporting period our COOP activities focused on agency command and control and mission support for Congress, the Office of the Federal Register, and the State Department.

   In support of the Congress, GPO has formalized liaison roles for COOP planning and coordination. Specific staff have been assigned primary responsibilities for each chamber. These COOP planners work with the appropriate GPO business units and congressional offices to ensure that GPO's planning and exercise strategy is well aligned with the needs of the House and Senate.

GPO's IT department continues to implement redundant capabilities for COOP. GPO's Blackberry servers are now redundant between separate facilities.

One of the complexities of COOP is that the Federal Government uses an "all hazards" approach that requires COOP planners to prepare for a wide variety of situations as part of the planning process. In order to more closely track the readiness level of GPO and its business units for various COOP events, the COOP team is instituting a maturity level metric to allow stakeholders to easily understand the current state of preparedness on an on-going basis.

9. *Strategic Vision and Customer Service:* In May 2010, senior management developed a draft update to GPO's Strategic Vision, which had been previously issued on December 4, 2004. The draft document provides an update to the situational analysis and identifies key trends impacting the development and execution of a strategic vision. In response to these trends, senior management also developed nine strategic goals, which include but are not limited to the creation of a customer service culture, support of the current Administration's transparency initiative, and a continued collaborative approach toward fiscal responsibility. The draft document is pending approval from executive staff.

10. *Sustainable Environmental Stewardship:* As the largest industrial manufacturer in the District of Columbia, GPO is committed to environmental stewardship and is focused on reducing manufacturing waste and green-house gasses, increasing the use of 100% post-consumer waste recycled paper, and purchasing energy from sustainable sources and products manufactured using sustainable raw materials. This commitment complements longstanding environmental practices carried out at GPO in compliance with applicable Federal laws and regulations.

    GPO reaffirms its commitment to reducing environmental impact on a daily basis by printing the *Congressional Record* and the *Federal Register* using 100% recycled newsprint. GPO has also made changes in the print procurement practices to allow customers to specify certified sustainable paper and is currently evaluating responses to a RFP for the most sustainable copier paper available in today's market. The evaluation criteria included the sourcing of raw materials, post consumer fiber content, use of renewable resources, use of bio-generation, chain of custody, recyclability and environmental sustainable packaging, chemicals and fillers, carbon footprint, waste generation, water consumption,

transportation, energy consumption, and total green house gas (GHG) emissions.

GPO has completed a printing industry process evaluation and is developing a chemical inventory management system that will manage the chemical inventory of cleaning supplies, paints and solvents, chemicals and oils, and press chemicals and inks. The Phase 1 chemical database is in development to standardize chemicals and solvents used throughout the facility, with additional phases to develop acquisitions processes and policy for sustainable goods that reduce energy consumption, environmental impacts and increase economic performance.

GPO has an agency-wide effort to reduce the amount of landfill waste leaving our facility. Over the past several months, GPO has established a voluntary partnership with EPA's WasteWise program to baseline and monitor waste reduction and prevention activities. These efforts diverted nearly 90% of GPO's landfill waste stream to new and existing recycling streams in 2008. Based on WasteWise's calculations, these actions resulted in the reduction of over 15 billion tons of GHG emissions. GPO is also developing criteria and requirements to issue a Total Waste Management RFP that will consolidate waste hauling contracts to achieve the most favorable rates and enhance our recycling efforts and landfill reduction initiatives.

GPO requires all new construction contracts to recycle and mitigate landfill waste for materials that leave our facility. GPO's efforts have reduced landfill waste by issuing a contract to ensure all of our wood waste (pallets, skids and old furniture) is recycled. Currently, GPO's wood waste is being used for mulch in Maryland.

GPO's roof project, completed in Spring 2010, will achieve energy conservation for the agency and utilize a bio-based ELMS coating that is Energy Star approved with 0.77 reflectivity and a tested emissivity of 0.93 under ASTM E409. The net result is a roof that reduces the effect of summertime heat islands, thereby reducing air conditioning costs and peak demand and providing the opportunity to earn LEED credit under LEED Sustainable Sites.

GPO actively participates in EPA's sustainability management workgroup and the CAO Green Council. GPO is currently seeking partnership with other legislative branch agencies to ensure each agency and Federal employee has ample opportunity to recycle and participate in sustainability initiatives, regardless of the size of the agency.

Over the past year, GPO has reduced our volatile organic compound (VOC) emissions in our plant operations by 86% which also reduced our purchasing costs for fountain solution by 22%. Our production managers have been testing new fountain solution concentrates that contain no or low VOCs and have been successful. Testing continues on other press solvents in hopes to further reduce our environmental footprint. GPO's paint shop has converted to exclusively using zero-VOC office paints throughout the building.

Audits and Inspections. During the reporting period, the OIG issued 6 new audit and assessment reports, with recommendations to help improve operational performance:

- *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).* This assessment continued the ongoing IV&V evaluation associated with the development of FDsys. This evaluation provides quarterly observations and recommendations on the FDsys program's technical, schedule, and cost risks, as well as related issues. This quarterly report identified a number of technical risks associated with FDsys configuration management and risk management activities. The report contains 11 recommendations designed to strengthen these activities. As the OIG's report notes, management generally concurred with the recommendations and has either taken or proposed responsive corrective actions.

- *Financial Statement Audit (Audit Report 10-02, January 8, 2010).* Title 44, U.S.C., requires that GPO obtain an annual audit of its financial statements, which the OIG oversees. The audit of GPO's FY 2009 financial statements was conducted by KPMG. KPMG issued an unqualified opinion on GPO's financial statements, stating the financial statements 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 report notes, KPMG made recommendations for each condition; management concurred with those recommendations and has either planned or initiated responsive corrective action.

- *GPO's Compliance with the Federal Information Security Management Act (Assessment Report 10-03, January 12, 2010).* FISMA mandates security measures for the information and information systems that support the operations and assets of executive branch agency. As a

legislative branch agency, GPO is not covered by FISMA but recognizes the need to be compliant because of the services it provides to executive branch agencies. A baseline assessment of GPO's compliance was conducted in 2007. GPO completed a full assessment in 2009, which concluded that although some progress had been made in compliance there are still weaknesses that can be identified, some of them dating to the 2007 report. This report included 21 recommendations to strengthen GPO's compliance with FISMA. As the OIG report states, each of the 21 recommendations provided by the recent FISMA compliance assessment is considered resolved and will remain open pending follow-up by the OIG.

- *GPO Network Vulnerability Management (Assessment Report 10-04, January 19, 2010).* This assessment of GPO's network vulnerability management program focused specifically on GPO's passport production system environment and public facing servers. As the OIG's report says, this assessment concluded that GPO implemented a robust and effective vulnerability management program that identifies and circumvents common internal and external network threats related to both the passport printing and production system and public-facing servers. The OIG says that since their last assessment the program has been significantly strengthened.

- 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). This report identified several technical risks associated with FDsys development practices, system engineering, COOP, existing PTRs, and the FDsys test program. It contained 6 recommendations to mitigate risks and strengthen program management. Three of the recommendations were subsequently closed and three remained unresolved at the close of the reporting period.

- *Security of GPO's Passport Supply Chain (Audit Report 10-06, March 31, 2010).* This audit focused on the security of passport components and supply chain. The audit disclosed that the passport supply chain process was largely informal and made recommendations to ensure continued security of the supply chain by establishing a formal security oversight process. As the OIG report notes, GPO management concurred with each of the recommendations and has either already implemented or planned responsive corrective actions.

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).* Two recommendations made in this report remain open. As the OIG report notes, the most recent Network Vulnerability Assessment found that implementation of corrective actions is still ongoing.

- *Report on GPO's Compliance with the Federal Information Security Management Act (FISMA) (Assessment Report 07-09, September 27, 2007).* As the OIG report notes, management continues to work on implementing corrective actions for the 7 remaining open recommendations.

- *Operating System Security for GPO's Passport Printing and Production System (Assessment Report 08-06, March 31, 2008).* One recommendation remains open.

- *Diversity Management Programs at GPO (Audit Report 08-10, September 11, 2008).* Two recommendations remain open. As the OIG's report states, management continues with implementation of the remaining essential elements of the Equal Employment Opportunity Commission's Management Directive 715 and the leading diversity management practices identified by the Government Accountability Office.

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

- *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).* As the OIG report notes, 3 recommendations remain open as management continues to work on implementing corrective actions.

- *Audit of GPO's Passport Printing Costs (Audit Report 09-02, December 22, 2008).* One recommendation remains open, as the OIG report notes, as management is in the process of revising indirect cost rates.

- *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).* Four recommendations remain open.

- *Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Security Analysis Report (Assessment Report 09-04, December 24, 2008).* Three recommendations remain open, as the OIG report states, as management continues to take responsive actions.

- 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, as the OIG report states, as management continues to take responsive actions.

- *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).* As the OIG report notes, the OIG made 25 recommendations in this report. Management generally concurred with all except for one and proposed responsive actions for each. At the end of the reporting period, 23 recommendations remain open.

- *Accounts Payable Service Billings (Audit Report 09-13, September 30, 2009).* One recommendation remains open. As the OIG report notes, the recommendation should be closed during the next reporting period.

- *GPO's Workers' Compensation Programs (Audit Report 09-14, September 30, 2009).* One recommendation remains open and should be closed by the end of the next reporting period, as the OIG report notes.

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 requests for investigations by other legislative branch agencies, in some cases resulting 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.