Section II: Financial

[Page Left Intentionally Blank]

MESSAGE FROM THE CHIEF FINANCIAL OFFICER

As the Acting Chief Financial Officer (CFO) of the Department of Health and Human Services (HHS), I recognize that our Department is accountable to our ultimate stakeholders -- the American Public. We are careful to use taxpayer resources wisely to carry out the Department's mission to enhance the health and well-being of Americans. With an annual direct budget authority of nearly $841 billion in fiscal year (FY) 2009, we are one of the largest, most complex financial organizations in the world. Through collaboration, our CFO Community manages financial accountability, compliance, and risk across HHS.

For the third year, we have chosen to participate in the Office of Management and Budget (OMB) pilot approach to improving performance and accountability reporting. Pursuant to OMB Circular A-136, *Financial Reporting Requirements*, this *Agency Financial Report* represents our accountability report for FY 2009. The *FY 2009 Performance Report* and the *FY 2011 Congressional Budget Justification* will be available in February 2010, as will the *Summary of Performance and Financial Information*. HHS believes that this approach makes information more transparent and useful to the President, Congress, and American people.

During FY 2009, the Department successfully sustained its standards for reporting and management controls. We have improved our reporting processes and successfully performed our fourth annual, more rigorous internal control assessment as required by OMB Circular A-123, *Management's Responsibility for Internal Control.* In Section I of this report, we present the Secretary's qualified Statement of Assurance reflecting the results of our assessment.

This report also contains our audited annual financial statements. For the eleventh consecutive year, I am pleased to report that our independent auditors have issued an unqualified or "clean" opinion. The FY 2009 independent auditors' report identifies two internal control material weaknesses relating to: (1) financial reporting systems, analyses, and oversight, and (2) financial management information systems. The Department recognizes the importance of effective internal control and is committed to resolving these material weaknesses promptly. During FY 2010, we will continue our collaborative efforts to improve our financial management and to further enhance information available through the implementation of a consolidated reporting solution.

With respect to our financial reporting capabilities, the Department continues to convert Medicare contractor systems, which will substantially comply with the *Federal Financial Management Improvement Act (FFMIA)* by the end of 2010. While much work remains, we are committed to resolving long-standing issues to strengthen our control structure. Many of our FY 2009 improvements resulted from our strong commitment to accountability, transparency, and effective stewardship. During FY 2009, our CFO executives throughout the Department worked together as a community to provide the public with transparent information concerning our implementation of the *American Recovery and Reinvestment Act of 2009*.

Finally, I want to thank our employees and partners who work each day to achieve our Nation's noblest human aspirations for safety, compassion, and trust. This report -- and the accomplishments it describes -- is a reflection of their extraordinary dedication to our mission. Together, we look forward to tackling an ambitious agenda in 2010.

Richard J. Turman
Acting Assistant Secretary for Financial Resources and Chief Financial Officer

[Page Intentionally Left Blank]

OFFICE OF INSPECTOR GENERAL TRANSMITTAL OF THE REPORT ON THE FINANCIAL STATEMENT AUDIT

[Page Intentionally Left Blank]

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Washington, D.C. 20201

NOV 10 2009

TO: The Secretary
Through: DS ________
COS ________
ES ________

FROM: Inspector General

SUBJECT: Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2009 (A-17-09-00001)

This memorandum transmits the independent auditors' reports on the Department of Health and Human Services (HHS) fiscal year (FY) 2009 financial statements, conclusions about the effectiveness of internal controls, and compliance with laws and regulations. The Chief Financial Officers Act of 1990 (P.L. No. 101-576), as amended, requires the Office of Inspector General (OIG) or an independent external auditor, as determined by OIG, to audit the HHS financial statements in accordance with applicable standards.

We contracted with the independent certified public accounting firm of Ernst & Young, LLP (E&Y), to audit the HHS consolidated balance sheet as of September 30, 2009, and the related consolidated statements of net cost and changes in net position, the combined statement of budgetary resources for the year then ended, and the statement of social insurance as of January 1, 2009. The contract required that the audit be performed in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in the "Government Auditing Standards," issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin 07-04, as amended, "Audit Requirements for Federal Financial Statements."

Results of Independent Audit

Based on its audit, E&Y found that the FY 2009 HHS financial statements were fairly presented, in all material respects, in conformity with accounting principles generally accepted in the United States of America. However, E&Y noted two matters involving internal controls over financial reporting that were considered to be material weaknesses under standards established by the American Institute of Certified Public Accountants:

- *Financial Reporting Systems, Analyses, and Oversight.* Internal control weaknesses continued in HHS's financial management systems, financial analyses and oversight, and

Page 2 – The Secretary

corrective actions. HHS's lack of an integrated financial management system impaired its ability to support and analyze account balances. Manual intervention was required to correct transactions that did not post in accordance with standards and to transfer information between systems that did not interface electronically. In addition, certain reconciliations and account analyses were not adequately or timely performed to ensure that differences were identified and resolved and that invalid or old transactions were identified and closed. Also, management has not implemented corrective action for some longstanding deficiencies in internal control. HHS's financial management systems did not substantially comply with Federal financial management systems requirements or the U.S. Government Standard General Ledger at the transaction level.

- *Financial Management Information Systems.* General control issues in both the design and the operation of key controls were noted in security management, access controls, configuration management, segregation of duties, and contingency planning. In addition, weaknesses were noted in general controls, business process controls, interface controls, and data management system controls for specific financial applications.

Evaluation and Monitoring of Audit Performance

In accordance with the requirements of OMB Bulletin 07-04, we reviewed E&Y's audit of the HHS financial statements by:

- evaluating the independence, objectivity, and qualifications of the auditors and specialists;
- reviewing the approach and planning of the audit;
- attending key meetings with auditors and HHS officials;
- monitoring the progress of the audit;
- examining audit documentation related to the review of internal controls over financial reporting;
- reviewing the auditors' reports; and
- reviewing the HHS Management Discussion and Analysis, Financial Statements and Footnotes, and Supplementary Information.

E&Y is responsible for the attached reports dated November 10, 2009, and the conclusions expressed in those reports. Our review, as differentiated from an audit in accordance with U.S. generally accepted government auditing standards, was not intended to enable us to express, and accordingly we do not express, an opinion on HHS's financial statements, the effectiveness of internal controls, whether HHS's financial management systems substantially complied with the Federal Financial Management Improvement Act, or compliance with laws and regulations. However, our monitoring review, as limited to the procedures listed above, disclosed no

Page 3 – The Secretary

instances in which E&Y did not comply, in all material respects, with U.S. generally accepted government auditing standards.

If you have any questions or comments about this memorandum, please do not hesitate to call me, or your staff may contact Joseph E. Vengrin, Deputy Inspector General for Audit Services, at (202) 619-3155 or through email at Joseph.Vengrin@oig.hhs.gov. Please refer to report number A-17-09-00001.

Daniel R. Levinson

Daniel R. Levinson

Attachments

cc:
Richard Turman
Acting Assistant Secretary for Resources and Technology

Sheila Conley
Deputy Assistant Secretary, Finance

[Page Intentionally Left Blank]

Independent Audit Reports

ERNST & YOUNG

Ernst & Young LLP
8484 Westpark Drive
McLean, VA 22102

Tel: 703-747-1000
www.ey.com

Report of Independent Auditors

To the Secretary and the Inspector General of the
U.S. Department of Health and Human Services

We have audited the accompanying consolidated balance sheets of the U.S. Department of Health and Human Services (DHHS) as of September 30, 2009 and 2008, and the related consolidated statements of net cost and changes in net position, and the combined statement of budgetary resources for the fiscal years then ended, and the statement of social insurance as of January 1, 2009 and 2008. These financial statements are the responsibility of DHHS's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with auditing standards generally accepted in the United States, the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended. Those standards and bulletin require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. We were not engaged to perform an audit of DHHS's internal control over financial reporting. Our audits included consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of DHHS's internal control over financial reporting. Accordingly, we express no such opinion. An audit also includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements, assessing the accounting principles used and significant estimates made by management, and evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of DHHS as of September 30, 2009 and 2008, and its net cost, changes in net position, and budgetary resources for the years then ended, and the financial condition of its social insurance program as of January 1, 2009 and 2008 in conformity with accounting principles generally accepted in the United States.

ERNST & YOUNG

Report of Independent Auditors
Page 2

As discussed in Note 26 to the financial statements, the statement of social insurance presents the actuarial present value of the Center for Medicare and Medicaid Services' Hospital Insurance (HI) and Supplementary Medical Insurance (SMI) trust funds' estimated future income to be received from or on behalf of the participants and estimated future expenditures to be paid to or on behalf of participants during a projection period sufficient to illustrate long-term sustainability of the social insurance program. In preparing the statement of social insurance, management considers and selects assumptions and data that it believes provide a reasonable basis for the assertions in the statement. However, because of the large number of factors that affect the statement of social insurance and the fact that future events and circumstances cannot be known with certainty, there will be differences between the estimates in the statement of social insurance and the actual results, and those differences may be material. In addition to the inherent variability that underlies the expenditure projections prepared for all parts of Medicare, the SMI Part D projections have an added uncertainty in that they were prepared using very little program data upon which to base the estimates.

In accordance with *Government Auditing Standards*, we also have issued our reports dated November 10, 2009 on our consideration of DHHS's internal control over financial reporting and on our tests of its compliance with certain provisions of laws and regulations and other matters. The purpose of those reports is to describe the scope of our testing of internal control over financial reporting and compliance and the results of that testing, and not to provide an opinion on the internal control over financial reporting or on compliance. Those reports are an integral part of an audit performed in accordance with *Government Auditing Standards* and should be considered in assessing the results of our audit.

Our audits were conducted for the purpose of forming an opinion on the 2009 and 2008 basic financial statements taken as a whole. The information presented in Management's Discussion and Analysis, required supplementary stewardship information, required supplementary information, and other accompanying information is not a required part of the basic financial statements but is supplementary information required by OMB Circular No. A-136. The other accompanying information has not been subjected to the auditing procedures applied in our audit of the basic financial statements and, accordingly, we express no opinion on it. For the remaining information, we have applied certain limited procedures, which consisted principally of inquiries of management regarding the methods of measurement and presentation of the supplementary information. However, we did not audit the information and express no opinion on it.

Ernst + Young LLP

November 10, 2009

Ernst & Young LLP
8484 Westpark Drive
McLean, VA 22102

Tel: 703-747-1000
www.ey.com

Report on Internal Control

To the Inspector General and Secretary of the
U.S. Department of Health and Human Services

We have audited the financial statements of the Department of Health and Human Services (DHHS or the Department) as of and for the year ended September 30, 2009, and the statement of social insurance as of January 1, 2009, and have issued our report dated November 10, 2009. We conducted our audit in accordance with auditing standards generally accepted in the United States; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended.

In planning and performing our audit, we considered the Department's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control over financial reporting. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 07-04, as amended. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982 (FMFIA), such as those controls relevant to ensuring efficient operations.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be significant deficiencies or material weaknesses and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified. However, as discussed below, we identified certain deficiencies in internal control that we consider to be material weaknesses.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. We consider both deficiencies related to Financial Reporting Systems, Analyses, and Oversight; and Financial Management Information Systems—to be material weaknesses.

ERNST & YOUNG

Report on Internal Control
Page 2

Material Weaknesses

Financial Reporting Systems, Analyses, and Oversight

Overview

In fiscal year (FY) 2004, DHHS began its implementation of a commercial web-based off-the-shelf product modified to replace five legacy accounting systems and numerous subsidiary systems with one modern accounting system with three components. The three components include:

- Healthcare Integrated General Ledger Accounting System (HIGLAS)—developed to support the financial activities of the Centers for Medicare & Medicaid Services (CMS) and its Medicare contractors. Although initiated in fiscal year (FY) 2005, full implementation is not expected until FY 2013.
- National Institutes of Health (NIH) Business System (NBS)—developed to support the financial activities at NIH. NIH completed certain aspects of its implementation in FY 2008 with more ancillary systems expected to be implemented over the next few years.
- Unified Financial Management System (UFMS)—developed to support the financial activities at the remaining operating divisions (OPDIVS) with full implementation completed in FY 2008. Certain processes to refine the implementation and address systemic issues are ongoing.

During FY 2009, DHHS continued its refinements of its financial management systems and processes. For example, in February, DHHS implemented its new Health and Human Services Consolidated Acquisition Solution (HCAS) which provides an integrated "Procure to Pay" process from initiation (purchase requisition, purchase orders) to close out and is integrated with UFMS.

Although certain progress was made in FY 2009, the organization was required to refocus much of its efforts and resources on the implementation of requirements of the American Recovery and Reinvestment (ARRA) Act. The ARRA Act, which was established on February 17, 2009, increased DHHS budgets by approximately $167 billion over ten years and provided for strict guidelines on how and exactly when those funds should be distributed, accounted for, monitored, and reported to OMB and Congress. These funds were distributed among most of DHHS's operating divisions and required new processes to be developed or modified within a very short time frame under DHHS's American Recovery and Reinvestment Implementation Plan to ensure compliance with the Act and OMB regulation.

Ernst & Young

Report on Internal Control
Page 3

Despite some progress, our testing of internal control continued to identify serious internal control weaknesses in financial systems and processes for producing financial statements, including lack of integrated financial management systems and weaknesses in entity-wide internal control which impaired DHHS's ability to report accurate and timely financial information. Within the context of the approximately $800 billion in departmental net outlays, the ultimate resolution of such amounts is not material to the financial statements taken as a whole. However, these matters are indicative of serious systemic issues that must be resolved.

Lack of Integrated Financial Management System

DHHS's financial management systems are not compliant with the Federal Financial Management Improvement Act (FFMIA) of 1996. FFMIA requires agencies to implement and maintain financial management systems that comply with federal financial management systems requirements. More specifically, FFMIA requires federal agencies to have an integrated financial management system that provides effective and efficient interrelationships between software, hardware, personnel, procedures, controls, and data contained within the systems and compliance with the United States Standard General Ledger (USSGL) at the transaction level and applicable federal accounting standards. The lack of an integrated financial management system continues to impair DHHS's and its OPDIVs' abilities to adequately support and analyze account balances reported.

Although DHHS implemented a commercial off-the-shelf product, approved by the former Joint Financial Management Improvement Program (JFMIP), DHHS's accounting systems lack integration and do not conform to the requirements. DHHS's management has identified configuration issues that result in inappropriate transactional postings. Finally, the financial systems are not fully integrated and are not expected to have full integration until FY 2013. Specific weaknesses noted include the following:

- Although progress was made during FY 2009, thousands of manual journal vouchers in excess of $259 billion in absolute value were required to be recorded in UFMS to post certain types of transactions—including transactions to record certain proprietary and budgetary entries, record accruals, perform adjustments between governmental and nongovernmental accounts, perform adjustments to agree budgetary to proprietary accounts, perform other reconciliation adjustments at period end, and correct errors identified related to configuration issues within UFMS. These entries are nonstandard postings to UFMS to record both the proprietary and budgetary affects of certain financial activities for which the financial system is not configured properly to post automatically. Although these entries are required to be posted to the general ledger in order for the financial statements to be accurate, many of these entries should have been configured as routine systematic entries within UFMS. Although these entries are considered manual postings, they are in fact subject to automated edit checks such as cross validation rules and funds control. Additionally, we noted certain weaknesses with

ERNST & YOUNG

Report on Internal Control
Page 4

the use of manual entries including improper or lack of approvals and limited descriptions as to the purpose of the entry. Late in FY 2008, new policies and procedures related to manual entries were issued. However, OPDIVs have not fully implemented policy to ensure entries are properly authorized and supported by appropriate documentation.

- As discussed in further detail below, reviews of general and application controls over financial management systems identified certain departures from requirements specified in OMB Circulars A-127, *Financial Management Systems*, and A-130, *Management of Federal Information Resources*. Additionally, we identified certain issues, including access control deficiencies related to systems as part of our Federal Information Security Management Act and other Office of Inspector General (OIG) engagements. Finally, DHHS management has identified financial management information systems as a material weakness as a result of its OMB Circular A-123 assessment.

- Although the OPDIVs are using UFMS to account for financial activities within the OPDIVs, the DHHS is utilizing the Automated Financial System (AFS) to compile the consolidated financial statements. AFS, a spreadsheet macro driven process, requires the OPDIVs to manually enter their trial balances and footnote disclosures for DHHS to compile the Department-level consolidated financial statements. The key entry process can be error-prone if effective detective controls are not in place. In our review of the initial financial statements provided on October 20, 2009, we noted several OPDIVs recording incorrect amounts causing certain financial statement line items to be incorrect. Additionally, we noted several adjustments totaling in excess of $2.2 billion were recorded within AFS to ensure proper balancing of statements or disclosure. As a result, certain amounts within AFS did not consistently agree to balances within the OPDIVs general ledger. During FY 2009, DHHS initiated its implementation of an automated reporting process at several locations. Full implementation is not expected until FY 2011.

- Due to certain configuration issues within UFMS, certain financial statement balances on the Statement of Budgetary Resources (SBR) require analysis of other accounts to derive/estimate the amounts reported. For example, financial accounting and reporting standards require that DHHS record prior year recoveries in a separate general ledger account and report these amounts on the SF-133 and the SBR. These items are currently not being captured within UFMS. As a result, most OPDIVs are required to analyze transactions in other accounts to derive the balance.

- CMS, the largest entity within DHHS processing 85% of total expenditure activity, continues its efforts to implement HIGLAS, which will integrate the CMS contractors' standard claims processing system and replace the CMS current mainframe-based financial system with a web-based accounting system. CMS relies on a decentralized organization/structure and complex financial management systems—not only within its

Ernst & Young

central office and regional offices' processes but within many of the Medicare contractor organizations—to accumulate data for financial reporting. Currently, CMS's lack of a single integrated financial management system continues to impair its ability to efficiently and effectively support and analyze financial reports. The Medicare contractors that have not implemented HIGLAS continue to rely on a combination of claims processing systems, personal computer-based software applications and other ad hoc systems to tabulate, summarize, and prepare information that is reported to CMS on the *750—Statement of Financial Position Reports*, the *751—Status of Accounts Receivable Reports*, and the reporting of funds expended, and the *1522—Monthly Contractor Financial Report*. The accuracy of these reports remains heavily dependent on inefficient, labor-intensive, manual processes that are also subject to an increased risk of inconsistent, incomplete, or inaccurate information being submitted to CMS.

Resource limitations and other priorities were noted as causes for delays in upgrading certain system and financial internal control processes limiting DHHS's ability to comply with requirements under FFMIA.

Financial Analysis and Oversight

The U.S. Government Accountability Office (GAO)'s *Standards for Internal Control in the Federal Government* states that internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the organization's control objectives. Examples of control activities include: top-level reviews, reviews by management at the functional or activity level, segregation of duties, proper execution of transactions and events, accurate and timely recording of transactions and events, and appropriate documentation of transactions and internal control.

Because weaknesses exist in the financial management systems, management must compensate for the weaknesses by implementing and strengthening additional controls to ensure that errors and irregularities are detected in a timely manner. Our review of internal control disclosed a series of weaknesses that impact DHHS's ability to report accurate financial information on a timely basis. Consistent with prior years, during FY 2009, we found that certain controls were not adequately performed to ensure differences were properly identified, researched, and resolved in a timely manner and that account balances were complete and accurate. We noted the following items in the current year audit that indicate additional improvements in the financial reporting systems and processes are required.

ERNST & YOUNG

Report on Internal Control
Page 6

Department/Operating Division Periodic Analysis and Reconciliation

When weaknesses exist in financial systems, as discussed above, management must compensate by implementing and strengthening entity-wide controls to ensure that errors and irregularities are detected in a timely manner. These entity-wide controls would include monitoring of budgets, reconciliations of accounts, analyses of fluctuation, and aging of accounts. During our audit, we found that certain controls were not adequately performed to ensure that differences were properly identified, researched, and resolved in a timely manner and that account balances were complete and accurate. The following represent specific areas we noted that need enhanced periodic reconciliation and analysis procedures:

- Fund Balance With Treasury—Treasury regulations require that each federal entity ensure that it reconciles on a monthly basis its financial records with Treasury's records and that it promptly resolves differences. If this reconciliation is not adequately performed, loss, fraud, and irregularities could occur and not be promptly detected, and/or financial reports that are inaccurate may be prepared and used in decision-making. On a monthly basis, the DHHS is responsible for reconciling approximately 500 Treasury appropriation symbols. As of June 30, 2009, the general ledger and Treasury's records differed by more than an approximate absolute value of $1.0 billion. This primarily relates to two (2) OPDIVs. One OPDIV did not perform fund balance with Treasury reconciliations and the second OPDIV only focused its resources on items that exceeded a subjective threshold and did not take any action on the remaining differences; for example, differences over $1.0 million are automatically assumed to be caused by timing difference and no action was performed on any differences relating to appropriations that are expiring at year-end but have not expired when the reconciliations were performed. Other differences were caused by a backlog of differences dating back to 2004. During the fourth quarter, management focused additional efforts on its fund balance with Treasury reconciliations which resulted in progress in reducing differences at September 30, 2009 to an approximate $400.0 million.
- OPDIV Financial Reconciliation Activity Certifications—As part of the accounting centers' monthly processes, the Department has instituted a policy whereby the accounting centers certify the status of completing required periodic reconciliations. For each required reconciliation, the preparer and approver sign off and provide a date of completion. On a monthly basis, the document is forwarded to the Department. No supporting documentation is required to be provided as part of the submission. Our review of the OPDIV's submissions and the supporting documentation maintained at the OPDIVs identified inconsistencies in the procedures performed, the reports utilized, and the results provided among the various OPDIVs. Our review of prepared certifications identified that although certain reconciliations were signed off and dated, the reconciliation had not been completed as differences within the reconciliation had not been identified on a timely basis. For example, the OPDIV management certifies to the accuracy of their financial statements submitted through AFS; however, we noted over

ERNST & YOUNG

$1.0 billion in errors, omissions, or unsupported amounts within the OPDIV level statements. Further, we noted that although the financial statements are submitted to OMB on the 21st day after the end of the quarter and we received draft financial statements on October 20, reconciliations were not required to be completed and certified until the end of the month. Finally, we noted that although desk officers have been assigned the responsibility of reviewing specific OPDIV financial reporting, the desk officers do not consistently review the supporting documentation to ensure that the submissions are accurate.

- Accounts Payable—We noted over $23.9 million of old/stale accounts payable transactions that should have been researched and removed. Many of the items were several years old and had not shown activity for at least two years.
- Undelivered Orders—As reported in FY 2008, DHHS does not have adequate controls in place to monitor undelivered orders which represent remaining amounts of obligated funds that have not been delivered or appropriately deobligated. As of September 30, 2009, we noted approximately 90,000 transactions totaling an approximate $1.1 billion which were over two years old without activity. Many of these transactions represented travel, grants, and contracts awaiting close-out. Additionally, for grants, although progress was noted, during our review of FY 2009 grant activity provided from the Payment Management System (PMS) as of March 30, 2009, we noted approximately 644 grant obligations totaling $40.3 million that were dated prior to FY 2002 that had not been closed out. We continue to note that these grants were already beyond a reasonable time frame for close-out. In prior years, a lack of resources was noted as the cause of backlog in closing out expired grants. Management needs to increase emphasis on close-out to reduce the backlog and ensure consistency between PMS and the OPDIVs official subsidiary systems.
- Budgetary Analyses—Within the federal government, the budget is a primary financial planning and control tool. OMB Circular A-11, *Preparation, Submission and Execution of the Budget*, establishes the requirements of budget formulation and execution including requirements related to apportionments, accounting systems to control spending, proper recording of obligations, and closing accounts. For internal control purposes, budgetary monitoring is a key management control that, if implemented correctly, identifies cost overruns and potential material misstatements in a timely fashion. Currently, DHHS is investigating two potential violations of the Anti-Deficiency Act and possibly others as discussed in the Procurement Activities section below. To ensure these violations do not continue, enhanced budgetary monitoring processes are required. Additionally, in our review of the Statement of Budgetary Resources, we compared balances in budgetary accounts to their related proprietary accounts. Based on our review and discussions with management, we noted differences of $1.5 billion that could not be explained.

ERNST & YOUNG

Report on Internal Control
Page 8

- Procurement Activities—During FY 2009, the DHHS Head of Contracting Activity initiated and performed an extensive review across all OPDIVs of its multiple year contracting activities, in an effort to assess compliance with existing Department guidance and Federal Acquisition Regulations applicable to incremental funding of its multiple year contracts and to identify avenues to improve multiple year contracting strategies within the framework of the regulations. The internal review, issued in July 2009, identified significant concerns and indicated that there was a potential pervasive misunderstanding of appropriation laws when acquiring goods and services that could lead to noncompliance with the Federal Acquisitions Regulations or the Anti-Deficiency Act. The report also reported to management that contract funding was not consistent with the current DHHS Acquisition Regulation or appropriations law. In September 2009, upon management's detailed review, a contractor was hired and findings from the report are currently being investigated to determine if reporting or corrective actions are warranted. Based on the latest study, the determination of whether any noncompliance with laws and regulations occurred has not been made.
- Communication and Information Sharing—During our audit, we noted occurrences when ineffective communication and information sharing among the relevant parties inhibited DHHS's ability to timely resolve known issues. For example, the Department became aware of a system related issue that arose in FY 2008, which has a pervasive impact on its processing of invoices and related activities. The system related issue is self correcting but only after all invoices related to the same invoice are received and matched. The Department implemented a detection and correction plan to address the issue; however, neither the issue nor the plan was effectively communicated to the OPDIVs whose financial transactions were impacted. In addition, when certain OPDIVs encountered the issue in its normal financial transactions, the OPDIVs spent considerable amounts of time and effort to resolve the transactions that resulted from the issue even though a solution had been developed approximately a year ago.

Monitoring of Financial Operations

The U.S. GAO's *Standards for Internal Control in the Federal Government* states that "information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities." Further, the standard indicates that financial statement information is needed not only on a periodic basis for external reporting but also on a day-to-day basis to make operating decisions, monitor performance, and allocate resources. Within a decentralized complex organization like DHHS, a single integrated financial system with strong internal controls is required for up-to-date accurate financial information needed for certain decision-making responsibilities. Currently, due to the number of manual correcting entries, evolving internal control, and outdated policies and procedures, accurate information needed for decision-making at all levels of the organization may not be readily available on a day-to-day or even monthly basis as required by FFMIA. Currently, except for the compilation of quarterly

ERNST & YOUNG

financial statements, there is limited available reporting of accurate financial activities at the program, contractor, regional office, OPDIV, and/or consolidated department level. During FY 2009, it is our understanding that certain OPDIVs have moved to a monthly close process; however, full implementation is not expected until FY 2011 with the implementation of the automated reporting process.

<u>Policies and Procedures and Additional Training of Personnel</u>
DHHS's formalized policies and procedures are out of date and may be inconsistent with actual processes taking place. During our internal control documentation and testing phases, we noted that although various internal control processes had been changed or updated, the Department had not completed its updating of procedural manuals or provided sufficient formalized guidance/training to personnel to ensure sufficient knowledge of financial management system/processes or consistency, and adequacy of internal control. For example, we noted that certain policies and procedures, including certain accrual processes, had not been updated since the mid-1980s. Further, we noted additional training on the financial systems was needed to enable DHHS personnel in their ability to access needed information from the system to complete their day-to-day responsibilities—including the preparation of reconciliations, research of differences noted, and the ability to identify and clear older "stale" transactions dating back several years.

It is our understanding that the Department and its OPDIVs are currently updating their procedures and developing further training for their personnel in the use of Oracle and other financial related systems and processes. Further training is expected to include training on Government-wide (including OMB and Treasury), DHHS, and OPDIV level policies and procedures; the use of UFMS and other subsidiary systems; the preparation of financial statements and related analysis and reconciliations; and system security.

<u>CMS Financial Management Analysis Function</u>
Critical financial management responsibilities, for example, reconciliations of Medicare Advantage (Part C) and Prescription Drug (Part D) payments and monitoring of Medicaid expenditures are performed in various program Centers/Offices of CMS. The dispersed nature of the financial management environment requires a high degree of coordination between the financial and program management personnel to ensure the effective operation of the controls. The decentralized nature of the organization results in a significant number of controls being performed at the contractors, regional offices, and other Centers/Offices outside of CMS' Office of Financial Management (OFM). Critical accounting matters identified within the organization require a robust review process, including the documentation of these critical accounting matters through CMS' white paper process. While the white paper process has improved, we noted areas for further improvement in gathering and assessing information from across CMS to aid in enhancing financial management.

Ernst & Young

CMS can improve its analysis processes to develop further robust analytical procedures or measures against benchmarks to monitor and mitigate risks associated with the decentralized nature of CMS operations. CMS performs an analysis of changes in prior year to current year balances; however, this analysis is not extensive nor is it supplemented by additional analyses (e.g., actual expenditures on a monthly, quarterly, or annual basis by program and by contractor compared to prior year periods and expectations, etc.). Although we noted that CMS performs limited financial statement analytical review procedures on a quarterly basis (i.e., changes in current quarter to prior quarter balances), these procedures were not performed and reviewed timely (e.g., the June 30, 2009 quarterly financial statement analytical review was not completed and reviewed until September 25, 2009). The limited analytical procedures performed centrally and circulated within CMS management increase the likelihood that adjustments, which are other than inconsequential to the financial statements, may not be identified and corrected in a timely manner. In addition, errors in the financial statements may not be detected if robust analytical analyses are not performed by the various program Centers/Offices and are not provided timely to OFM.

Consistent with the prior year, we noted that CMS does not perform a claims-level detailed look-back analysis for the Medicaid Entitlement Benefits Due and Payable (EBDP) to determine the reasonableness of the various state calculations of incurred but not reported (i.e., unpaid claims) liability. The Medicaid EBDP is approximately $25.0 billion as of September 30, 2009 and is a significant liability on the financial statements. Currently, CMS does not obtain the Medicaid claims data from the states' systems. Accordingly, CMS is not able to validate its methodology in a manner similar to the Medicare methodology by using a claims-based approach. CMS continues to rely on its historical three-year average to record the Medicaid EBDP without the ability to confirm the reasonableness of its methodology.

All individuals within the organization are responsible for establishing, managing, and maintaining an effective control environment. A good control environment not only ensures accountability but provides oversight and reasonable assurance that the organization's goals are met. The goals may pertain to promoting orderly, economical, efficient, and effective operations, adhering to laws, regulations, and management policies or developing, maintaining, and reporting reliable financial and management information timely. The purpose of the monitoring or review function is to determine whether the controls are adequately designed, properly executed, and effective. During the internal control tests, errors were noted that were not detected by the organization's monitoring and review function, and accordingly, the control was not functioning as designed or intended. The errors identified by our audit procedures at the central office and regional offices and Medicare contractor locations may be summarized as follows: (i) no review or monitoring function was established (identified as a design deficiency); (ii) review or monitoring function was established but was not performed or effective; and (iii) the review or monitoring function was not performed timely. An example of a deficiency for each category includes: (i) no documentation of the execution of the centralized oversight to

ERNST & YOUNG

assess compliance with laws and regulations in connection with periodic financial reporting; (ii) formula or mathematical errors were noted in a specific reconciliation and related supporting documentation that were not identified by the review function; and (iii) the final cost reports for certain cost-based plans were not reviewed timely and the related FY 2009 cost plan settlements were not evaluated or recorded in the financial statements.

CMS Business Partner Risk Management

CMS, as the steward of the Medicare and Medicaid programs' administrative and financial operations, has a fiduciary responsibility to ensure that the program funds are spent in the best interest of the beneficiaries and the American taxpayers. CMS administers an extensive internal control program to protect the CMS' resources from fraud, waste and mismanagement. CMS also relies heavily on third-party contractors as it outsources substantially all the day-to-day operations for its information technology systems, the payment of Medicare and Medicaid fee-for-service claims and the Medicare Advantage (Part C) and Part D Drug programs.

CMS has developed internal controls that help prevent fraud and waste from occurring such as edits in the claims processing systems that attempt to identify and filter inappropriate claims. CMS also has developed internal controls that will help detect fraud and waste that may have occurred. Any strong control environment will have a combination of both prevent and detect controls with a greater emphasis on prevent controls.

While we noted during the current year audit that CMS had both prevent and detect controls in operation, we noted several examples of areas where improvements could be made in the overall control environment. This is especially true of CMS' relationships with its third-party contractors.

During 2007, CMS transferred a majority of the Medicare Secondary Payor recovery process to a single third-party contractor. This contractor is responsible for initiating collection of several hundred million dollars on an annual basis. Although some additional procedures were implemented, we continued to note several instances where internal controls related to this third-party contractor were not designed or operating effectively, including lack of, or an ineffective level of, review and the untimely application of cash receipts.

In addition, the processes designed to prevent errors should also be supplemented by controls and analyses that highlight any material errors that may occur. In this regard, errors or abuses within the Medicare fee-for-service claim data, if material, should be detected in the annual Comprehensive Error Rate Testing (CERT) process, while for Medicaid the Payment Error Rate Measurement (PERM) process can be useful in this regard. Processes to assess accuracy rates as applicable and monitor Parts C and D plans, particularly prescription drug event (PDE) data, continue to evolve, but these monitoring activities also can be useful, and the initial error rate development processes developed by CMS are important steps forward in this regard. To be fully

ERNST & YOUNG

effective in compensating for inherent risks in the programs, the monitoring activities must be well understood, susceptible to replication and highly credible. We reviewed these error analyses and these analyses quantify the challenges that CMS has regarding improper payments. Our audit procedures also consider the audit activities performed by the OIG and others for the Parts C and D programs. Findings, such as timeliness of the plan audits and the accumulation of True-Out-of-Pocket costs (TROOP) and PDE data, are inherent risks of the programs.

In the prior year, the OIG recommended revisions to the error rate review methodology, which were implemented by CMS during fiscal year 2009. Preliminary indications are that the refined process has resulted in higher projected error rates. Similarly, ensuring that a fully reconciled population of claims is susceptible to testing is an important starting point in the development of PERM error rates. The work performed by the OIG in reconciling such populations indicates that further focus on this area is needed.

Statement of Social Insurance (SOSI)

The SOSI for CMS presents a long-term projection of the present value, of over a 75-year time horizon, of the benefits to be paid for the closed and open groups of existing and future participants of the Medicare social insurance programs, less the income to be received from or on behalf of those same individuals. The presentation assumes the programs will continue in their current form under current law, albeit with certain economic assumptions that serve to constrain growth of the programs and imply refinements in response to the burden of the programs on economic activity and observations in the related report of the Board of the Trustees of the Federal Hospital Insurance and Federal Supplementary Medical Insurance Trust Funds (the Trustees Report) that growth as projected will substantially strain the nation.

The presentation in the CMS annual report includes estimates not only of the payroll taxes, premiums, and other contributions to be made directly by the participants but also estimates of general fund contributions on their behalf to help finance the programs for which this funding mechanism exists. In contrast, the presentation included in the consolidated annual financial statements of the U. S. government excludes such intragovernmental transfers. Starting in FY 2006, the SOSI was required to be presented as part of the basic financial statements rather than as Required Supplementary Information as previously presented. As such, the process for preparing the SOSI must comply with appropriate financial reporting internal control requirements established by OMB.

The SOSI models are complex, 75-year projections that contain a high degree of estimation. The lack of robust controls over spreadsheet changes and inputs, and complexity of the models may result in output that varies from management's intentions. We noted the following deficiencies that, if improved, would enhance the reliability and credibility of the SOSI model and process:

- CMS has developed and implemented a change management process over the SOSI model, which applies to significant changes or changes in the methodology of the model. During our testing, we noted that certain changes made to the models were not tracked through the change management process. For example, certain formula changes were made within, and other spreadsheets were removed from, the models and the reasons were not documented.
- The SOSI model is password protected to ensure that only authorized access and changes are made to the analyses within the model. During our testing, we noted that one CGE spreadsheet was not password protected, which could allow unauthorized access and changes to the CGE analysis.
- CMS' policies and procedures require that any input or output data within the SOSI models should be documented to properly understand the flow of the data. During our testing, we noted that the Office of the Actuary (OACT) did not document their methodology and related calculations/estimates for certain assumptions and hard-coded adjustments within the model. In addition, the documentation for the Part C analysis was not completed. This purpose of the documentation is to describe the steps within the process and the source of the input and output data.

Management Corrective Actions

In some cases, the DHHS management has not properly implemented corrective actions for long standing deficiencies in internal controls. For certain deficiencies, including:

- untimely and incomplete Fund Balance with Treasury reconciliation processes;
- cleanup of old "stale" account balances;
- differences and manual adjustments in financial reporting; and
- significant weaknesses surrounding the various information technology systems upon which that DHHS relies heavily for its operations and financial reporting; have been continuously identified and reported to management over the past decade.

This insufficient progress of implementing corrective actions has resulted in limited improvement and continues to impair DHHS's capability to support and report accurate financial information. In other cases, actions to address weaknesses are documented as late as the last week of the fiscal year, with limited or no documentation that the controls were placed in operation during the period under audit. To the extent circumstances such as resource constraints and implementation of new financial systems occur which can lead to multiple years of efforts in addressing issues, some delays may be unavoidable. A more robust process to assess ongoing risks and adopt strategies to mitigate control risks pending overarching solutions can assist in assuring stakeholders that management is systemically addressing control deficiencies and fostering a tone at the top to address audit findings on a timely basis.

* * * * *

Recommendations

We recommend that DHHS continue to develop and refine its financial management systems and processes to improve its accounting, analysis, and oversight of financial management activity. Specifically, we recommend that DHHS:

- Continue to strengthen controls related to its entity-wide structure for account reconciliation, analyses, and oversight by providing more in-depth on-site quality reviews of OPDIV and headquarter financial functions, periodically requesting the supporting documentation to compare to the results communicated, and to improve communication between the various parties so that issues may be identified and resolved in a more timely manner. Further we recommend that the operating divisions allocate adequate resources to perform the required account reconciliations and analyses on a timely basis.
- Continue to improve its financial reporting and internal quality review procedures to reasonably assure that information presented in the interim financial statements and Annual Financial Report are accurate, fully supported, and completed timely and consistent with the requirements of OMB Circular A-136, *Financial Reporting Requirements*, including rigorous use of checklists and enhanced supervisory review processes.
- Continue to improve its process to timely closeout "stale" or old account balances, including undelivered orders, accounts payable, and grants.
- Continue to devise short-term and long-term resolutions to systematic and integration issues that complicate use of the UFMS. DHHS should continue to assess whether systems used to prepare the financial statements are complete and have been sufficiently tested prior to year-end reporting dates.
- Continue to offer updated guidance and training to personnel to ensure specific guidelines are documented as to the source of data, required follow-up with timetables, and documentation retention policies. Further, training should be provided to OPDIV and headquarter personnel to ensure a complete understanding of the financial management system and reports that are available to perform certain tasks.
- Consider moving to a monthly departmental close of financial data to provide for a more timely compilation of accurate data that may be needed for decision-makers at all levels.

Ernst & Young

Report on Internal Control
Page 15

The monthly consolidation of financial statements will be more feasible with management's implementation of Hyperion to consolidate its financial statements, for which initial pilots occurred during FY 2009.

- Improve internal control surrounding manual nonroutine entries, including requiring a log of all manual entries and preparing documentation to support the entry and the approval by upper management.
- Ascertain whether the operating divisions, in conjunction with DHHS, properly track and implement corrective actions to mitigate deficiencies that impair the capability to support and report accurate financial information.
- Complete its analysis of its contracting activities to determine specific weaknesses in the acquisition processes and develop corrective actions to resolve such issues.

Additionally, in regard to CMS, we recommend that CMS continue to develop, enhance, refine, and provide robust analyses over its financial reporting systems and processes. Specifically, CMS should:

- The various program Centers/Offices should provide robust analytical analyses to OFM on a periodic basis (e.g., quarterly) that would be analyzed and reconciled by OFM in connection with the preparation of the quarterly CMS financial reports.
- Establish a process to perform a claims-level detailed look-back analysis on the Medicaid EBDP to determine the reasonableness of the methodology utilized to record the $25.0 billion accrual. One potential method to verify the reasonableness of the Medicaid EBDP balance would be to use the detail claims data from the PERM process to calculate the average days outstanding or sample the largest states and determine if information is available for subsequent analysis.
- Evaluate the monitoring and review function to determine the reason the reviews are not performed effectively. Reinforce the importance of the detect control within the internal control structure, the accountability of the control, and the oversight required to maintain an effective control environment.
- Continue to implement an integrated financial management system for use by Medicare contractors and CMS to promote consistency and reliability in accounting and financial reporting.
- CMS should evaluate its overall directives to third-party contractors to ensure that adequate controls are in place and that appropriate documentation is maintained to support the conduct of those controls.
- Continue the process of enhancing the integrity, improving the process and capturing the benefits of the CERT, PERM, Part C, and Part D error rate development and analysis tools. Error rate results should be developed at a sufficient level of detail to analyze,

ERNST & YOUNG

Report on Internal Control
Page 16

scrutinize, and classify errors and identify anomalies to begin separate investigations or studies of the root causes of the errors and appropriate prevention, mitigation, and recovery plans.

- Critically assess findings from OIG and other reviews of the Parts C and D programs to ensure that the evolving nature of these programs are accompanied by robust internal control processes utilized by CMS to address the inherent risks of these programs. Continue to consider and implement the recommended audit results and modify the processes to hold plan sponsors more accountable for the findings identified. The financial management group should ensure it monitors and maintains oversight over the programs and its activities to identify the appropriate financial statement impact and disclosure.
- Strengthen change management controls to test, review, and document all formulae and spreadsheet changes to the SOSI model. In addition, CMS should verify that all spreadsheets are password protected to avoid unauthorized access or changes.
- Adhere to established policies and procedures to ensure that the SOSI model methodology and related calculations and estimates are consistently documented. Adherence to these policies will ensure that the model is evaluated to verify that the input/output data is appropriate based on the expected results of the data and spreadsheet changes.

Finally, in light of the extraordinary financial crisis that existed in 2008 and continues in 2009, the pattern of advances to Part D drug plans, we believe that CMS should continue to evaluate its risks with respect to all its third-party contractors and providers to ensure that the CMS is appropriately protecting its resources.

Financial Management Information Systems

Many of the business processes that generate information for the financial statements are supported by DHHS information systems. Adequate internal controls over these systems are essential to the confidentiality, integrity, and reliability of critical data while reducing the risk of errors, fraud, and other illegal acts. As part of our assessment of internal controls, we have conducted general control reviews for systems that are relevant to the financial reporting process.

General control review categories are department-wide security management, access controls (physical and logical), configuration management, segregation of duties (SoD), and contingency planning. These categories combined to safeguard data, protect business process application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the department-wide, systems, and business process application levels. GAO Federal Information Systems Controls Audit Manual (FISCAM) dated February 2009 states, "the effectiveness of general controls is a significant factor in determining the

Ernst & Young

Report on Internal Control
Page 17

effectiveness of business process application controls, which are applied at the business process application level. Without effective general controls, business process application controls can generally be rendered ineffective by circumvention or modification."

Our audit included general controls testing for the NIH Center for Information Technology (CIT) and Office of the Secretary (OS) Information Technology Operations (ITO). Our testing noted issues in both the design and the operations of key controls. We noted weaknesses in the following FISCAM review areas:

- Security Management
- Access Control
- Configuration Management
- Segregation of Duties
- Contingency Planning

More broadly within DHHS, a topic of major concern is the lack of remediation of prior year audit findings, with respect to Federal Information Security Management Act (FISMA), some dating back to FY 2006. In addition, the process by which these findings are identified and managed, Plan of Actions and Milestones (POA&M) does not function effectively. For example, many of the prior year audit findings were not recorded in the Security and Privacy Online Reporting Tool (ProSight FISMA).

Because of the pervasive nature of general controls, the cumulative effect of these significant deficiencies represents a material weakness in the overall design and operation of internal controls. DHHS should take a department-wide view in developing a top-down strategy implementing information security programs to drive information security control design and operations in accordance with standards established by DHHS and federal standards such as the National Institute of Standards and Technology (NIST) and OMB. Detailed descriptions of control weaknesses may be found in the management letters issued on information technology general controls and audited applications. The following discusses the summary results by review area.

Security Management

These programs are intended to ensure that security threats are identified, risks are assessed, control objectives are appropriately designed and formulated, relevant control techniques are developed and implemented, and managerial oversight is consistently applied to ensure the overall effectiveness of security measures. Security programs typically include formal policies on how and which sensitive duties should be separated to avoid conflicts of interest. Similarly, policies on background checks during the hiring process are usually stipulated. Department-wide

Ernst & Young

security programs afford management the opportunity to provide appropriate direction and oversight of the design, development, and operation of critical systems controls. Inadequacies in these programs can result in inadequate access controls and software change controls affecting essential, systems-based operations.

"A department-wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Overall policies and plans are developed at the department-wide level. System and application-specific procedures and controls implement the department-wide policy. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources. Through FISMA, Congress requires each federal agency to establish an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those managed by a contractor or other agency," as written in GAO FISCAM dated February 2009. Our procedures identified the following issues:

- **Certification & Accreditation:** For ITO, SSP documentation was found to have not been updated to reflect the current technology environment.
- **Plan of Actions and Milestones (POA&M):** For ITO and CIT, management did not implement an adequate POA&M process to record POA&M in a timely manner and to track and monitor the POA&M to enforce completeness and accuracy; no formal reporting process of the status of weaknesses to management exist.
- **Vulnerability Management:** For ITO, vulnerability assessments are performed; however, there is a lack of effective management of the identified vulnerabilities; some identified vulnerabilities are not tracked within the vulnerability tracking system and a formal process of tracking and monitoring the identified and remediated vulnerabilities does not exist; CIT vulnerability scans were not run for the period under review. Exceptions noted during the vulnerability scans were found to have been closed three months after issues were discovered.
- **Background Investigation:** For ITO, management has not fully implemented an information technology new hire personnel security program; security trainings are not completed by all employees and contractors. For CIT, exceptions were noted for new employee background investigations.

ERNST & YOUNG

Access Control

Access controls ensure that critical systems assets are physically safeguarded and that logical access to sensitive applications, system utilities, and data is granted only when authorized and appropriate. Access controls over operating systems, network components, and communications software are also closely related. These controls help to ensure that only authorized users and computer processes can access sensitive data in an appropriate manner. Weaknesses in such controls can compromise the integrity of sensitive program data and increase the risk that such data may be inappropriately used and/or disclosed. Our procedures identified the following issues:

- **Access Identification & Authentication:** For ITO and CIT, password policies and authentication settings need enhancement.
- **Access Authorization:** For CIT, the annual validation of user security awareness training and account monitoring is inadequately documented to maintain appropriate user access on the network. For ITO, periodic monitoring of administrative access rights needs to be enhanced along with monitoring of idle network accounts.
- **Protect Sensitive System Resources:** For ITO, the infrastructure and application servers have not fully implemented authorization controls.
- **Remote Access:** For ITO and CIT, a significant number of users access the DHHS network using their own personal home computers that lack security controls; no evidence of authorization or reauthorization of remote user accounts.
- **Local Admin Rights:** Some general DHHS users have local administration access rights to their individual computers.
- **Security Monitoring:** For ITO and CIT, various computer platform operating system (Windows, UNIX and mainframe) security logs are not monitored.
- **Penetration Testing:** For CIT and ITO, insufficient security controls are in place to protect access to hosts, web applications, databases, and Windows.

Configuration Management

Configuration management procedures should be established to ensure that critical components of the organization's technology resources have been appropriately identified and are maintained. There should be an integrated process whereby current and future processing demands are measured and provide input to the technology resource acquisition and change process.

- **Maintenance of Configuration Identification:** For ITO and CIT, baseline configurations for the Window and Solaris servers needed updating.

ERNST & YOUNG

Report on Internal Control
Page 20

- **Test, Track & Authorize Changes:** For ITO, testing revealed lack of authorization, testing, deployment, and segregation of duties.
- **Configuration Monitoring: Access Identification & Authentication:** For CIT, procedures have not been developed for monitoring operating systems changes for Windows and UNIX.
- **Software Updates:** For CIT, patch testing revealed missing system updates for the operating system.

Segregation of Duties

Appropriate Segregation of Duties (SoD) policies implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. SoD helps ensure that personnel are performing only authorized duties relevant to their respective jobs and positions.

- **SoD Policies:** For ITO, the change management tool does not enforce SoD; CIT has a security administrator with full mainframe access.
- **SoD Review:** For ITO, review of administrative logs for inappropriate actions are not performed.

Contingency Planning

The process to prevent, mitigate and recover from disruption. The terms "business resumption planning", "disaster recovery planning," and "contingency planning" also may be used in this context; they all concentrate on the recovery aspects of continuity.

- **Document & Develop a Contingency Plan:** For ITO, the GTC contingency plan needs review and update to include critical processing location.
- **Contingency Plan Testing:** For ITO, no testing was performed to support system contingency in the event of a disaster.

Financial Application Specific Concerns

GAO FISCAM states, "business process financial application level controls, commonly referred to as application controls" are those controls over the completeness, accuracy, validity, and confidentiality of transactions, and data during application processing. The effectiveness of application controls is dependent on the effectiveness of DHHS department-wide and general controls. Weaknesses in department-wide and general controls can result in unauthorized changes to business process applications and data that can circumvent or impair the effectiveness of financial application controls. Application controls are divided into the following four control

ERNST & YOUNG

categories:

- **Application general controls (AS)** consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.
- **Business Process controls (BP)** are the automated and/or manual controls applied to business transaction flows. They relate to the completeness, accuracy, validity, and confidentiality of transactions, and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level, and operate over individual transactions or activities across business processes.
- **Interface controls (IN)** consist of those controls over the: i) timely, accurate and complete processing of information between applications, and other feeder and receiving systems on an on-going basis; and ii) complete and accurate migration of clean data during conversion.
- **Data management system controls (DA)** enforce user authentication/authorization, availability of system privileges, data access privileges, application processing hosted within the data management systems, and segregation of duties. Technology includes database management systems, specialized data transport/communications software (often called middleware), data warehouse software and data extraction/reporting software."

As part of our assessment of internal controls, we reviewed the UFMS; NBS; Grants Administration, Tracking and Evaluation System (GATES); HCAS; Enterprise Human Resources and Payroll System (EHRPS); Information for Management, Planning, Analysis, and Coordination (IMPACII); Accounting for Pay System (AFPS); Managing/Accounting Credit Card System (MACCS); AFS; and Commissioned Corps Personnel and Payroll System (CCP). Our testing noted application controls issues in the design and the operations of key controls. We noted weaknesses in all four (4) control categories with significant issues around application level general controls:

- **Application Level General Controls**
    - **Access Authorization/Separation:** For some users, access to key financial systems such as AFPS, EHRP, GATES, HCAS, IMPACII, MACCS, and UFMS and were not appropriately granted, recertified, or removed.
    - **Periodic Account Review:** Privileged users and system administrator account are not being reviewed for AFPS, EHRP, GATES, HCAS, or IMPACII.

ERNST & YOUNG

Report on Internal Control
Page 22

- **Financial System Security Plan:** Security plan documentation is not complete or contains inconsistent language for AFPS, EHRP, GATES, HCAS, IMPACII, NBS, and UFMS.
- **Audit Log Monitoring:** For AFPS, GATES, HCAS, MACCS, and UFMS systems, audit log monitoring procedures were not documented. Further, audit trails that were generated were not monitored.
- **Segregation of Duties:** Access assignments were excessive for AFS, AFPS, EHRP, GATES, HCAS, IMPACII, MACCS, and NBS systems and did not provide an adequate segregation of duties. Assignment conflicts represent instances whereby accesses assigned may have allowed users to perform all phases of transactions without intervention by other users or approvers. In addition, application developers had full access to both development and production systems.
- **User IDs and Passwords:** AFPS, EHRP, HCAS, IMPACII, and UFMS application users shared system IDs or had multiple IDs associated to accounts. Sharing of user IDs eliminates personal accountability for any system activity. Number of other systems password configurations does not comply with DHHS standards.
- **Change Management:** Change management procedures for AFPS, EHRP, GATES, HCAS, IMPACII, NBS, and UFMS were insufficient to ensure only properly authorized changes were implemented into production systems.
- **Security Management:** Documentation to support corrective actions is not complete or not provided for the POA&M for AFPS, EHRP, GATES, and HCAS.
- **Certification & Accreditation:** Compliance with the C&A policies and procedures has not been formalized for HCAS. Documentation is not complete or contains inconsistent language for IMPACCII and NBS.
- **Contingency Management:** Contingency plans for AFPS, EHRP, and GATES could be enhanced. Plans did not include effective scenarios to address business resumption or address effective testing.
- **Application Limitations:** No evidence was provided to demonstrate functions and authorities of privileged accounts and system administrator account for AFPS and EHRP.

- **Business Process Controls**
  - **Error Handling Activities:** Procedures do not exist in that the Global Error Handler is monitored and that transactions held in error are reviewed and processed timely.

ERNST & YOUNG

Report on Internal Control
Page 23

- **Interface Controls**
  - **System Interfaces**: For GATES and UFMS systems, consistent policies and procedures do not exist over these interfaces to ensure that necessary inputs are processed, control logs are monitored and reviewed with issues adequately followed up, and errors held in rejection files during processing are resolved.
- **Data Management System Control**
  - **Configuration Controls:** EHRP, IMPACII, NBS, and UFMS Oracle financial systems settings for the selected databases and operating systems are not optimized to provide a secure computing environment.
  - **Key Management Report:** Management does not regularly or consistently review output reports detailing the interface activity to the financial system.

Recommendations

To provide a secure computing environment for critical applications throughout all the operating divisions, DHHS should:

- Improve overall security management program to update documentation and review of C&A, Plan of Action and Milestones, vulnerability management, and background investigations.
- Develop safeguards around access controls to limit unauthorized access to system assets, including controls around remote access and penetration testing.
- Develop and implement effective tools, policies, and procedures to review platform security settings for all components, on a continuing basis.
- Develop overall HHS platform configuration security standards for all operating platforms and databases, following the guidance issued by NIST, for all components.
- Continue to test, track, and authorize all system changes planned for release into the live environment.
- Continue to review segregation of duties log to ensure less privilege is granted to users with significant security and change management responsibilities.
- Review and update contingency plans for the applications, critical processing locations, and ensure proper testing is performed.
- Continue to review user access to critical financial applications to ensure access is properly granted, recertified, and removed on a periodic basis.
- Maintain updated system security plans for all critical applications and validate that information is accurate.

Ernst & Young

Report on Internal Control
Page 24

- Develop an effective data management program to establish optimal security settings on the database.

CMS Specific Financial Management System

Business Environment Overview

A substantial portion of CMS' data and claims processing is performed by geographically dispersed contractors. Because of CMS' enormous size and decentralized nature, it relies on extensive information systems operations. These systems, resident at the CMS Central Office and Medicare contractor sites, are designed to assure consistency in administration of the Medicare program, in addition to processing, accounting for, and reporting on Medicare expenditures. Internal controls over these operations are essential to ensure the integrity, confidentiality, and reliability of the Medicare data and to reduce the risk of errors, fraud, and other illegal acts.

Controls over information systems should be augmented by controls designed to detect, on a timely basis, errors that have occurred, and therefore mitigate the potential impact of imperfections in the prevent controls. Generally, detect controls are accomplished by means of robust manual, financial reporting, and periodic monitoring controls. As noted above under the caption, Financial Reporting Systems, Analyses and Oversight, improvements are needed in the detect controls at CMS. This weakness in detect controls increases the importance of a thorough and closely followed system of IT security.

The contracts between CMS and its contractors that process or support the processing of Medicare fee-for-service claims include provisions requiring the adherence to security standards described in a series of documents, the cornerstone of which is the Business Partners Systems Security Manual (BPSSM). The specific security standards followed at each contractor are to be documented in their System Security Plan (SSP). Contractors are also required to periodically (at least annually) test and certify their systems for operation. Recent restructuring has centralized data processing services in Enterprise Data Centers (EDCs). CMS is transitioning the business function of claims processing to Medicare Administrative Contractors (MACs) who are responsible for processing Hospital Insurance (HI) and Supplemental Medical Insurance (SMI) claims activity for their assigned jurisdictions. Prior to the restructuring, claims processing contractors were responsible for both the data processing and the claims processing function. CMS has contractually required contractors who are designated as MACs to obtain Statement on Auditing Standards (SAS) No. 70 reports to document compliance with the BPSSM and the contractor's SSP. The EDCs, fiscal intermediaries, carriers, and software maintainers are monitored by CMS through annual reviews using Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Internal Control, which provides updated

ERNST & YOUNG

Report on Internal Control
Page 25

internal control standards and specific requirements for conducting management's assessment of the effectiveness of internal control over financial reporting.

We performed our information systems general and application control procedures at six MACs, and general control procedures at the Baltimore Data Center at the CMS Central Office and two contractor Enterprise Data Centers (collectively EDCs). These three EDCs now provide the majority of the electronic data processing and hosting operations to accommodate fee-for-service claims submitted by hospitals, physicians, and other providers. The applications reviewed included the Fiscal Intermediary Shared System (FISS), the ViPS Medicare System (VMS), the Multi-Carrier System (MCS) and the Common Working File (CWF) (collectively, "shared systems"). At the CMS Central Office, we performed procedures over financial applications, including Financial Accounting Control System (FACS), HIGLAS and Medicare Advantage Prescription Drug System (MARx).

While efforts have been made to remediate the prior year findings, we have identified the following similar areas where information technology controls need to be improved.

CMS Oversight of Information Security

CMS has developed processes and policies for supporting their Information Security Program in accordance with NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* and NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. These policies are documented in the CMS BPSSM, CMS Information Security (IS) Certification and Accreditation (C&A) Program Procedures, and SSP Methodology that present the CMS requirements for information security. CMS embeds compliance with these overarching criteria in its formal policies and in contracts with the entities executing claims processing and other federal information system responsibilities on its behalf, while providing flexibility to the participants in meeting the objectives. A combination of such contractual requirements, contractor self assessments, selected third-party reviews, and follow-up processes for remediation of prior findings provide principal monitoring and oversight information for CMS. However, these processes have not been fully effective in identifying information security issues or ensuring that they are timely remediated by contractors.

During our audit activities as part of the Chief Financial Officer financial audit, we identified weaknesses in information security oversight, including:

- CMS did not ensure that user roles and responsibilities were clearly defined. We noted this weakness at one EDC and two MACs where the MACs and the EDC have not formally documented the coordination of their user access roles. The BPSSM requires that business owners periodically review system access authorization listings and determine whether they remain appropriate. The lack of clearly defined user roles and

ERNST & YOUNG

responsibilities and coordination within the organization (for example, between the EDC and MACs as noted above) has resulted in insufficient reviews by the EDC and MACs of access and situations where users were granted excessive or conflicting access to the shared systems, as illustrated by the examples in section II below.

- We noted a lack of periodic review of user access over the mainframe and shared systems at one EDC and four MACS. Periodic review of access is essential to ensure that access is appropriate and still required.
- CMS did not ensure the default passwords for several system accounts on a mission critical database were changed since its implementation in 2006. This resulted in vulnerabilities that could have allowed unauthorized users access to unencrypted personally identifiable information (PII) and sensitive user data.
- During our security assessment, we noted that certain MACs did not implement all of the system settings as required by CMS to secure their information systems. As a result, we were able exploit vulnerabilities at two MACs to gain access to sensitive user data.
- Backup magnetic tapes managed by EDCs contained unencrypted PII (Medicare claims data). CMS is not following the DHHS) Standard for Encryption (DHHS Standard 2008-0007.001S, dated December 23, 2008) that "all portable media that contains sensitive information shall be encrypted" and OMB Memorandum No. M-06-16, *Protection of Sensitive Agency Information*. CMS did not receive a waiver from OMB related to this issue.
- The EDCs did not implement all mainframe security settings as required by CMS to secure their information systems. In addition, we noted an excessive number of users (150 users at one EDC and 300 users at another EDC) who also had excessive system access to the mainframe. For example, the 150 users at one EDC were granted elevated security administrative privileges even though they only required limited access for resetting passwords. This access could allow users unauthorized access to Medicare data.
- Noncompliance with CMS security standards were not reported to CMS. At one MAC, we noted that 8 out of 39 critical security settings tested were not in compliance with the established standard. Examples of these exceptions include dormant accounts not removed, privileged accounts not restricted based on job function and hard drive not encrypted.

The aggregation of these information technology vulnerabilities increases the risk of misappropriation of funds or unauthorized disclosure of PII. The risk of the vulnerabilities is magnified by the insufficient oversight and monitoring of the information technology controls by CMS management.

ERNST & YOUNG

Report on Internal Control
Page 27

Access to Financial Systems

Access controls ensure that critical system assets are physically protected from unauthorized access and logical controls provide assurance that only authorized personnel are granted access to data and programs maintained on systems; such controls include monitoring of security events for proper assessment and remediation.

- The application security design for MCS did not support appropriate segregation of duties between security administrators and computer support activities or business functions. This access allows security administrative privileges to Medicare (Part B) claims processing at all contractors using MCS. Specifically, we noted that 24 business users at 2 MACs and 28 help desk users at another MAC were granted excessive security administrative privileges even though they only required limited access (resetting passwords).
- We noted that inappropriate and excessive access was granted to 72 users at two MACs. Specifically, access control privileges were granted that provide users with update and delete access to production data files although the users only needed update access. At one MAC, we noted that users were application developers and at another MAC the users were business function users. This access would allow users to create and also delete production files (Medicare data files).
- We noted that access was granted to four FISS users resulting in inappropriate segregation of duties at two MACs. The lack of segregation of duties may result in erroneous Medicare (Part A) claims processing.
- Segregation of duties conflicts also exist at the CMS Central Office between the business function and the information security administration function of the Office of Financial Management's (OFM) Financial Accounting and Control System (FACS) general ledger-related application. CMS OFM has assigned personnel to function as system and security administrators, who are able to grant access to the FACS general ledger application, and process transactions. A similar condition was noted last year.

These security weaknesses could allow internal users to access and update financial systems, program parameters, and data without proper authorization.

Control over Application Configuration Management

Configuration management depends on the consistent application of change management processes and policies to automated computer systems in order to ensure the integrity and security of financial and claims data. CMS has contracted with software maintainers to provide software development and support of the shared systems used to process Medicare claims.

ERNST & YOUNG

The review of change management for Central Office financial applications identified inconsistencies in the processes and methods used for mainframe applications. The infrastructure change management process is centralized and uses a change configuration board to manage changes across the enterprise. However, Central Office mainframe application program changes are not part of the enterprise change process and rely on individual change processes within each business function. During the audit, the following weaknesses were noted:

- NIST requires a change management control and tracking process to ensure that all phases of the change control process (e.g., justification for change, approval, implementation, and test of the change) are satisfied. We noted 9 Central Office Medicare or financial applications that do not have an adequate change control process to manage configuration changes. For example, we tested 47 changes to the MARx and MBD systems and noted that there was no evidence of approval and no evidence of testing for 40 and 18, respectively, of the changes. In addition, we noted that monitoring of configuration changes for HIGLAS was not being performed. Specifically, the HIGLAS production environment is not reviewed and compared with approved changes to validate that only authorized and appropriate changes are made to the system. As a result of these weaknesses, unauthorized or unapproved changes may be implemented which could lead to inaccurate Medicare payments.
- We noted that segregation of duties conflicts existed with the change management software used to track changes in Central Office Medicare applications. We identified one individual each in five different Medicare applications where they were able to develop and also approve system changes. As a result of these weaknesses, unauthorized or unapproved changes may be implemented which could lead to inaccurate Medicare payments.

Software maintainers provide services for the shared systems that include system development, system documentation, training, and unit testing. The MACs' responsibilities over the shared systems include configuration of edits, customization of Automated Adjudication Software (AAS or script) and administration of security. During the audit, the following weaknesses were identified:

- In 2008, CMS management established formal control processes for the use of AAS, including methods to establish, test, peer review, and approve AAS programs prior to their use. Our testing noted issues at five MACs regarding compliance with these processes for AAS. More than 25% of the tested AAS was not documented by four MACs as to the business purpose and planned date to activate and/or deactivate the script. In addition, we noted that scripts created several years ago and scripts inherited from previous claims processors have not been tested or documented as to the business purpose. Also, at one MAC, we noted five users were able to develop and write the scripts and also were able to activate the scripts, which results in a lack of segregation of duties. Finally, we noted that there is no CMS requirement for the MACs to recertify the AAS on a periodic basis.

AAS programs provide a powerful tool to process large volumes of Medicare claims rapidly, without human intervention. The use of such programs, without the enforcement of strong controls, could result in inconsistent, uncertain, or improper Medicare payments. While new AAS is subject to an improved process, this condition has not been resolved for AAS programs from prior fiscal years.

Recommendations

CMS has made efforts to remediate specific information security and control weaknesses. CMS management should continue its efforts to appropriately coordinate and direct the information security program administered by Office of Information Services (OIS) for all of the affected information system processing activities. Such activities should include continuous monitoring of the information security program at the Central Office and contractor sites.

Specifically as part of the program improvements, CMS should:

- Improve its process for monitoring and managing its contractors through additional communication, coordination, and assignment of clear responsibilities for processing Medicare data and adhering to CMS' policies.
- Provide specific direction to the MACs and EDCs as to their roles and responsibilities for performing information security functions and validate appropriate segregation of duties.
- Enforce the requirement that user access reviews are performed periodically and in a timely manner.
- Ensure the encryption of personally identifiable information on its information systems, including portable devices, as required by OMB and DHHS to protect sensitive data against unauthorized disclosure.
- Strengthen its information technology systems by ensuring that the system and security settings have been implemented, monitored for compliance, and identified errors are corrected on a timely basis.
- Ensure that appropriate segregation of duties is established in all systems that support Medicare and financial processing to prevent excessive or inappropriate access. In addition, access to all systems should be periodically reviewed to ensure that access remains appropriate and no incompatible duties exist.
- Move the FACS application security administration process and configuration management process from personnel within OFM to OIS. CMS has continued to use its

ERNST & YOUNG

existing process for supporting FACS, augmented by what it believes to be compensating manual controls to review activity. Pending replacement of FACS, we suggest CMS continue to periodically reassess and confirm this decision at senior levels and remain vigilant as to the risks posed by the segregation of duties issues noted. OIS has an established user security administration process as well as an established configuration management process. CMS would strengthen the internal controls by utilizing these OIS processes for FACS. In addition, CMS should ensure that segregation of duties are appropriately addressed in the implementation of the new accounting system.

- Require all changes to Medicare and financial applications to follow NIST guidance including reviewing and approving all changes. All phases of the change management process should be documented and retained.
- Ensure that all AAS programs are documented as to their business purpose and tested prior to being installed at a MAC. The scripts should be periodically tested and recertified as to business need and any prior year script should be properly validated.

CMS should continue its efforts to increase contractor compliance by enhancing controls through oversight activities and proactively monitoring contractor compliance with security settings and related directives for data access control and application programs. In addition, CMS management should validate the implementation of the requirements and standards by the contractors, review and evaluate the deviations noted, document the conclusions and, if acceptable, approve the documentation.

The combination of the need to improve CMS oversight of its contractors, prevent inappropriate or excessive access and incompatible duties to Medicare and financial systems, and validate that scripts are functioning as intended has resulted in more than a reasonable possibility that a material misstatement of the financial statements will not be prevented, detected or corrected on a timely basis by CMS' internal controls. Accordingly, if the internal controls associated with the noted weaknesses are not functioning as intended, this may result in inconsistent and uncertain claims processing that could lead to inaccurate Medicare payments.

ERNST & YOUNG

Report on Internal Control
Page 31

STATUS OF PRIOR YEAR FINDINGS

In the reports on the results of the FY 2008 audit of the DHHS financial statements, a number of issues were raised relating to internal control. The chart below summarizes the current status of the prior year items:

Material Weaknesses		
Issue Area	**Summary Control Issue**	**FY 2009 Status**
Financial Reporting Systems, Analyses, and Oversight	• Lack of Integrated Financial Management System • Financial Analysis and Oversight	Repeat Condition
Financial Management Information Systems	• Security Management • Access Control • Financial Application Specific Concerns	Repeat Condition
	Significant Deficiency	
Statement of Social Insurance	• Lack of robust automated controls over spreadsheet changes and inputs	Repeat Condition; summarized into *Financial Reporting Systems, Analyses, and Oversight*

We have reviewed our findings and recommendations with DHHS management. Management generally concurs with our findings and recommendations and will provide a corrective action plan to address the findings identified in this report. We did not audit DHHS's response and accordingly, we express no opinion on it.

This report is intended solely for the information and use of the management and the OIG of DHHS, OMB, GAO, and Congress. The report is not intended to be and should not be used by anyone other than these specified parties.

Ernst + Young LLP

November 10, 2009

ERNST & YOUNG

Ernst & Young LLP
8484 Westpark Drive
McLean, VA 22102

Tel: 703-747-1000
www.ey.com

Report on Compliance with Laws and Regulations

To the Secretary and the Inspector General
of the U.S. Department of Health and Human Services

We have audited the financial statements of the U.S. Department of Health and Human Services (DHHS) as of and for the year ended September 30, 2009, and the statement of social insurance as of January 1, 2009, and have issued our report thereon dated November 10, 2009. We conducted our audit in accordance with auditing standards generally accepted in the United States, the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended.

The management of DHHS is responsible for complying with laws and regulations applicable to DHHS. As part of obtaining reasonable assurance about whether DHHS's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts, and certain other laws and regulations specified in OMB Bulletin No. 07-04, as amended, including the requirements referred to in the Federal Financial Management Improvement Act of 1996 (FFMIA). We limited our tests of compliance to these provisions, and we did not test compliance with all laws and regulations applicable to DHHS.

The results of our tests of compliance with the laws and regulations described in the second paragraph of this report disclosed instances of noncompliance with the following laws and regulations or other matters that are required to be reported under *Government Auditing Standards* and OMB Bulletin No. 07-04, as amended. DHHS's management is currently investigating whether it violated certain provisions of the Anti-Deficiency Act (P.L. 101-508 and OMB Circular A-11). Additionally, DHHS management is currently investigating whether it violated certain provisions of the Federal Acquisition Regulations.

Finally, the Improper Payments Information Act (IPIA) of 2002 requires federal agencies to identify the program and activities that may be susceptible to significant improper payments and estimate the amount of the improper payments. While DHHS is not in full compliance with the requirements of IPIA, it has developed and reported error rates for each of its seven high-risk programs, or components of such programs. DHHS continues its efforts to fully implement IPIA and OMB's implementing regulation.

ERNST & YOUNG

Report on Compliance with Laws and Regulations
Page 2

Under FFMIA, we are required to report whether DHHS's financial management systems substantially comply with federal financial management systems requirements, applicable federal accounting standards, and the United States Standard General Ledger (USSGL) at the transaction level. To meet this requirement, we performed tests of compliance with FFMIA Section 803(a) requirements. The results of our tests disclosed instances in which DHHS's financial management systems did not substantially comply with certain requirements as discussed above. We have identified the following instances of noncompliance:

- Certain subsidiary systems are not integrated with the Unified Financial Management System (UFMS) and are not complemented by sufficient manual preventative and detective type controls. For example, although operational at some of the Medicare Contractors, DHHS has not yet completed the implementation of the HIGLAS general ledger system. Additionally, manual key input continues to be required for each Operation Division (OPDIV) to upload trial balances into the Automated Financial System for consolidation in preparation of the departmental consolidated financial statements. Further, certain OPDIV-level reconciliations/analyses were not performed on a timely basis.

- During fiscal year 2009, hundreds of manual journal vouchers were required to be recorded in UFMS to post certain types of transactions—including budgetary and proprietary, not currently configured correctly within UFMS and for the purpose of developing quarterly financial statements.

- Reviews of general and application controls over financial management systems identified certain departures from requirements specified in OMB Circulars A-127, *Financial Management Systems*, and A-130, *Management of Federal Information Resources*. Additionally, the Office of Inspector General (OIG) identified certain issues, including access control deficiencies related to systems as part of its Federal Information Security Management Act and other OIG engagements. Finally, DHHS management has identified certain weaknesses within its information technology general and application controls during its assessment of corrective action status and its OMB A-123 processes.

* * * * *

Ernst & Young

Report on Compliance with Laws and Regulations
Page 3

Our Report on Internal Control dated November 10, 2009, includes additional information related to the financial management systems that were found not to comply with the requirements, relevant facts pertaining to the noncompliance to FFMIA, and our recommendations related to the specific issues presented. It is our understanding that management agrees with the facts as presented and that relevant comments from DHHS's management responsible for addressing the noncompliance are provided as an attachment to its report. We did not audit management's comments and accordingly, we express no opinion on them. Additionally, DHHS is updating its agency-wide corrective action plan to address FFMIA and other financial management issues.

Providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit, and accordingly, we do not express such an opinion.

This report is intended solely for the information and use of management and the OIG of the DHHS, OMB, and Congress and is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

November 10, 2009

[Page Intentionally Left Blank]

DEPARTMENT'S RESPONSE TO THE AUDIT

Date: November 10, 2009

To: Daniel R. Levinson, Inspector General

From: Richard J. Turman, Acting Assistant Secretary for Financial Resources and Chief Financial Officer

Subject: FY 2009 Financial Statement Audit

We would like to thank the Office of Inspector General and your contractors, Ernst & Young LLP for your efforts on our behalf. We appreciate the professionalism exhibited by your staff and contractors during this significant effort. We appreciate the opportunity to comment on the draft reports.

We concur with the findings in the *Report on Internal Control* and *Compliance with Laws and Regulations*, to be included in our *FY 2009 Agency Financial Report*. In response to these reports, we will prepare corrective action plans to address the findings within the next 60 days.

HHS management is committed to working toward resolving these challenges and we look forward to continued collaboration with the OIG to improve the health and well-being of the American people through improved stewardship of taxpayer funds.

[Page Intentionally Left Blank]

Financial Statements and Notes

[Page Intentionally Left Blank]

FINANCIAL STATEMENTS

CONSOLIDATED BALANCE SHEETS
As of September 30, 2009 and 2008
(In Millions)

	2009	2008
Assets (Note 2)		
Intragovernmental		
Fund Balance with Treasury (Note 3)	$ 161,962	$ 124,280
Investments, Net (Note 4)	381,116	385,397
Accounts Receivable, Net (Note 5)	913	880
Other (Note 8)	92	92
Total Intragovernmental	544,083	510,649
Accounts Receivable, Net (Note 5)	5,504	7,419
Cash and Other Monetary Assets (Note 1)	357	354
Inventory and Related Property, Net (Note 6)	5,604	4,603
General Property, Plant & Equipment, Net (Note 7)	5,047	5,011
Other (Note 8)	2,185	1,235
Total Assets	**$ 562,780**	**$ 529,271**
Stewardship PP&E (Note 1)		
Liabilities (Note 9)		
Intragovernmental		
Accounts Payable	$ 566	$ 406
Accrued Payroll and Benefits	111	105
Other (Note 13)	1,071	1,057
Total Intragovernmental	1,748	1,568
Accounts Payable	554	633
Entitlement Benefits Due and Payable (Note 10)	72,218	65,851
Accrued Grant Liability (Note 12)	4,040	3,878
Federal Employee & Veterans' Benefits (Note 11)	9,690	8,742
Contingencies & Commitments (Note 18)	4,048	3,782
Accrued Payroll & Benefits	851	784
Other (Note 13)	1,218	1,356
Total Liabilities	**94,367**	**86,594**
Net Position		
Unexpended Appropriations - Earmarked funds	3,492	12,172
Unexpended Appropriations - Other funds	124,037	81,350
Unexpended Appropriations, Total	127,529	93,522
Cumulative Results of Operations - Earmarked funds	336,811	346,287
Cumulative Results of Operations - Other funds	4,073	2,868
Cumulative Results of Operations, Total	340,884	349,155
Total Net Position	**468,413**	**442,677**
Total Liabilities & Net Position	**$ 562,780**	**$ 529,271**

The accompanying "Notes to the Financial Statements" are an integral part of these statements.

CONSOLIDATED STATEMENTS OF NET COST
For the Years Ended September 30, 2009 and 2008
(In Millions)

	2009	2008
Responsibility Segments		
Centers for Medicare and Medicaid Services (CMS)		
Gross Cost	$ 749,004	$ 657,910
Exchange Revenue (Notes 15 and 16)	(57,294)	(54,071)
CMS Net Cost of Operations	691,710	603,839
Other Segments:		
Administration for Children and Families (ACF)	52,326	48,545
Administration on Aging (AoA)	1,441	1,398
Agency for Healthcare Research and Quality (AHRQ)	(55)	(59)
Centers for Disease Control and Prevention (CDC)	9,274	8,643
Food and Drug Administration (FDA)	2,629	2,127
Health Resources and Services Administration (HRSA)	7,314	7,053
Indian Health Service (IHS)	5,225	4,415
National Institutes of Health (NIH)	30,369	29,776
Office of the Secretary (OS)	2,341	2,234
Program Support Center (PSC)	1,650	1,086
Substance Abuse and Mental Health Services Administration (SAMHSA	3,501	3,163
Other Segments Gross Cost of Operations	116,015	108,381
Exchange Revenue (Notes 15 and 16)	(3,820)	(3,074)
Other Segments Net Cost of Operations	112,195	105,307
Net Cost of Operations	**$ 803,905**	**$ 709,146**

The accompanying "Notes to the Financial Statements" are an integral part of these statements.

CONSOLIDATED STATEMENT OF CHANGES IN NET POSITION
For the Year Ended September 30, 2009
(In Millions)

	2009			
	Earmarked Funds	All Other Funds	Eliminations	Consolidated Total
Cumulative Results of Operations				
Beginning Balances	$ 346,287	$ 2,868	$ -	$ 349,155
Budgetary Financing Sources				
Appropriations Used	209,273	373,868	-	583,141
Nonexchange Revenue				
Non-exchange Revenue - Tax Revenue	194,330	-	-	194,330
Non-exchange Revenue - Investment Revenue	18,686	1	-	18,687
Non-exchange Revenue - Other	503	(9)	(127)	367
Donations and Forfeitures of Cash and Cash Equivalents	128	3	-	131
Transfers-in/out Without Reimbursement	(2,918)	1,465	4	(1,449)
Other Financing Sources (Non-Exchange)				
Donations and Forfeitures of Property	-	5	-	5
Transfers-in/out Without Reimbursement (+/-)	-	9	(2)	7
Imputed Financing	32	498	(105)	425
Other (+/-)	-	(10)	-	(10)
Total Financing Sources	420,034	375,830	(230)	795,634
Net Cost of Operations (+/-)	429,510	374,625	(230)	803,905
Net Change	(9,476)	1,205	-	(8,271)
Cumulative Results of Operations	336,811	4,073	-	340,884
Unexpended Appropriations				
Beginning Balances	12,172	81,350	-	93,522
Budgetary Financing Sources				
Appropriations Received	213,023	431,868	-	644,891
Appropriations Transferred in/out	-	1,854	-	1,854
Other Adjustments	(12,430)	(17,167)	-	(29,597)
Appropriations Used	(209,273)	(373,868)	-	(583,141)
Total Budgetary Financing Sources	(8,680)	42,687	-	34,007
Total Unexpended Appropriations	3,492	124,037	-	127,529
Net Position	$ 340,303	$ 128,110	$ -	$ 468,413

The accompanying "Notes to the Financial Statements" are an integral part of these statements.

CONSOLIDATED STATEMENT OF CHANGES IN NET POSITION
For the Year Ended September 30, 2008
(In Millions)

	2008			
	Earmarked Funds	All Other Funds	Eliminations	Consolidated Total
Cumulative Results of Operations				
Beginning Balances	$ 332,966	$ 1,230	$ -	$ 334,196
Budgetary Financing Sources				
Appropriations Used	193,008	314,749	-	507,757
Nonexchange Revenue				
Non-exchange Revenue - Tax Revenue	197,426	-	-	197,426
Non-exchange Revenue - Investment Revenue	19,241	-	-	19,241
Non-exchange Revenue - Other	569	33	36	638
Donations and Forfeitures of Cash and Cash Equivalents	50	5	-	55
Transfers-in/out Without Reimbursement	(2,663)	1,338	-	(1,325)
Other Financing Sources (Non-Exchange)				
Donations and Forfeitures of Property	-	4	-	4
Transfers-in/out Without Reimbursement (+/-)	(1)	5	(3)	1
Imputed Financing	25	399	(126)	298
Other (+/-)	-	10	-	10
Total Financing Sources	407,655	316,543	(93)	724,105
Net Cost of Operations (+/-)	394,334	314,905	(93)	709,146
Net Change	13,321	1,638	-	14,959
Cumulative Results of Operations	**346,287**	**2,868**	**-**	**349,155**
Unexpended Appropriations				
Beginning Balances	8,887	78,830	-	87,717
Budgetary Financing Sources				
Appropriations Received	205,320	318,130	-	523,450
Appropriations Transferred in/out	(4)	2,089	-	2,085
Other Adjustments	(9,023)	(2,950)	-	(11,973)
Appropriations Used	(193,008)	(314,749)	-	(507,757)
Total Budgetary Financing Sources	3,285	2,520	-	5,805
Total Unexpended Appropriations	12,172	81,350	-	93,522
Net Position	**$ 358,459**	**$ 84,218**	**$ -**	**$ 442,677**

The accompanying "Notes to the Financial Statements" are an integral part of these statements.

COMBINED STATEMENTS OF BUDGETARY RESOURCES
For the Years Ended September 30, 2009 and 2008
(In Millions)

	2009 Budgetary	2009 Non-Budgetary Credit Program Financing Accounts	2008 Budgetary	2008 Non-Budgetary Credit Program Financing Accounts
Budgetary Resources				
Unobligated Balance, Brought Forward, October 1	$ 34,349	$ 95	$ 24,104	$ 145
Recoveries of Prior Year Unpaid Obligations				
Actual	12,719	-	14,969	-
Anticipated	-	-	-	-
Budget Authority				
Appropriation	1,153,357	1	1,004,447	1
Borrowing Authority				
Spending Authority from Offsetting Collections		2		
Collected	10,449	19	12,192	51
Change in Receivables from Federal Sources	(263)	-	(177)	-
Change in Unfilled Customer Orders				
Advance Received	154	-	(106)	-
Without Advance from Federal Sources	(766)	-	297	-
Anticipated for rest of year, Without Advances	-	-	-	
Previously Unavailable	306	-	-	
Expenditure Transfers from Trust Funds				
Actual	3,512	-	3,521	-
Change in Receivables from Trust Funds	515	-	179	-
Anticipated	-	-	-	-
Subtotal	1,167,264	22	1,020,353	52
Nonexpenditure Transfers, Net, Anticipated and Actual	2,100	-	2,259	-
Temporarily not available pursuant to Public Law	(1,515)	-	(16,416)	-
Permanently not available (-)	(29,731)	-	(12,141)	(45)
Total Budgetary Resources	$ 1,185,186	$ 117	$ 1,033,128	$ 152
Status of Budgetary Resources				
Obligations Incurred				
Direct	$ 1,127,560	$ 44	$ 991,979	$ 56
Reimbursable	7,321	-	6,800	1
Subtotal	1,134,881	44	998,779	57
Unobligated Balances Available				
Apportioned	40,647	72	25,893	63
Exempt from Apportionment	389	-	427	-
Subtotal	41,036	72	26,320	63
Unobligated Balances Not Available	9,269	1	8,029	32
Total Status of Budgetary Resources	$ 1,185,186	$ 117	$ 1,033,128	$ 152
Change in Obligated Balance				
Obligated Balance, Net				
Unpaid Obligations, brought forward, October 1	$ 145,222	$ -	$ 142,248	$ -
Uncollected Customer Payments from Federal Sources, brought forward, October 1	(7,192)	-	(6,893)	-
Total Unpaid Obligated Balance, Net	138,030	-	135,355	-
Obligations Incurred Net	1,134,881	44	998,779	57
Gross Outlays	(1,095,645)	(44)	(980,841)	(57)
Obligated Balance Transferred, Net				
Actual Transfers, Unpaid Obligations	-	-	5	-
Total Unpaid Obligated Balance Transferred, Net	-	-	5	-
Recoveries of Prior Year Unpaid Obligations, Actual	(12,719)	-	(14,969)	-
Change in Uncollected Customer Payments from Federal Sources	514	-	(299)	-
Obligated Balance, Net, end of period				
Unpaid Obligations	171,739		145,222	-
Uncollected Customer Payments from Federal Sources	(6,678)	-	(7,192)	-
Total, Unpaid Obligated Balance, Net, end of period	165,061		138,030	-
Net Outlays				
Gross Outlays	$ 1,095,645	$ 44	$ 980,841	$ 57
Offsetting Collections	(14,115)	(19)	(15,607)	(51)
Distributed Offsetting Receipts	(284,264)	(28)	(264,186)	(44)
Net Outlays	**$ 797,266**	**$ (3)**	**$ 701,048**	**$ (38)**

The accompanying "Notes to the Financial Statements" are an integral part of these statements.

STATEMENTS OF SOCIAL INSURANCE

75-Year Projection as of January 1, 2009 and Prior Base Years

(In Billions)

		Estimates From Prior Years			
	2009	**2008**	**2007**	**2006**	**2005** unaudited
Actuarial present value for the 75-year projection period of estimated future income (excluding interest) received from or on behalf of: (Notes 26, and 27)					
Current participants who, in the starting year of the projection period:					
Have not yet attained eligibility age					
HI	$6,348	$6,320	$5,975	$5,685	$5,064
SMI Part B	16,323	14,932	12,112	12,446	11,477
SMI Part D	6,144	6,527	7,285	7,366	7,895
Have attained eligibility age (age 65 and over)					
HI	209	202	178	192	162
SMI Part B	1,924	1,785	1,648	1,606	1,436
SMI Part D	595	581	746	750	817
Those expected to become participants					
HI	5,451	5,361	4,870	4,767	4,209
SMI Part B	4,909	4,480	4,460	3,562	3,658
SMI Part D	2,632	2,856	2,735	2,134	2,522
All current and future participants:					
HI	12,008	11,883	11,023	10,644	9,435
SMI Part B	23,156	21,197	18,221	17,613	16,571
SMI Part D	9,371	9,964	10,766	10,250	11,233
Actuarial present value for the 75-year projection period of estimated future expenditures for or on behalf of: (Notes 26, and 27)					
Current participants who, in the starting year of the projection period:					
Have not yet attained eligibility age					
HI	18,147	17,365	15,639	15,633	12,668
SMI Part B	16,342	14,949	12,130	12,433	11,541
SMI Part D	6,144	6,527	7,273	7,338	7,913
Have attained eligibility age (age 65 and over)					
HI	2,958	2,747	2,558	2,397	2,179
SMI Part B	2,142	1,986	1,834	1,773	1,622
SMI Part D	595	581	794	792	880
Those expected to become participants					
HI	4,673	4,506	5,118	3,904	3,417
SMI Part B	4,672	4,262	4,257	3,407	3,408
SMI Part D	2,632	2,856	2,699	2,121	2,440
All current and future participants:					
HI	25,778	24,619	23,315	21,934	18,264
SMI Part B	23,156	21,197	18,221	17,613	16,571
SMI Part D	9,371	9,964	10,766	10,250	11,233
Actuarial present values for the 75-year projection period of estimated future excess of income (excluding interest) over expenditures (Notes 26 and 27)					
HI	$(13,770)	$(12,737)	$(12,292)	$(11,290)	$(8,829)
SMI Part B	-	-	-	-	-
SMI Part D	-	-	-	-	-
Additional Information					
Actuarial present values for the 75-year projection period of estimated future excess of income (excluding interest) over expenditures (Notes 26 and 27)					
HI	$(13,770)	$(12,737)	$(12,292)	$(11,290)	$ (8,829)
SMI Part B	-	-	-	-	-
SMI Part D	-	-	-	-	-
Trust Fund assets at start of period					
HI	321	312	300	285	268
SMI Part B	59	53	38	23	19
SMI Part D	1	3	1	-	-
Actuarial present value for the 75-year projection of estimated future excess of income (excluding interest) and Trust Fund assets at start of period over expenditures (Notes 26 and 27)					
HI	$(13,449)	$(12,425)	$(11,993)	$(11,006)	$(8,561)
SMI Part B	59	53	38	23	19
SMI Part D	1	3	1	-	-

Note: Totals do not necessarily equal the sums of rounded components.

With the exception of the 2007 projections presented, current participants are assumed to be the "closed group" of individuals who are at least age 15 at the start of the projection period, and are participating in the program as either taxpayers, beneficiaries, or both. For the 2007 projections, the "closed group" is assumed to be individuals who are at least 18 at the start of the projection period, and are participating in the program as either taxpayers, beneficiaries, or both.

The accompanying "Notes to the Financial Statements" are an integral part of these statements.