PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers LLP
Suite 900
1800 Tysons Boulevard
McLean VA 22102
Telephone (703) 918 3000
Facsimile (703) 918 3100
www.pwc.com

Report of Independent Auditors on Internal Control

To the Secretary of the Department of Health and Human Services and the Inspector General of the Department of Health and Human Services

We have audited the financial statements of the Department of Health and Human Services (HHS) as of and for the year ended September 30, 2007 and the statement of social insurance for the year ended January 1, 2007, and have issued our report dated November 14, 2007. We conducted our audit in accordance with auditing standards generally accepted in the United States of America, 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.* The management of HHS is responsible for maintaining effective internal control over financial reporting.

In planning and performing our audit, we considered HHS's internal control over financial reporting by obtaining an understanding of the design effectiveness of HHS's internal control, determining whether these controls had been placed in operation, assessing control risk, and performing tests of HHS's controls in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and not to provide an opinion on the internal controls. Accordingly, we do not express an opinion on the effectiveness of the HHS's internal control over financial reporting.

We limited our control testing to those controls necessary to achieve the following OMB control objectives that provide reasonable, but not absolute assurance, that: (1) transactions are properly recorded, processed, and summarized to permit the preparation of the financial statements in accordance with accounting principles generally accepted in the United States of America, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition; (2) transactions are executed in compliance with laws governing the use of budget authority, government-wide policies and laws identified in Appendix E of OMB Bulletin No. 07-04, and other laws and regulations that could have a direct and material effect on the financial statements; and (3) transactions and other data that support reported performance measures are properly recorded, processed, and summarized to permit the preparation of performance information in accordance with criteria stated by management. We did not test all internal controls relevant to the operating objectives broadly defined by the Federal Managers' Financial Integrity Act of 1982.

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control

deficiency, or combination of control deficiencies, that adversely affects HHS's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of HHS's financial statements that is more than inconsequential will not be prevented or detected by HHS's internal control.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by HHS's internal control. Our consideration of internal control was for the limited purpose described in the second paragraph of this report and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. We noted eight matters, discussed below, involving the internal control and its operation that we consider to be significant deficiencies (of which four are considered to be material weaknesses).

Material Weaknesses

I. Financial Reporting Systems and Processes

I.1 *Coordination and Communication*

HHS lacks a coordinated end-to-end process among cross-functional teams of financial management, information technology, actuarial and operations personnel to monitor business activities and identify those situations where accounting evaluation or decision-making may be necessary. The lack of coordination led to the following:

I.1.1 *Prescription Drug Program Accrual*

In FY 2006, HHS implemented the Part D Drug Program. The implementation of the new program created an enormous challenge for the agency, not only on the programmatic side but also for accounting challenges, that continues today. Management continues to identify and implement processes and controls to enable the agency to reflect the accounting impact of this complex and challenging program within their financial statements.

Throughout the plan contract year (calendar year), HHS makes prospective payments to the Part D plans. In general, the payment amounts are based on information in the approved plan bids, which includes the plans' estimate of direct and indirect remuneration, and on data provided by HHS that updates payments throughout the year.

Subsequent to the contract year, HHS is required to reconcile the prospective Part D plan payments made during the year to actual drug costs incurred by the plans. Because the Part D program commenced operations in January 2006, the fiscal year ended September 2007 is the first year of the reconciliation. An accrual as of September 2007 was recorded on the books

that included the contract year reconciliation (Calendar Year 2006) and estimated payable/receivables covering the fiscal year under audit.

In order to calculate the CY 2006 accruals, HHS developed a mechanism to obtain actual drug cost data from the plans, the Payment Reconciliation System (PRS), to automate the reconciliation process - including robust system documentation - and a SAS program to validate the calculation performed by the PRS system. The systems used to obtain actual drug data from the plans include edit checks that reject invalid data. In addition, management performs several outlier and analytical analyses to ensure the validity of the PRS results including analysis over the DIR amounts submitted by the plans.

The estimated accrual for the period of January 2007 to September 2007 was developed by actuarial analysis. HHS refined the methodology used during FY 2006 to better reflect the cyclical nature of the accrual, documented the methodology used to develop the estimate and retained appropriate evidence of the calculation.

The Part D reconciliation and accrual process, for all intended purposes, was a new process for HHS. This new process has not yet been fully developed and therefore; faced the following challenges during the current year.

- Validation of Actual Drug Costs and Direct and Indirect Remuneration (DIR)
  HHS does not currently have a monitoring control in place to ensure the accuracy of the prescription drug data (PDEs) submitted by the plans which forms the basis for the reconciliation. HHS relies on the plans to certify the accuracy of this data. Unsupported or erroneous drug cost data submitted by the plans could lead to inaccuracies within the reconciliation and erroneous payments.

  Similarly, HHS does not currently have monitoring controls in place to ensure the completeness and accuracy of the DIR information (commonly referred to as rebates). Management acknowledges the importance of complete and accurate DIR information due to the significant impact that it has on reimbursements to the plans.

- Timing of Estimate Development
  As of July 2007, HHS had not calculated the 2006 contract year reconciliation which would cover the period of January 2006 to December 2006, nor had HHS calculated the estimated accrual for the period of January 2007 to June 2007. The lack of timely calculation of the estimate resulted in inaccurate reporting within the interim financial statements.

- Documentation of the Estimation Process
  HHS documented the procedures used to develop the 2006 Part D reconciliation within their Part D cycle memo; however, procedures and related controls to develop the FY 2007 Part D estimate, including the estimate related to invalidly rejected PDE data, was not documented within this memo. The calculation of the FY 2007 estimate was based upon

an actuarial analysis. The methodology used by HHS to develop this estimate was significantly different from what was used during the prior fiscal year. In addition, as of September 2007, the methodology used by management to develop the estimate related to invalidly rejected PDE data and related controls had not been documented.

Although all the elements of the estimate were eventually documented, all relevant controls have not yet been documented. According to OMB Circular A-123 *Implementation Guide* the level of detail of documentation should ensure management understands the entire financial reporting process and can identify how processes relate to financial reporting assertions, potential errors or misstatements, and control objectives.

I.1.2 *Obsolete Reports/Lack of Data*

With the Medicare Contractors transition to HIGLAS, HHS no longer requires the contractors to report certain data. This data which was collected in the Fiscal Intermediary Benefit Payment Report (IBPR) via the Contractor Administrative Budget and Finance Management (CAFM) systems is no longer available for those contractors who have implemented HIGLAS, which resulted in the following:

- Impact on the Statement of Social Insurance (SOSI):
  The IBPR provided data used by HHS to develop aspects of the SOSI projection. A total of six SOSI data sources and one validation source previously provided by the IBPR are no longer reported by contractors who have transitioned to HIGLAS. HHS was able to find suitable replacements for three of the data sources; however; it has not yet identified an appropriate source of data for the remaining three sources and for the validation source. Although the lack of data sources does not pose a significant risk to the current year SOSI calculation, because of the nature of the projection, the risk could increase on future projections.

- Entitlement Benefit Due and Payable Liability:
  The Entitlement Benefit Due and Payable Liability line item on the balance sheet is mainly composed of an estimate of claims incurred but not reported (IBNR). A key report used by HHS in the calculation of the IBNR liability is the National Claims History (NCH) processing report. Before this report is considered reliable and appropriate for use, management performs certain analytical procedures between the data in the report and data obtained from CMS-456 Intermediary Benefit Payment Report. However, since the CMS-456 report was produced from the CAFM system and is no longer submitted by those contractors that transition to HIGLAS, the appropriate NCH processing report validation procedures were not performed. In response to the issue, management has created a special HIGLAS query to generate the data previously reported by the CMS-456 report for the contractors under HIGLAS and is in the process of identifying an appropriate NCH processing report validation source.

I.2 ***Controls Over Trust Fund Draws***

In order to ensure amounts drawn from the HI and SMI trust funds are accurate and complete, management reconciles “cash” payment amounts recorded by HHS and the Department of the Treasury with the corresponding “incurred” claims amounts from Medicare claims data. However, this reconciliation is not performed at a level that allows management to detect errors timely.

The lack of a reconciliation at this level affected HHS's ability to identify that payments for hospice services were incorrectly being drawn from the Part B SMI trust fund. Because Hospice care is covered only under Part A of the Medicare program, these payments should have been drawn from the HI trust fund. The error led to an overstatement of benefit expenses attributed to the Part B Medicare program and an understatement of benefit expenses attributed to the Part A program. In addition, the error led to inaccuracies within the SOSI. These errors were corrected within the final financial statements.

I.3 ***Lack of Integrated Financial Management System***

Federal Agencies are required by law and OMB regulations to establish, "single integrated financial management systems" to be used to manage financial operations. As a result of implementing an integrated financial management system, agencies should be able to prepare timely and reliable financial reports, including financial statements. The completeness and accuracy of the financial statements are dependent on an integrated system which provides sufficient structure, effective internal controls and reliable data. HHS relies on decentralized processes and complex systems to accumulate data for financial reporting. In addition to an integrated financial system, a sufficient number of properly trained personnel and strong management oversight are needed to ensure periodic analyses and reconciliations are completed to detect and resolve errors and irregularities in a timely manner.

Within HHS, the newly implemented UFMS is designed to have three components, HIGLAS, the NIH Business System (NBS), and UFMS (Indian Health Services will implement UFMS in FY 2008). In addition, the consolidating reporting module is expected to be implemented in FY 2009. However, HHS's financial management systems, as currently configured, are not compliant with the Federal Financial Management Improvement Act of 1996 (FFMIA). 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, non-compliance with the USSGL at the transaction level and weaknesses in internal controls and business processes impair HHS's ability to efficiently and effectively support and analyze accounts, as well as, prepare timely

and reliable financial statements. HHS uses “work-arounds,” cumbersome reconciliation and consolidation processes, and significant adjustments to produce the financial statements. The following matters illustrate the challenges presented by the existing systems:

- The majority of Medicare contractors currently rely on a combination of claims processing systems, personal computer based software applications and other ad hoc systems to tabulate, summarize and prepare information presented to HHS on the "750 – Statement of Financial Position Reports" and the "751 – Status of Accounts Receivable Reports". These reports are the primary basis for the accounts receivable amounts reported within the financial statements. Because both HHS and their contractors do not have a compliant financial management system, the preparation of the 750 and 751 reports and the review and monitoring of individual accounts receivable, are dependent on labor-intensive, manual processes that are subject to an increased risk of inconsistent, incomplete or inaccurate information being submitted to HHS. Likewise the reporting mechanism used by the HHS contractors to reconcile and report funds expended, the "1522 – Monthly Contractor Financial Report", is 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 HHS.

- HHS continues to experience significant challenges in resolving issues related to the UFMS conversion and implementation. This is evidenced by the following:

    - Despite the implementation of UFMS, HHS recorded more than 800 entries manually into the system during the year exceeding $170 billion. These entries were necessary to correct balances and accurately record transactions reported in UFMS.

    - During our testing, we noted transactions for current year activity that were inappropriately posting against opening balance accounts. These transactions were in excess of $1 billion which were not detected during the year through normal controls, but rather detected during the process of preparing the interim financial statements when it was noted that opening balances for the current financial statements were different from the ending balances of the prior financial statements.

    - HHS has not completed the development of management information reports from the UFMS system. Ad-hoc extracts from UFMS are used to support monthly reconciliations and the interim and year-end financial statements. HHS continues to use a cumbersome manual process to compile its financial statements.

    - Management is unable to provide timely and complete transaction level extracts from UFMS to support general ledger balances including:

- Undelivered Orders
- Unfilled Customer Orders
- Obligations
- Offsetting Receipts
- Reimbursable Revenue and Expenses

- Systematic controls and front end edits have not been implemented to sufficiently mitigate the risk of Anti Deficiency Act (ADA) violations or a misstatement of financial management reports as evidenced by:

  - UFMS allows receiving transactions to be posted in excess of the corresponding obligation transactions.
  - UFMS allows the posting of grant expense accruals in excess of the funds available for grants.
  - UFMS allows the manual posting of entries which may not comply with the USSGL including inappropriate account combinations which omit the corresponding budgetary entries.

- The NBS had more than 2000 manual accounting entries for more than of $45 billion entered into the accounting system outside the automated transaction process. In addition, to prepare financial statements at year-end, 55 top-side adjustments totaling more than $85 billion were made. Processing these transactions was needed to ensure that the proprietary and budgetary accounts accurately reflected the current year activity. Additionally, the NBS does not provide for tracking manual or non-routine entries. As a result, adjustments and corrections cannot be readily identified. During our testing we noted that manual intervention is needed to assign appropriate transaction identifiers to ensure the correct classification within the financial statements.

- Systematic controls and front end edits have not been implemented to sufficiently mitigate the risk of Anti Deficiency Act (ADA) violations or a misstatement of financial management reports as evidenced by:

  - NBS does not have system edits to prevent the obligation of funds in excess of allowances, allotments, or appropriations.
  - NBS allows the manual posting of entries which may not comply with the USSGL including inappropriate account combinations which omit the corresponding budgetary entries.

- The CORE accounting system is a data repository that was not designed to function as an accounting general ledger system. Accordingly, it does not capture all transactions properly and does not facilitate the preparation of timely financial statements. The accounting data in CORE must be downloaded and compiled to facilitate the preparation of adjusting entries. These entries are necessary to accurately reflect the current year activity and balances for financial reporting purposes. Approximately 30 miscellaneous

journal vouchers were posted into CORE, each representing multiple accounting transactions with an aggregate value of $9 billion.

I.4 *Financial Statement Preparation*

HHS compiles its financial statements through a multi-step process using a combination of manual and automated procedures. Responsibility segments must manually enter adjusted trial balances or statements into a separate system in order to generate consolidated financial statements and reports. Due to system limitations, HHS records numerous non-standard entries through journal vouchers as well as topside adjustments not entered into the general ledger systems and employs manually intensive procedures using Excel spreadsheets and database queries to prepare the financial statements. These processes increase the risk that errors may occur in the HHS financial statements. The following issues were identified during the financial statement preparation process:

- To prepare financial statements, information must be extracted from the general ledger systems and reviewed by an analyst to determine the following types of non-standard journal vouchers:
    - Correction of beginning balances that were incorrectly impacted by transactions during the year and for accounts that the system did not properly close or inadvertently dropped from the general ledger system.
    - Adjustment of balances to record the impact of reimbursable transactions that the system did not properly record during the year
    - Correction of the system trial balance for journal entries from the prior year that were not recorded in the system.

- During the testing of the supporting spreadsheets, calculations, and journal vouchers used to produce the financial statements we noted the following matters:
    - Calculation errors in the spreadsheet used to support the grant accrual.
    - Numerous journal vouchers for proprietary transaction did not contain the appropriate corresponding budgetary transaction as prescribed in the USSGL.
    - Journal vouchers posted to correct beginning balance errors were not recorded properly.
    - Manual keying errors where debits and credits were inversed and incorrect amounts were posted.
    - Lack of standardized methodology that ensures the analysis used to determine adjustments includes the potential impact of subsequently performed adjustments.
    - Procedures used to determine the reimbursable adjustments contained numerous deviations from the prescribed methodology resulting in multiple errors.

HHS does not have uniform policies and procedures for the preparation of the financial statements. This results in significant manual "work arounds" and delays in financial reporting. While the errors, unexplained differences, and unsupported entries noted were not material to the HHS financial statements taken as a whole, they serve to illustrate that errors are more likely to occur in an environment that necessitates a time-consuming, manually-intensive financial statement preparation process, as well as the need for additional strengthening of the HHS's financial statement preparation, review, and approval processes.

I.5 ***Incomplete and Untimely Completion of Reconciliations***

Since weaknesses currently exist in the financial management systems, management must compensate by implementing and strengthening mitigating controls to ensure that errors and irregularities are detected in a timely manner. A key compensating control is the monthly and quarterly reconciliations that are performed to ensure the balances in the general ledger system are accurate.

Our review of management's reconciliations disclosed a series of weaknesses that impact HHS's ability to report accurate financial information. We found that certain processes were not adequately performed to ensure that differences were properly identified, researched and resolved in a timely manner. The following issues were identified related to the reconciliation process:

- During the first half of the fiscal year, management did not perform key reconciliations due to an inability to obtain information from UFMS and the redirection of resources from these processes to allow for a successful conversion to UFMS. In addition, we noted other reconciliations were not completed within the timeframes established by Departmental policy.

- HHS policy and procedures do not provide thresholds that personnel are required to follow in determining whether a difference has to be investigated. This allows for individual staff to determine amounts that may be inconsistent with the design of these controls.

- The explanations of differences identified by management are incomplete and do not fully explain the business reasons for the outstanding items.

- Reconciliations were incomplete with differences remaining unreconciled for more than 90 days. While individual items may appear to be immaterial to the Department no analysis is performed by management to determine the aggregate impact of all unreconciled items.

Recommendation

We recommend that management continue to develop and refine its financial reporting systems and processes. Specifically, HHS should:

- Establish appropriate policies, procedures and a protocol to address situations or transactions that require cross-functional involvement in order to ensure interim and year-end financial statements are accurate and complete. This includes policies and procedures to ensure changes to critical systems outputs are appropriately vetted with all users. The financial management function should serve as the primary coordinator to facilitate the input and involvement of the other cross-functional units whose involvement and input are important factors to consider in formulating accounting treatment and financial reporting implications.

- Continue to develop its policies and procedures related to the development, documentation, and validation of the Part D accrual process.

- Continue to implement an integrated financial management system for use by Medicare contractors and HHS to promote consistency and reliability in accounting and financial reporting.

- Management should develop appropriate reconciliation procedures between claims incurred to cash drawn from each of the trust funds that would enable the timely identification of potential errors in Medicare Trust Fund draws.

- Fully utilize the built in system functionality designed to perform complete transaction processing and financial reporting in compliance with Federal financial reporting requirements.

- Enhance the documentation related polices and procedures for the preparation of financial statements and ensure compliance through a monitoring process**.**

- Establish appropriate reconciliation policy and procedures which include the following:

    - Thresholds based on the type and purpose of the reconciliation to ensure differences are appropriately identified and researched.
    - Require the clearing of differences with ninety days of identification.
    - Require documentation to be completed which supports the explanation of the difference.

II. Budgetary Accounting

HHS lacks sufficient controls over its accounting and business processes to ensure budgetary transactions are properly recorded, monitored and reported. Management routinely uses high level analysis to develop adjustments and derive balances for financial reporting purposes. Due to the lack of sufficient controls over the process, management has not mitigated the risk of a misstatement or potential violation of laws and regulations to an acceptable level. The following sections highlight the key issues that were identified with the budgetary process.

II.1 *Undelivered Orders (UDO)*

HHS does not have adequate controls in place to monitor undelivered orders which represent remaining amounts of obligated funds that have not been delivered nor appropriately deobligated. UDO oversight is the key to the status of budgetary resources is accurate.

Management was unable to provide evidence to demonstrate controls existed and operated effectively during the fiscal year. As a result we performed substantive test of details to quantify the potential misstatement due to the lack of controls. Our results revealed a projected error $1.1 billion in errors, including both over and understatements. The following types of errors were detected:

- Grants/Contracts which had expired periods were not closed and deobligated timely
- Obligations were recorded late or not recorded at all
- Deliveries were applied inaccurately to obligations which have been converted from prior systems as a lump sum and not at a document level
- Inaccurate and unsubstantiated postings to the general ledger

II.2 *Recoveries of Prior Year Obligations*

HHS does not have adequate controls in place to capture the recoveries of prior year obligations as required by federal accounting and reporting requirements, which require prior year recoveries to be recorded in a separate general ledger account and reported on the SF-133s and SBR. We noted inconsistent methodologies in use across the Department to derive the prior year recovery amounts.

During our testing we noted:

- One responsibility segment failed to report any recoveries on their financial statements.
- Nine responsibility segments must analyze transactions in other accounts to derive the balance.
- One responsibility segment currently has a waiver from OMB on reporting recoveries until the full implementation of their financial system is complete

II.3 ***Recording of Obligations***

HHS does not have adequate controls to ensure its obligations are recorded appropriately. While the majority of HHS obligations are automatically posted through system interfaces, HHS lacks controls over its manually-processed obligations. During our testing of undelivered orders, we noted several obligating documents that were not recorded into the system. Additionally, we noted that management did not have a sufficient process in place to prevent or detect unrecorded obligations at year end.

Management performed an analysis of unrecorded obligations for all of HHS's operating divisions. Based on our review of this analysis the amount of unrecorded obligations at year end was not material to the fiscal year 2007 financial statements.

II.4 ***Budgetary Reimbursable Accounting***

Management manually analyzes revenues and expenses to derive the budgetary account balances for reimbursable activities. This process is prone to error. For year end reporting, HHS posted more than $2.5 billion in adjustments to the SBR to account for these activities. Our review of the journal vouchers and supporting documentation noted keying errors, incorrect application of the USSGL, and inconsistency in the calculations by HHS analysts which went undetected by management.

Recommendation

In order to remove the risks associated with the current budgetary reporting environment, HHS should:

- Implement department wide procedures requiring the periodic review of Undelivered Orders.
- Implement department wide policies and procedures requiring the recording of recoveries in accordance with federal accounting standards.
- Implement a commitment accounting function within the current general ledger system to allow automated reconciliation obligations.
- Implement the projects module of UFMS across the department to ensure obligations are recorded in a timely manner through automated processes.

III. Financial Management Information Systems

Many of the business processes that generate information for the financial statements are supported by HHS 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 controls involve the entity-wide security programs, access controls (physical and logical), application development and program change controls, segregation of duties, operating systems software, and service continuity. General controls impact the integrity of all applications operating within a single data processing facility and are critical to ensure the reliability, confidentiality, and availability of financial information.

Our testing noted general controls issues in both the design and the operations of key controls. We noted weaknesses in the following review areas:

- Entity-wide security program,
- Access controls (physical and logical),
- Application development and program change controls, and
- Operating systems software, and
- Service continuity.

Of particular concern, we noted the lack of pervasive Information Technology (IT) security standards for areas such as IT security settings on platforms, policies regarding the control and use of passwords, and policies regarding the control over changes to applications whether they be developed in-house or purchased, for HHS at the department level. Our testing consistently noted that management of the various component entities within HHS either had developed their own IT security standards or simply stated that they do not follow HHS standards.

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. Detailed descriptions of control weaknesses may be found in SAS70 reports and the management letters issued on information technology general controls and audited applications. The following discusses the summary results by review area.

III.1 ***Entity-Wide Security Programs***

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. Entity-wide 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 mission-critical, systems-based operations. Our procedures identified the following issues:

- **Information System Platform and Database Security Controls:** HHS lacks accepted and used standards for information system platform security settings that are

consistent with NIST standards for securing information system platforms and databases.

- **Information System Platform and Database Security Control Monitoring:** HHS lacks processes to monitor security settings continuously to ensure they remain effective.
- **Security Plans:** Security plans for some of the systems have not been updated, finalized, approved, and communicated.
- **Certification & Accreditation:** Required certification and accreditation statements for some of the major financial applications and general support systems have expired or have not been reviewed or updated recently.
- **Security Training:** Relevant security and security awareness training was not provided to all employees and contractors.

III.2 *Access controls (logical and physical)*

Access controls ensure that critical systems assets are physically safeguarded and that logical access to sensitive application, 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 Authorizations**: For some of the systems, the approval of access requests was not, or was inadequately, documented.
- **Access Revalidations**: For some of the systems, the periodic revalidation of user accounts is either not performed or inadequately documented.
- **Password Controls**: The password controls applied to some of the systems do not provide an adequate level of authentication controls.
- **Access Assignments**: Access assignments were excessive for some systems and did not provide an adequate segregation of duties.
- **Access Removal**: For some of the systems, users' access was not terminated, upon termination of their role.

III.3 *Systems software*

Systems software is a set of computer programs designed to operate and control the processing activities for a variety of applications on computer hardware and related equipment. The systems software helps coordinate the input, processing, output, and data storage associated with all of the applications that are processed on a specific system. Some systems software is designed to change data and programs without leaving an audit trail. Overall, problems in managing routine changes to systems software to ensure an appropriate implementation and related configuration controls were identified. Our procedures identified the following issues:

- **Configuration Controls**: Systems settings for selected databases and operating systems are not optimized to provide a secure computing environment.
- **Patch Management**: The controls over timely and consistent application of system patches are not effective for all of the systems.
- **Change Management**: Change management procedures were insufficient to ensure only properly authorized changes were implemented into some production systems.

III.4 ***Application software development and change controls***

A well defined and effectively controlled development and change management process should be in place to ensure that only authorized, tested, approved, and documented new programs, or changes to existing programs, are applied to the production environment. Additionally, the process facilitates that new or changed programs meet the requirements with regards to security and controls; such as providing for programmed integrity controls, audit trails, logging capabilities, etc. Our procedures, which included findings during our SAS70 Reviews of the Division of Financial Operations, the Centers for Information Technology, and the Human Resource Services operation, identified the following issues:

- **Change Controls**: For some applications, there is no formal and consistently applied change control process.
- **Change Management**: Evidence to support that change management procedures and processes were followed was not provided.
- **Access Controls**: Periodic reviews of user access permissions were not conducted and/or not documented. Procedures to approve access assignments and to control terminated and transferred employees were either non-existent or not followed.
- **Application Controls**: Error reports were not properly reviewed and used to correct issues noted and reconciliations of application data were not always performed.
- **Configuration Controls**: Password controls and system lockouts for incorrect password attempts were not sufficient to provide effective security. Platform security configuration settings were also insufficient to provide effective security.

III.5 ***Application Specific Concerns - General Ledger System***

As part of our assessment of internal controls, we have conducted application control reviews for systems that are relevant to the financial reporting process. Application controls involve access controls, data input controls, data processing controls and data output controls. Our testing noted application controls issues in both the design and the operations of key controls. We noted weaknesses in the following review areas:

III.5.1 Access Control

Procedures related to the conversion and entry of data through terminals should be established to deter unauthorized use. Key duties and responsibilities performed within the application should be adequately separated to reduce the risk of errors, waste, or wrongful acts.

- **Access Authorization:** For some users, access to key financial system was not appropriately granted.
- **Password Controls**: The password controls applied to some of key financial systems do not provide an adequate level of authentication controls.
- **Access Assignments**: Access assignments were excessive for some key financial systems and did not provide an adequate segregation of duties, with more than 600 possible segregation of duties issues identified in the G/L system. Assignment conflicts represent instances whereby accesses assigned may have allowed users to perform all phases of transactions without intervention by other users or approvers. For example, creation and approval of transactions from inception of the transaction to payment.
- **Access Removal**: For some of key financial systems, user's access was not terminated, upon termination of their role.

III.5.2 *Data Input*

All authorized source documents should be complete and accurate, properly accounted for, and transmitted in a timely manner for input to the computer system. Input data should be validated and edited to provide reasonable assurance that erroneous data are detected before processing. Procedures should be established for the conversion and entry of data that ensure a separation of duties as well as routine verification of work performed in the input process. Formal procedures should be established for data processing to ensure that data is processed completely, accurately, and on time. We noted the following weaknesses:

- **System Interfaces:** For some key financial 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.
- **Configuration Controls**: Application settings are not optimized to provide a controlled processing environment. For example, edits were not properly configured to prevent erroneous input of data.
- **Data Processing Controls:** Procedures were not established for the entry of data to ensure a separation of duties as well as routine verification of work performed during processing. Errors identified during data processing should be promptly investigated, corrected, and resubmitted.
- **Audit Trails:** For some systems, it was not possible to identify the user or users who made modification to key system transactions and standing data. Further, audit trails were generated showing a count of transactions performed in each module by specific users.

III.5.3 *Data Output*

Procedures should exist to report and control errors contained in output. Reports produced outside the normal production cycle (i.e. ad hoc reporting) should be adequately controlled. Output should be balanced to record counts and control totals, and audit trails should be available to facilitate tracing and reconciliation. We noted the following weaknesses:

- **Error Handling Activities**: Procedures do not exist that the Global Error Handler is monitored and that transactions held in error are reviewed and processed timely. Business owners indicated that documentation to evidence the review of transactions in the Global Error Handler was not maintained.
- **Key management reports**: Procedures do not exist to ensure that key management reports are reviewed and maintained

Recommendations

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

- Develop overall HHS platform configuration security standards for all operating platforms and databases, following the guidance issued by NIST, for all components.

- Ensure the acceptance and implementation of the platform configuration security standards by all components.

- Develop and implement effective tools, policies and procedures to review platform security settings for all components, on a continuing basis.

- Develop an effective and documented patch management process for all critical systems to reduce systems vulnerabilities to a minimum.

- Enhance policies and procedures to ensure that system administrators perform periodic reviews of access authorizations for all applications and that a process exists for communicating terminated employees to administrators for their timely removal.

- Revalidate access rights on a periodic basis to limit systems access to the least privilege required to perform job responsibilities.

- Complete certification and accreditation activities, including the corresponding risk assessments, to limit the residual risk to an acceptable level.

- Maintain system security plans to provide security and controls commensurate with risk changes associated with systems.

- Train all employees and contractors on security awareness and responsibilities to effectively communicate security policies and expectations.

- Maintain effective program change controls processes for all applications to limit the risk of unauthorized changes to the production systems.

IV. Medicare Claims Processing Controls

Overview

HHS relies on extensive information systems operations at the Centers for Medicare and Medicaid Services Central Office (CMS Central Office) and Medicare contractor sites to administer the Medicare program and to process and account for 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. The internal control structure is inclusive of, but not limited to, automated controls. The internal control structure also includes monitoring controls over claims processing.

Our internal control testing for the audit covered both general and application controls. General controls involve organizational security plans, referred to as entity-wide security plans (EWSP), access controls (physical and logical), application software development and program change controls, segregation of duties, operating systems software for servers and mainframe platforms, and service continuity plans and testing. General controls provide the foundation to ensure the integrity of application systems, and combined with application level controls, are essential to ensure proper processing of transactions and integrity of stored data. Application controls include controls over input, processing of data, and output of data from HHS application systems.

Our audit included various general controls testing for nine contractors and site visits to six data centers supporting Medicare claims processing. We also reviewed application controls at the CMS Central Office and at Medicare contractors for systems integral to Medicare financial information including the Fiscal Intermediary Shared System (FISS), the Viable Information Processing Systems (VIPS) Medicare System (VMS), the Multi-Carrier System (MCS) and the Common Working File (CWF). At CMS Central Office we performed procedures over the Financial Accounting Control System (FACS), Health Plan Management System (HPMS), Medicare Advantage Prescription Drug System (MARx), Healthcare Integrated General Ledger Accounting System (HIGLAS), Medicaid Budget and Expenditure System (MBES), and Children Budget and Expenditure System (CBES).

We also conducted vulnerability reviews of network controls at six data center sites and the CMS Central Office. Further, desktop-based audit procedures were conducted to review the high level management controls regarding direct access to claims data, control over edits within the FISS, MCS and VMS systems, and controls over software supplementing the FISS, MCS and VMS systems used to process Medicare claims. We noted some improvements in

each of these 3 areas, which were first identified in FY 2006 or earlier audits, but the progress of these improvements was not sufficient enough to address the concerns expressed below.

During FY 2004, management launched a program to evaluate the security levels of all contractors regarding their compliance with the Federal Information Security Management Act (FISMA) under the requirements of the Medicare Modernization Act. This evaluation program includes all eight key areas of FISMA: periodic risk assessments; policies and procedures to reduce risk; systems security plans; security awareness training; periodic testing and evaluation of the effectiveness of IT security policies and procedures; remedial activities, processes and reporting for deficiencies; incident detection, reporting and response; and continuity of operations for IT systems. We believe that the evaluations obtained as a result of this effort have served and continue to serve HHS greatly in better understanding the current state of security operations at all Medicare contractors; not just those contractors tested as a result of the financial statement audit or for which a SAS 70 was conducted.

In addition to the steps noted above, to address the material weakness conditions, HHS continues its programs to review the contractors through SAS 70 audits, an extensive contractor self-assessment program, and reporting process and greater central oversight by contractor management. Additionally, HHS continues to request and receive system security plans, risk assessments, contingency plans, self-assessments, and test results of contingency plans from its contractors and has a certification and accreditation program initiative featuring system vulnerability assessments for all contractors.

Efforts to address the findings noted in our review have been and will continue to be challenged by budgetary constraints and the decentralized nature of Medicare operations, the complexity of fee-for-service processing, the modernization of the claims processing applications and the ongoing contractor transition process related to the legislative mandate under MMA to competitively procure claims administration contractors to replace fiscal intermediaries and carriers by 2011. According to HHS officials, the HHS modernization program to centralize data processing and reduce the number of data centers represents a long-term solution to simplify the application software code and change controls needed for more robust security. HHS is also in the process of implementing significant changes to its claims administration contracting environment, which will result in consolidation and reduce the number of contractors and data centers.

IV.1 ***Direct Update Access to Medicare Claims Data***

For the direct update access to Medicare claims data control weakness, improvements were noted regarding the number of employees at contractors who had been granted access to directly change claims data, thereby bypassing application controls built into the FISS, MCS and VMS systems. Specifically, the audit showed that fewer employees generally had such access. This progress could be attributable in large measure to further guidance and information that HHS provided to contractors both in a series of briefings, and in writing via joint signature memoranda (JSM) and distributing white papers specifying in detail how to

meet the requirement for users of the mainframe ACF2, RACF and Top Secret security packages.

Still, the audit noted significant numbers of contractor employees who had been granted direct access without consistent logging and review. The ability to directly change claims without comprehensive review provides no assurance that changes performed by such employees will result in proper claims payment. We consistently noted employees, particularly those at contractors using the MCS system, who had been granted inappropriate standing update access to Medicare data but who did not require direct access to data and application software programs to perform their job responsibilities. Further, activity was not logged and reviewed.

IV.2 ***Control Over Edit Settings in the FISS, VMS and MCS Application Systems***

For controls over edit settings in the FISS, VMS and MCS application systems, management worked diligently during FY 2006 to establish workgroups to determine the proper settings for controlling edits within each of these three applications processing Medicare claims. Additionally, the CMS Central Office issued a JSM to formally establish procedures to report and control changes to edits in these systems.

During FY 2007, our audit noted general compliance and improvement with the FISS mandated edits (when claims are processed within the common working file software), and the VMS mandated edits. However, our audit noted exceptions at selected contractors. Moreover, we noted that the JSM procedures and workgroup settings for MCS were not correct for numerous edits resulting in incorrect edit setting at contractors.

Additionally, we noted that management could not provide reports to document the volume and nature of claims bypassing the CWF application. Approximately 2,000 edits were not enforced within the FISS application because the edits were redundant in the CWF application. The inability to determine the number of claims bypassing CWF does not allow management to understand the effect of claims not subjected to CWF edits. Thousands of edit controls were built into the Medicare claims processing applications to enforce consistency over claims processing. The ability of claims to bypass application edit controls may result in inconsistent and uncertain claims processing leading to payment inaccuracies.

IV.3 ***Controls Governing the Use of Supplemental Software Used to Process Claims***

We noted a lack of controls with respect to software supplementing the FISS, MCS and VMS systems used to process Medicare claims. The inability of the FISS, MCS and VMS claims processing application systems to efficiently process all Medicare claims types has caused Medicare contractors to develop additional programs to effectively process claims. These additional systems, sometimes referred to as automated adjudication systems (AAS), were developed to automate the handling of claims that could not be processed by the standard claims processing applications without human intervention. AAS programs are developed and used independent of the standard application systems to process valid claims rejected by the standard systems. During FY 2006, management established formal control processes for the

use of the AAS, including methods to establish, test, peer review and approve AAS programs prior to their use. Our testing noted issues at numerous contractors regarding compliance with these processes. AAS systems 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 again result in inconsistent and uncertain claims processing leading to payment inaccuracies.

IV.4 *Lack of CMS Oversight*

For the areas of direct update access to Medicare claims data, control over edit settings in the FISS, VMS and MCS application systems, and controls over the use of supplemental software used to process claims into the FISS, VMS and MCS application systems, we observed that often CMS Central Office had issued guidance and requirements to address internal control concerns. In each of these areas, we noted instances where contractors simply did not implement the needed controls although they had been directed to do so. In some cases the contractor staff simply did not appear to understand what was needed, for example the direct access to data instructions are of necessity quite technical. In other cases, contractors on the verge of leaving the Medicare program may no longer have the same incentive to comply with requirements. Regardless, HHS lacks sufficient management processes and procedures in place to track compliance with its requirements and to assess the impact of exceptions and findings on the HHS financial statements.

1V.5 *Other Matters*

Of lesser risk, our audit noted the following issues:

IV.5.1 *Logical Access Controls*

Access controls ensure that critical system assets are physically protected from unauthorized access and that logical controls provide assurance that only authorized personnel may access data and programs maintained on systems. Besides the access control issues described in the "Direct Update Access to Medicare Claims Data" section, we noted that numerous contractors were not consistently recertifying user access to systems to ensure such access was needed for job requirements. We also noted that contractor management was not effectively performing reviews of violations for the FISS, MCS and VMS application systems. These security weaknesses could allow internal users to access and update sensitive systems, program parameters and data without proper authorization. Our review did not disclose any exploitation of critical systems tested; however, clear potential existed.

We also noted that many contractors had not performed procedures to recertify access granted to employees on an annual basis as required by HHS standards. As a result, we noted inconsistencies regarding access assignments, removal of access for terminated or transferred employees and the enforcement of policies and procedures regarding the administration of access approval and maintenance at the contractor sites.

IV.5.2 *Systems Software*

Systems software is a set of computer programs designated to operate and control the processing activities for all applications processed on a specific computer, including network servers, mainframe systems, and personal computers. Controls over access to, and use of, such software are especially critical. We again noted inconsistencies in logical security controls over various platforms at contractor sites. Although contractors have established configuration security standards for platforms such as the mainframe, WINDOWS and UNIX, such standards were not consistently established on these platforms and/or monitored to ensure they remained in effect. Of mention, we did not note significant issues at three of the data center locations we audited which shows progress by HHS compared to prior year audits. Guidance issued by HHS for the implementation of controls, configurations, and design of the mainframe OS/390 and z/OS may have contributed to this improvement.

Recommendation

During FY 2007, management worked to establish and document consistent controls over the use of direct update access to claims data, control over edits within FISS, MCS and VMS and the use and control of AAS programs. However, the processes to consistently enforce these controls over twenty eight contractor and thirteen data center locations remains challenging. Although, the controls have not been fully implemented, we encourage management to continue their efforts to gain contractor support for full implementation of these controls. Effective management controls over the use of direct update access to claims, changes to edits within the three major Medicare application processing systems and AAS programs is imperative to establish a reasonable range of comfort over the accuracy of Medicare claims processing.

Additionally, we recommend that management should:

- Establish a process to periodically review and test contractor reports of employees with direct update access to Medicare claims data. The testing should include steps to ensure such access is logged and reviewed by contractors.

- Establish ongoing workgroups to review FISS, MCS and VMS edits that should be turned on or off and establish processes to distribute quarterly the results of these reviews to the contractors to allow them to determine their compliance.

- Establish a formal review process to, on a selected and unannounced basis, obtain and review actual in use edit settings for the FISS, VMS and MCS systems running at the contractor sites.

- Use the results of bullet point three above to identify edit settings not in compliance with the recommended edit settings suggested by the workgroups. For edits not matching the workgroup recommendations, match these differences to error trends resulting from

contractor claims processed during periods when edits are turned off (use CWFMQA report results). Document the results, including specific matching of error types to contractors from which the errors emanated, and follow-up with contractors. Alternatively, management may wish to research other methods to more efficiently identify and track errors for subsequent review with contractors.

- Establish reports to determine the volume and reason for claims bypassing the CWF application.

- Work with contractors and maintainers of the FISS, MCS, and VMS systems to ensure AAS programs such as SuperOps and SCF maintain complete audit trails and that changes to programs associated with these systems follow the rules outlined in CR 3011 for testing, peer review and approval.

- Continue to enhance processes for the recertification of contractor employee access and the review of violation reports for the FISS, MCS and VMS application systems.

Significant Deficiencies

I. Inadequate Oversight of Managed Care Organizations

Overview

HHS is responsible for 1) determining which organizations are eligible to contract and participate in the Medicare Managed Care (Part C) and Part D programs, 2) making payments to the participating organizations, and 3) providing oversight over the participating organizations.

Our prior year audits identified weaknesses in HHS internal control surrounding the management procedures to review and process Medicare Part C and Part D payments, and lack of documentation and procedures to determine eligibility of organizations during the initial application review. During our current year audit, we noted significant improvements in those areas. Specifically, management enhanced the procedures used to validate and authorize payments for Medicare Part C and the Part D benefit. Enhancements were made to a number of validation functions including the Beneficiary Payment Validation (BPV), the Plan Payment Validation (PPV), and the monitoring and tracking of payment issues. In addition, management made significant improvements in documentation that evidence their determination of eligibility of organizations during the initial application review.

However, we noted recurring issues with management oversight of the Medicare Advantage Organizations (MAOs). Management's oversight of MAOs is a monitoring control designed to ensure MAOs are in compliance with regulations established within applicable Medicare law, and therefore eligible to participate in the Managed Care program. Our review of the monitoring procedures in place over MAOs noted the following:

I.1 *Monitoring Review Selection Methodology*

Because of the significant increase in MAOs in the managed care program and limited resources, management developed a risk-based approach for their oversight of the Managed Care organizations. The risk-based approach was used to identify which plans would be within the scope of the review, in addition to what organizational eligibility elements would be reviewed. The following inconsistencies were noted with the newly-developed selection approach:

- Management sporadically provided us with a complete set of formal monitoring policies and procedures used throughout the fiscal year. The inability of HHS to readily provide a comprehensive set of the guidance to be used throughout the fiscal year increases the risk of inappropriate execution of the reviews.

- Management did not properly document the rationale and sampling approach for the population or universe used for each element selected for review. In addition, management selected an arbitrary percentage for sampling for the PACE organization reviews, with no documentation of the rationale.

- Management has a process in place for the completion of a standard form if additional elements and/or reviews are performed, by a Regional Office Manager. However, we noted instances where management deviated from the risk-based approach and included or excluded elements of the review without documenting the rationale for inclusion or exclusion.

I.2 *Monitoring Review Documentation*

HHS has ten Regional Offices which perform the monitoring reviews. Management issues Standard Operating Procedures and holds training sessions for new releases to the monitoring audit guides.

However, because of a lack of formalized policies and procedures regarding the level of documentation required to evidence the review, management was unable to provide sufficient documentation to evidence the appropriate on going monitoring of managed care organizations by the Regional Offices. The following was noted:

I.2.1 *Evidence of Review*

During the review, the reviewer must identify if organizational requirements are "met" or "not met".

- We noted instances where the reviewer noted that the MAO had "met" the required element; however; documentation supporting the rationale and conclusion were not available.

- We noted significant inconsistencies with how the determination of "met," "met with note," and "not met" was made on different reviews for the same element.
- Documentation available to support the review varied by Regional Office.

I.3 *Corrective Actions*

Upon the completion of the review, management is required to communicate non-compliances identified during the review to the organizations and the organizations are required to submit a corrective action plan. Management is required to evaluate the corrective action plan in order to make a final determination of the plan's eligibility.

- We found instances where findings identified during the review and corrective action plans developed by the MAO in response to the review, were not released and/or approved within the prescribed time frame. In some cases, required corrective action plans were not received at all. In these instances, documentation supporting the ultimate conclusion to continue to allow the organization to participate as a MAOs did not exist.

- We noted the acceptance of corrective action plans that did not properly identify how the MAO would correct each of the items identified.

I.4 *Oversight Status Tracking*

The Health Plan Management System (HPMS) is used by HHS to monitor the execution and status of managed care organization oversight. This system lies at the core of HHS's management process for MAOs. Inaccurate information within HPMS weakens management ability to monitor the MAOs. We noted the following:

- Management uses a Microsoft Excel spreadsheet and HPMS to monitor the progress of the monitoring reviews, versus one central tracking module. We noted additional reviews were performed that were not tracked within the spreadsheet or HPMS.

- The HPMS monitoring review module was not updated, in accordance with HHS's policy, with the results of review. We noted multiple instances where Regional Offices did not update HPMS with exception items noted during the reviews of the managed care organizations.

Recommendation

We recommend that management continue to develop and refine its financial management systems and processes to improve its accounting, analysis, and oversight of Medicare managed care activity. Specifically, HHS should:

- Establish policies for Regional Office monitoring of the various organizations (MA, MA-PD, PDP, PACE, RPPO, etc.) that include tailored procedures to address the unique requirements or risks of each organization.

- Ensure that existing policies and procedures for the monitoring of organizations within the Managed Care program are consistently implemented and applied and that the monitoring of these organizations is documented in accordance with appropriate standards and guidelines.

- Develop detailed policies and procedures outlining the minimum documentation requirements that must be maintained as part of the monitoring reviews, in order to appropriately support the review outcome.

- Document the compliance with regulations for the monitoring of specific chapters and/or elements for organizations. For example, PACE organizations are required to be monitored every year for the first three years of acceptance into the program, and every other year thereafter.

- Ensure findings, corrective action plans, and acceptance of the provider's correction action plans are provided, reviewed, and released within the proposed time frames.

- Ensure that relevant data are updated timely in order to provide the information necessary for adequate management oversight.

II. Lack of Controls over Monitoring of Grant Closeout

One of the largest work streams at HHS is the management of grants, with the award of more than $200 billion in discretionary and mandatory grants each year and over one trillion dollars in open grants under management throughout the year.

II.1 *Grant Closeouts*

The closeout portion of the *HHS Grants Policy Statement* is insufficient as it does not require the respective Grants Management Offices to develop formal and detailed controls to address final grant closeout.

Based on inquiry with grant management personnel, an effort to closeout grants is being made, but the Department has limited authority to ensure grantees comply with HHS grant closeout policy. The compliance actions available (i.e., drawdown restrictions and withholding of future awards) are rarely utilized because there is not a directive in the existing policy to support and encourage the grant offices to use these actions. The Division of Payment Management (DPM) _Grant Closeout Eligibility Report is considered unreliable by the Grants Management Offices and thus is not utilized for grant close-out monitoring.

The DPM report identified more than 25,000 grants with a remaining net obligation balance of $1.5 billion that are potentially eligible for closeout. For 80% of the grants identified as

potentially eligible for closeout by management, the grant project period expired more than eighteen months ago. The inability to properly closeout grants has a corresponding effect on funds which have been obligated to settle claims from grantees. To the extent that HHS is able to closeout grants in a timely manner, additional funds could be de-obligated and returned to the US Treasury as required by appropriations law.

II.2 ***Grant Documentation Retention***

While HHS has documentation retention policies related to grants that set minimum standards, this policy is not being followed and the systems in place are not sufficient to allow for document retrieval on an as needed basis. This was evidenced by management's inability to provide all requested documentation for 12 out of 105 sample items tested during our audit.

Examples of missing grant documentation include:

- Approved Applications
- Ranks and Approval Lists
- Secondary Review Documentation for grant above $50 thousand

II.3 ***Grant Monitoring***

Management was unable to provide documentation to evidence their ongoing monitoring of open grants. Examples of missing grant documentation are the grant monitoring statements and progress reports.

Financial Status Reports (FSRs or SF-269s) were not submitted in a timely manner and evidence of follow-up by the respective Grants Management Offices (GMO) was not available. The following causes were identified during our testing:

- The grant management automated information systems utilized by HHS do not provide notification (alert) to the Grant Management Specialist (GMS) when an FSR has not been received within the allotted time period.

- Management communicated it does not have sufficient staffing to ensure the FSRs are submitted within the allotted time period.

If the FSR is not received, management is unable to accurately determine if grant funds are being spent in accordance with the approved budget. Management is also unable to tell if financial benchmarks such as cost sharing are being attained by the grant recipient.

In addition, there are no sanctions mentioned in the HHS Grants Management policy that can be imposed on a grantee when they are late in providing an FSR. Repercussions only exist when a grantee is applying for a future award, at which time the grantee must provide the delinquent FSR.

Recommendation

To improve the oversight of grants, better safeguard taxpayer monies and decrease the administrative costs related to grants HHS should:

- Implement a standard document retention system. At a minimum, the system should be organized by unique identifier (grant document number) so that each grant and all of the associated documentation can be retrieved as needed.

- Scan hard-copy documents into their document retention systems, thus reducing the dependence on extensive paper files.

- Assign a GMS to focus solely on monitoring the FSR submission during the course of the project period.

- Develop standardized documentation requirements to ensure all correspondence between a GMS and a grantee is completed consistently and timely. The HHS Grant Policy Statement should be updated to include specific repercussions for not complying with the documentation requirements.

- Management should implement a systematic function to provide automated alerts to the appropriate GMS when the FSR has not been received by the due date.

III. Lack of Controls over Timely Invoice Payment

HHS lacks standardized policies and procedures for the processing of invoices to ensure proper and timely payment as well as compliance with the Prompt Payment Act (5CFR 1350). During our testing we noted the following:

- The Division of Financial Operations (DFO) accounting technician processing the invoice enters the invoice receipt date in UFMS, using the date of the Paying Office (DFO) receipt date of the invoice rather than the actual invoice receipt date by the receiving (program) office. This methodology is inconsistent with the Prompt Pay Act.

- Not all receiving (program) offices have a requirement to date stamp invoices upon their receipt. While some receiving (program) offices are utilizing date stamps upon receipt of invoices, this process is not performed consistently. Without a date stamp, HHS is unable to ensure that invoices are paid in a timely manner.

- According to the HHS policy, the receiving date should be entered into the UFMS system upon receipt of goods or services by the project officer or their designee. However, during our testing we found instances where entry of receiving date was

delayed by up to one month, causing the receiving date to be incorrect. The UFMS system calculates the payment due date based on the later of the goods being received or the receipt of a valid invoice. Payment will not be made until the receiving date is entered into UFMS by the project officers which, if not entered timely, results in the payment due date being inaccurately calculated.

During our testing we noted 19 invoices being paid on average 54 days after the receipt of goods and invoices. In 6 of these instances, HHS failed to pay interest to the vendor as required by the Prompt Payment Act. In addition, in 6 of the 13 invoices where interest was paid it was calculated incorrectly. The lack of controls has resulted in violations of the Prompt Pay Act and the use of tax payer monies for the payment of interest that could have been used for program expenses to benefit the public.

Recommendation

In order to ensure compliance with the Prompt Pay Act and decrease the monies paid on interest that could be used for program expense, management should:

- HHS management should assign a "Designated Agency Office" on all contracts, purchase orders and agreements to receive invoices and date stamp the invoices to ensure consistency and timely payment of invoices. Management should also ensure that vendors are aware of the procedures to send invoices to the Designated Agency Office.

- Develop stronger polices at the receiving (program) offices to ensure timely entry of goods received. There should also be regular monitoring of these dates involving reconciliation of financial system data to the hard-copy receiving reports.

- HHS should ensure that the training for employees who enter receiving into the financial system is clear as to what the receiving date should be and that receiving officials are aware of the importance of entering receiving information correctly and within the specified time period.

IV. Statement of Social Insurance (SOSI)

The SOSI is a long-term projection of the present value of income to be received from or on behalf of existing and future participants of social insurance programs, the present value of the benefits to be paid to those same individuals, and the difference between the income and benefits.

Starting in FY 2006, the SOSI was required to be presented as part of the basic financial statements rather than as RSSI as previously presented. As such, the process for preparing the SOSI must comply with appropriate financial reporting internal control requirements established by OMB.

HHS has implemented policies, processes, controls and related documentation that will enable them to support the related financial statement assertions. During the current year audit, we noted significant improvements in the areas of change control, access controls, and internal control documentation. However the following control design deficiencies where noted:

- Data are moved within and between spreadsheets by copying the data from cells and pasting the data to new cell locations. Errors from this process could result in significant unintended changes to the SOSI. While the input of data is subjected to secondary validation and review by supervisory actuarial personnel, such manual validation and review processes do not sufficiently mitigate the risk associated with the copying and pasting of data from cell to cell within this complex set of spreadsheets.

- Spreadsheets are named with the same name as the prior version after changes. Further, there are no automated controls to prevent users from inadvertently overwriting changes made by other users. This could result in unintended changes to critical spreadsheets resulting in unreliable outputs.

- Formulae changes are not in all cases independently tested, reviewed and verified. While formulae changes are subjected to secondary validation and review by supervisory actuarial personnel, such manual validation and review processes do not sufficiently mitigate the risk associated with the direct posting of formulae changes into cells by users of this complex set of spreadsheets.

The lack of robust automated controls over spreadsheet changes may result in output that varies significantly from management's intentions.

Recommendation

We recommend that HHS continue to develop and refine its SOSI financial reporting spreadsheet applications and processes. Specifically, HHS should:

- Implement automated controls to ensure that data moved between and within spreadsheets are moved correctly.
- Implement automated controls to prevent the possibility of overwrite to critical spreadsheet data or formula cells due to insufficient naming convention protocols.
- Implement automated controls to test, review and verify all formulae changes within and between spreadsheets (e.g. spreadsheet change logging capabilities).

*** * * * * * * * * * * * ***

Internal Control Related to Key Performance Indicators and RSSI

With respect to internal control relevant to data that support reported performance measures, we obtained an understanding of the design of significant internal controls relating to the

existence and completeness assertions, as required by OMB Bulletin No. 07-04. Our procedures were not designed to provide assurance on internal control over reported performance measures. Accordingly, we do not provide an opinion on such controls.

We also identified other less significant matters that will be reported to HHS's management in a separate letter.

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

PricewaterhouseCoopers LLP

November 14, 2007