Section IV - Independent Auditor's Report on Financial Statements and Management Response

INDEPENDENT AUDITOR REPORT

To: The Secretary of Health
and Human Services

We have audited the accompanying consolidated balance sheets of the U.S. Department of Health and Human Services (HHS) as of September 30, 2003 and 2002; the related consolidated statements of net cost, changes in net position, and financing; and the combined statement of budgetary resources for the fiscal years then ended. These financial statements are the responsibility of HHS 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 01-02, Audit Requirements for Federal Financial Statements. These standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the consolidated and combined financial statements referred to in the first paragraph present fairly, in all material respects, the financial position of HHS as of September 30, 2003 and 2002 and its net cost, changes in net position, budgetary resources, and reconciliation of net costs to budgetary obligations for the fiscal years then ended, in conformity with accounting principles generally accepted in the United States.

We conducted our audits for the purpose of expressing an opinion on the consolidated and combined financial statements referred to in the first paragraph. The information presented in the Management's Discussion and Analysis of HHS, required supplementary stewardship information, required supplementary information, and other accompanying information is not a required part of the consolidated and combined financial statements but is supplementary information required by OMB Bulletin 01-09 and the Federal Accounting Standards Advisory Board or provided for purposes of additional analysis of the consolidated and combined financial

statements. We have applied certain limited procedures to such information, which consisted principally of inquiries of management regarding the methods of measurement and presentation of this information. However, we did not audit the information and express no opinion on it. We were unable to assess control risk relevant to HHS's intragovernmental transactions and balances, as required by OMB Bulletin 01-02, because reconciliations were not performed with certain Federal trading partners as required by OMB Bulletin 01-09.

In accordance with "Government Auditing Standards," we have also issued our reports, dated November 14, 2003, on our consideration of HHS's internal controls and on its compliance with certain provisions of laws and regulations. Those reports are an integral part of an audit performed in accordance with "Government Auditing Standards" and should be read in conjunction with this report in considering the results of our audit.

Dara Corrigan
Acting Principal Deputy
Inspector General

November 14, 2003
A-17-03-00001

INDEPENDENT AUDITOR REPORT ON INTERNAL CONTROLS

To: The Secretary of Health and Human Services

We have audited the consolidated and combined financial statements of the Department of Health and Human Services (HHS) as of September 30, 2003 and 2002 and have issued our report, dated November 14, 2003, on those statements. 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 01-02, Audit Requirements for Federal Financial Statements.

Management of HHS is responsible for establishing and maintaining effective internal controls. The objectives of internal controls are to provide management with reasonable, but not absolute, assurance that:

- transactions will be properly recorded, processed, and summarized to permit the preparation of the consolidated and combined financial statements in accordance with Federal accounting standards;
- assets will be safeguarded against loss from unauthorized acquisition, use, or disposition; and
- transactions will be executed in accordance with (1) laws governing the use of budget authority and other laws and regulations that could have a direct and material effect on the consolidated financial statements and (2) any other laws, regulations, and Governmentwide policies identified in OMB Bulletin 01-02.

In planning and performing our audit, we considered HHS's internal controls over financial reporting by obtaining an understanding of the internal controls, determining whether they had been placed in operation, assessing control risk, and performing tests of controls in order to determine our auditing procedures for the purpose of expressing our audit opinion on the financial statements. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin 01-02. We did not test all internal controls relevant to

operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982, such as those controls relevant to ensuring efficient operations. The objective of our audit was not to provide assurance on internal controls. Consequently, we do not provide an opinion on internal controls.

In addition, we considered HHS's internal controls over required supplementary stewardship information by obtaining an understanding of the internal controls, determining whether these internal controls had been placed in operation, assessing control risk, and performing tests of controls as required by OMB Bulletin 01-02. Accordingly, we do not provide an opinion on such controls.

Finally, with respect to internal controls related to 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 01-02. Our procedures were not designed to provide assurance on internal controls over reported performance measures; accordingly, we do not provide an opinion on such controls.

Our consideration of internal controls over financial reporting would not disclose all matters in such control that might be reportable conditions. Under standards issued by the American Institute of Certified Public Accountants, reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of internal controls that, in our judgment, could adversely affect the agency's ability to record, process, summarize, and report financial data consistent with management's assertions in the financial statements. Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts that would be material to the financial statements may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in internal controls, misstatements, losses, or noncompliance may nevertheless occur and not be detected. As discussed below, we noted certain matters involving internal controls that we consider to be material weaknesses.

MATERIAL WEAKNESSES

Financial Systems and Processes (Repeat Condition)

Since passage of the Chief Financial Officers Act of 1990, as amended by the Government Management Reform Act of 1994, agencies have prepared financial statements for audit by the Inspectors General. The Act emphasized production of reliable financial statements; consequently, HHS worked diligently to prepare statements capable of receiving an unqualified audit opinion. With this year's audit, HHS has sustained the important achievement of an unqualified, or "clean," opinion, which we issued for the first time on the FY 1999 financial statements, and has improved the timeliness of its financial reporting. A clean audit opinion,

however, provides no assurance as to the effectiveness and efficiency of agency financial systems and controls.

In our view, the Department continues to have serious internal control weaknesses in its financial systems and processes for producing financial statements. These weaknesses caused delays in meeting accelerated reporting deadlines and hundreds of millions of dollars of unexplained differences in reconciliations and account analyses. Within the context of the almost $600 billion in departmental outlays, the ultimate resolution of such amounts is not material to the financial statements. However, these matters are indicative of serious systemic issues that must be resolved. As detailed below, these weaknesses concerned financial statement preparation, financial management systems, and financial analyses and reporting.

Financial Statement Preparation

To prepare for the FY 2004 mandated reporting deadline, the Department implemented a pilot to accelerate the issuance of the FY 2003 "Performance and Accountability Report." The pilot included the establishment of three workgroups to address accelerated audit issues, estimation and closing procedures, and performance and accountability reporting. In addition, we designed a new audit approach premised on an effective internal control environment, timely receipt of supporting documentation, and prompt and ongoing reconciliations and extensive analyses by management. Strict milestone dates were also established. Accelerating the timeliness of financial reporting, pending implementation of modern accounting systems that are compliant with the Joint Financial Management Improvement Program and fully support the financial reporting process, provided challenges for us and for the Department.

We were able to overcome certain weaknesses in the internal control environment due to mitigating and compensating controls; however, documentation must be more readily available for examination. For instance, it took management over 3 months to provide certain internal control documentation. A property subsidiary ledger for September 30, 2003 was not provided until November 4, 2003. Furthermore, management stated that a fluctuation analysis as of June 30, 2003 was not performed for many operating divisions, resulting in the need for a more extensive analysis in the shortened timeframe at yearend.

Procedures need to be reassessed and modified to prepare accurate and complete financial statements in a more timely manner:

- The Department initially submitted draft financial statements for 11 of its 12 operating divisions on the October 10, 2003 due date. However, the statements did not pass all internal edit checks of its Automated Financial Statements system.

- Over the next 4 weeks, the operating divisions' financial statements were submitted several times with hundreds of millions of dollars in adjustments. In addition, the

Department made aggregate adjustments of approximately $4 billion to reclassify amounts in FY 2002. This adjustment was not resolved until November 14, 2003.

- At the completion of our audit, unexplained differences in balances totaling $1.4 billion remained, including unusual balances in credit reform-related accounts.

Financial Management Systems Issues

The Federal Financial Management Improvement Act (FFMIA) of 1996 was intended to advance Federal financial management by ensuring that financial management systems provide reliable, consistent disclosure of financial data, that they do so uniformly across the Federal Government from year to year, and that they consistently use accounting principles generally accepted in the United States. Policies and standards for agencies to follow in developing, operating, evaluating, and reporting on financial management systems are prescribed in OMB Circular A-127, Financial Management Systems.

Within the Department, the Centers for Medicare & Medicaid Services (CMS), the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC)/Agency for Toxic Substances and Disease Registry (ATSDR), and the Food and Drug Administration (FDA) are responsible for their respective financial management and accounting. The remaining operating divisions, including the Administration for Children and Families (ACF), rely on the Program Support Center's Division of Financial Operations (DFO) for these services.

While we observed steady improvement in the process of preparing financial statements, the lack of an integrated financial management system(s) and weaknesses in internal controls made it difficult to prepare timely and reliable financial statements. The Department expects the systems used by certain operating divisions, including CDC, FDA, NIH, and CMS, to be significantly enhanced by the end of FY 2005. Full implementation of the CMS system and the Unified Financial Management System is not anticipated until 2007. These systems are expected to provide improved financial information for better decisionmaking, potential cost savings, and a means to meet Federal accounting and budgetary reporting requirements. In the interim, substantial "work-arounds," cumbersome reconciliation and consolidation processes, and significant adjustments to reconcile subsidiary records to reported balances have been necessary. The following matters illustrate the challenges presented by existing departmental systems.

Centers for Medicare & Medicaid Services. CMS is the Department's largest operating division with about $503.3 billion in net FY 2003 budget outlays. To accumulate and report financial data, CMS, which operates as a decentralized organization, relies on complex systems as well as ad hoc and manually intensive reporting processes. As a result, the CMS financial management system is not fully integrated and, as reported in prior years, is not compliant with FFMIA.

During FY 2003, CMS engaged about 50 contractors to manage and administer the Medicare program. These contractors report Medicare activity on various financial reports, such as the

CMS 750/751 reports, which accumulate transactions and activity throughout the year. The Medicare claim processing systems have limited system interfaces to process and prepare data for these reports. Additionally, because the claim processing systems lack general ledger capabilities, preparing the 750/751 reports is labor intensive and requires reconciliations between various systems and ad hoc spreadsheet applications.

To address its systems problems, CMS is developing the Healthcare Integrated General Ledger Accounting System (HIGLAS) for the Medicare contractors and the CMS regional and central offices. HIGLAS will have capabilities to incorporate Medicare contractors' financial data, including claim activity, into the CMS internal accounting system and will replace the current central office general ledger and accounting system. Once implemented and fully operational—anticipated in FY 2007—the new system is expected to strengthen Medicare financial management and enhance oversight of contractor accounting systems.

National Institutes of Health. In FY 2003, NIH had net budget outlays of approximately $22.8 billion. The NIH Central Accounting System was not designed for financial reporting purposes and did not apply the U.S. Standard General Ledger at the transaction level. For example:

- The NIH process for preparing financial statements included downloading necessary data from its Central Accounting System and using spreadsheets to process adjusting entries and prepare financial statements. This process continues to be manually intensive, time consuming, and prone to error.

- To compensate for noncompliance with the U.S. Standard General Ledger, NIH recorded 1,900 nonstandard accounting entries totaling $14.2 billion in the Central Accounting System during the year. These entries were necessary to properly adjust account balances, including inventory, accrued leave, personal property, receipt of donations, and other revenues. In addition, NIH developed a process to record the impact of current-year, day-to-day entries in budgetary and expended appropriations accounts at the yearend. The use of nonstandard accounting entries increases the risk of bypassing accounting controls, as well as the risk of errors.

- Late in FY 2003, NIH identified a series of leases that had been recorded as operating leases in the financial records. Initial analysis indicates that these leases, which have a net present value of approximately $200 million, may need to be capitalized in the financial statements. Departmental analysis of this issue is ongoing.

To launch the Oracle General Ledger portion of the NIH Business System, NIH reconfigured all transaction codes to be compliant with the Standard General Ledger during FY 2003. On October 1, 2003, the Oracle General Ledger became the official accounting system of record. Management expects the new general ledger to expedite the preparation of quarterly and yearend financial statements

Entities Supported by the Program Support Center. In FY 2003, the operating divisions serviced by the Program Support Center had net budget outlays of approximately $63.3 billion. The Program Support Center's DFO CORE accounting system, which supports the activities of these operating divisions, did not facilitate the preparation of timely financial statements. The necessary data had to be downloaded from CORE, with numerous adjusting entries processed throughout the year before compiling the statements. For example, in FY 2003, approximately 2,300 nonstandard accounting entries with an absolute value of almost $41 billion were recorded in CORE to compensate for noncompliance with the U.S. Standard General Ledger, to correct for misstatements, to record reclassifications, and to correct reported balances.

The accelerated FY 2003 closeout severely taxed the Program Support Center's resources and highlighted the need to devote resources to reconciling and analyzing accounts, researching and correcting errors in underlying subsidiary records, and performing rigorous closing processes on an interim basis. These procedures should allow time for researching and addressing issues before the critical FY 2004 "Performance and Accountability Report" submission deadlines.

Centers for Disease Control and Prevention and Agency for Toxic Substances and Disease Registry. The CDC/ASTDR operated with combined net budget outlays of about $5.6 billion in FY 2003. Their central financial system did not have the capability to generate financial statements; the trial balance and financial statements had to be created offline by summarizing appropriate data. This process was manually intensive, used excessive resources, and increased the chance of error.

Financial Analyses and Reporting Issues

OMB Circular A-123, Management Accountability and Control, provides guidance to Federal managers on improving management controls to ensure that (1) programs achieve their intended results; (2) resources are used consistent with agency missions; (3) programs and resources are protected from waste, fraud, and mismanagement; (4) laws and regulations are followed; and (5) reliable, timely information is obtained, maintained, reported, and used for decisionmaking.

During FY 2003, several HHS operating divisions improved their financial accounting and supervisory review processes, including the preparation of more timely account analyses and periodic reconciliations. However, our review disclosed numerous weaknesses in some operating divisions' ability to report accurate, timely financial information. Certain reconciliation processes 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.

In prior years, HHS had sufficient time for significant analyses by its own staff, as well as outside consultants, in the months after the close of the year. This time was necessary to determine proper balances for financial reporting purposes. With the accelerated closing process in FY 2003, this analysis period was substantially shortened and presented significant challenges. Had the operating divisions followed departmental policies and conducted all required financial analyses

and reconciliations throughout the year, many account anomalies would have been detected earlier. The need for enhanced periodic reconciliation and analysis procedures is illustrated by matters noted at CMS, the entities supported by the Program Support Center, and NIH.

Centers for Medicare & Medicaid Services. Pending implementation of HIGLAS, strong oversight of the Medicare contractors and properly trained personnel are needed to (1) reduce the risk of material misstatements in financial data and (2) ensure that periodic analyses and reconciliations are completed to detect and resolve errors and irregularities in a timely manner. We identified improvements in CMS's oversight of the Medicare contractors during the current year; however, continuing weaknesses affected CMS's ability to analyze and accurately report financial information on a timely basis.

CMS reported that during the year, certified public accountants contracted to review Medicare contractors' accounts receivable transactions discovered a total of $98.3 million in errors. Collectively, these errors resulted in an $11.6 million overstatement of accounts receivable, which CMS corrected. These errors were attributable, in part, to the following internal control weaknesses identified through CMS procedures:

- Contractors did not send demand letters in a timely manner, contrary to existing policy and procedures.
- Contractors did not maintain adequate audit trails for Medicare secondary payer recoveries.
- Contractors did not implement policies and procedures to accurately refer debt to Treasury for collection.
- Contractors did not maintain adequate documentation to support the classification, accumulation, or reporting of accounts receivable.
- Contractors did not accurately calculate interest on outstanding accounts receivable.

During our testing of accounts receivable at nine Medicare contractors, we noted other indicators of control weaknesses that are also attributable to the previously discussed system weaknesses. The manual processes that CMS and the contractors implemented to track and report accounts receivable were inefficient, labor intensive, and subject to the types of internal control findings noted below:

- At one contractor, credit balances owed to providers were inappropriately offset against valid accounts receivable due from other providers.

- A contractor inappropriately excluded from the 750/751 report cash received but not applied against a corresponding account receivable.

- Three contractors did not maintain documentation to support the application of cash against existing accounts receivable.

- We could not reconcile a contractor's detailed accounts receivable reports to the aging of accounts receivable on the 750/751 reports.

- We could not reconcile the periodic interim payment receivable balances to the supporting documentation at one contractor.

- An allowance for doubtful accounts was understated because a contractor had failed to accurately report the corresponding accounts receivable balance.

- One contractor did not apply cash received against existing accounts receivable in a timely manner.

Entities Supported by the Program Support Center. More robust and timely financial analyses and reconciliations are critical to reduce the likelihood of errors in the financial statements of the entities supported by the Program Support Center and to effectively accumulate, assemble, and analyze information to timely develop financial statements. For example:

- To prepare financial statements, more than 175 entries with an absolute value of approximately $123 billion were recorded outside the general ledger system. Many of these accounting entries were made to record yearend accruals, adjust between governmental and nongovernmental accounts, record expenditures not posted to the general ledger prior to the month-end close, adjust proprietary to budgetary accounts, and post reconciliation adjustments. A majority of the entries could have been eliminated by more timely analyses and reconciliations, as well as improved estimation methodologies.

- For FY 2002 and prior years, approximately 98,000 entries totaling $1.8 trillion remained in the detail supporting the general ledger. Most of these entries were posted to ensure agreement between the subsidiary ledgers and the general ledgers, to record budgetary entries, and to record depreciation for capitalized property maintained by the operating divisions. Maintaining supporting subsidiary ledgers would greatly facilitate the financial reporting process.

- The accounts payable subsidiary ledgers included transactions with an absolute value of $4.1 billion that had to be deducted from the subsidiary balance in order to reconcile to the

general ledger. Approximately $1.3 billion related to balances aged 3 years and older, dating back as early as 1989.

- On a monthly basis, the Program Support Center is responsible for reconciling approximately 250 Treasury appropriation symbols. The Center prepares four separate monthly reports that reconcile the general ledger with Treasury's records. As of September 30, 2003, the general ledger and Treasury's records differed by approximately $142 million (net). Management could not explain the variance. In addition, one of the reports generated to compare detailed transactions in the general ledger with Treasury's records had lost its usefulness due to old and invalid items that remained in the general ledger. For example, the September 30, 2003 report identified approximately $46 billion of differences in transactions dating back as early as 1990. Management indicated that due to staffing limitations, the Center primarily focused on the larger, more recent differences.

- A high-level, exception-based analysis was not performed sufficiently to ensure that management had a comprehensive understanding of what activities had occurred during the year that affected account balances. Trending analyses by the Center and the supported operating divisions on the March 30 and September 30, 2003 financial statements contained many documented explanations that were incomplete and required additional research as to why certain trends occurred.

- Contrary to HHS policy, complete, periodic reconciliations of appropriated capital used and budgetary accounts were not performed until yearend. As a result, approximately 1,400 miscellaneous adjustments with an absolute value of $35 billion were recorded to various net position accounts. Additionally, unsupported entries were recorded to the beginning-of-period unobligated balances to ensure that the trial balance agreed with the FY 2002 audited ending unobligated balances. For example, a $397 million adjustment was recorded to ACF to ensure that balances agreed between years within the statement of budgetary resources. Other unexplained differences existed in preparing budgetary reporting and other financial schedules.

- Although final financial statements were completed before the November 7, 2003 FACTS II fourth-quarter submission deadline, the September 30, 2003 trial balance of accounts used to prepare the financial statements differed from that submission by over $2 billion. As of the end of fieldwork, the differences had not been fully identified to us, and the financial statements could not appropriately disclose such differences, if any.

- In the area of credit reform reporting, the manual adjustments processed through the financing account resulted in unusual and unexplained activity. In addition, the liquidating account currently reflects cumulative results of operations of approximately $300 million. Such balances are more appropriately reflected in a Due to Treasury account, as the

resulting resources from collecting the liquidating accounts receivable are to be transmitted to Treasury and not retained by the Department.

National Institutes of Health. The NIH financial systems did not facilitate automatic reconciliation between general ledger accounts and subsidiary accounts. In addition, the financial analysis and reconciliation procedures in place during FY 2003 were challenged to provide reliable information needed for the consolidation process. For instance, to prepare the FY 2003 financial statements, NIH recorded 46 entries with an absolute value of $39.6 billion outside the Central Accounting System. The adjustments included entries related to removing an appropriation included in the trial balance but not reported on the NIH financial statements, reclassifying Standard General Ledger account balances, recording revenue, removing canceled expired annual accounts not yet closed, adjusting for depreciation expense, correcting cash in the suspense account, and reversing FY 2002 yearend accruals and recording FY 2003 yearend accruals.

Recommendations

Pending installation of the new systems under development, routinely meeting accelerated reporting deadlines without heroic efforts will require a change in processes. We recommend that the Assistant Secretary for Budget, Technology, and Finance (ASBTF):

- ensure that CMS, NIH, and the Program Support Center implement corrective actions, pending full operation of HIGLAS, the NIH Business System, and the Unified Financial Management System, respectively, to mitigate system deficiencies that impair the capability to support and report accurate financial information;

- ensure that the operating divisions (1) develop formal procedures to conduct periodic, detailed reviews and analyses of transactions within the subsidiary ledgers and (2) establish controls to identify, research, and resolve significant accounting anomalies in a timely manner;

- oversee CMS's corrective actions to provide a mechanism for central and regional office monitoring of contractors' activities and enforcement of compliance with CMS financial management procedures;

- ensure that the operating divisions allocate adequate resources to perform required account reconciliations and analyses monthly;

- direct that the operating divisions prepare quarterly reports on the status of corrective actions on recommendations identified in the individual operating division reports on internal controls; and

- ensure, as required by OMB Bulletin 01-09, Form and Content of Agency Financial Statements, the preparation of future years' interim financial statements supported by reconciliations and account analyses to ensure such reporting is accurate for decisionmaking.

Medicare Information Systems Controls (Repeat Condition)

Our review of Medicare information systems controls continued to disclose weaknesses in general and application controls at Medicare contractors, data centers where Medicare claims are processed, maintainers of "shared" application system software used in claim processing, and the CMS central office. The number of identified weaknesses remained consistent with that found in FYs 2001 and 2002.

General controls affect the integrity of all applications operating in the claim processing environment—whether at an individual location or across the Medicare fee-for-service system as a whole. They include the entity-wide security program, access controls (physical and logical), application development and program change controls, segregation of duties, operating systems software, and service continuity. Application controls include input, processing, and output controls related to specific applications.

To administer the Medicare program and to process and account for Medicare expenditures, CMS relies on extensive, interdependent information systems operations at its central office and Medicare contractor sites. The central office systems maintain administrative data, such as Medicare beneficiary enrollment, eligibility, and paid claims data, and process all payments for managed care. The Medicare contractors and data centers use several shared systems to process and pay fee-for-service claims. All of the shared systems, which are maintained by "system maintainers," interface with the CMS Common Working File (CWF) to obtain authorization to pay claims and to coordinate Medicare Parts A and B benefits. Strong internal controls over these operations are essential to ensure the integrity, confidentiality, reliability, and availability of critical data while reducing the risk of errors, fraud, and other illegal acts.

Audit Scope

Our full-scope CFO audits included general controls at 17 sites: the CMS central office and 16 Medicare contractors. We reviewed application controls at the CMS central office for several systems integral to Medicare financial information. We also reviewed application controls at six of the Medicare contractors that included the Fiscal Intermediary Standard System (FISS), the Viable Information Processing Systems (VIPS) Medicare System (VMS), the Arkansas Part A Standard System (APASS), the Multi Carrier System (MCS) and the Common Working File (CWF) System. Our audit also relied on the work and findings of the (SAS) 70 reviews for the 16 Medicare contractors audited.

Further, we conducted vulnerability reviews of network controls at the same 17 sites. The vulnerability reviews included external penetration testing at 16 of the 17 sites (1 site did not permit such testing) and internal penetration testing and network vulnerability assessments, including security configurations of network servers, at all 17 sites. Both the scope of the vulnerability testing and the number of sites tested were significantly expanded this year.

Additionally, we followed up on selected prior-year findings at six other Medicare contractor locations. These reviews were performed, in part, to verify the status of corrective actions taken by the contractors and to validate CMS's process for ensuring timely and effective correction of reported weaknesses.

Control Weaknesses Noted

As in previous years, we identified a number of general and application control weaknesses. Vulnerability testing also disclosed numerous security settings/controls that required enhancement. The majority of weaknesses were noted at the Medicare contractors, rather than the CMS central office. Our procedures disclosed no evidence of actual system compromise of security; however, we consider the cumulative effect of the weaknesses noted to represent a material weakness. Areas where weaknesses were identified are described below.

Entity-Wide Security Programs. These programs provide the foundation for an organization's security culture and awareness. A sound program ensures effective security controls throughout the organization. We noted that several contractor locations lacked a robust, detailed entity-wide security program. At these locations, security was treated as a directive, rather than a cultural norm that guides daily activities. As a result, numerous weaknesses were noted in the areas of access and systems software controls. Two overriding factors in the pervasiveness of poor security controls were that these sites had assigned security administration duties to personnel who did not possess the proper background and education and that resources were only minimally directed to security programs, training, and understanding.

Other personnel-related security issues were found as well. At some sites, security administration duties were improperly segregated from the duties of application programming. Other sites did not conduct sufficient background checks on certain contracted support personnel and did not periodically reinvestigate staff in sensitive positions or with increased job responsibilities involving access to sensitive records and/or facilities.

Security controls cannot be effective without a robust, detailed entity-wide security program that is fully sponsored and practiced by senior management. Proper training and understanding, as well as security personnel with the proper background and education, are necessary to ensure the function of the program.

Logical and Physical Access Controls. Physical access controls ensure that critical systems assets are physically protected from unauthorized access, and logical controls provide assurance

that only authorized personnel may access data and programs maintained on systems. Our vulnerability testing noted many security settings/controls that required enhancement. Our external penetration testing was successful at multiple sites, primarily due to poor or nonexistent security settings resulting from the lack of sufficient security configuration standards for network computers. In addition, we were easily able to bypass security controls without prior knowledge of the systems tested, and numerous security weaknesses existed that would allow internal users to easily access sensitive systems, programs, and data without proper authorization. Our review did not disclose any exploitation of the critical systems tested.

A lack of specific guidance on computer security configuration settings and ineffective entity-wide security programs administered by personnel without proper knowledge and experience prevent contractors from providing adequate security controls to ensure that only properly authorized personnel access sensitive CMS data and programs.

Application Security, Development, and Program Change Controls. Application security, development, and program change controls provide assurance that programs are developed with standards that ensure their effectiveness, efficiency, accuracy, security, and maintenance and that only authorized and properly tested programs are implemented for production use. We noted that contractor-based processing sites had the ability to turn on and off front-end edits in the Fiscal Intermediary Standard System and that some transactions bypassed CWF processing. These application control issues are an important area of concern; they could affect the accuracy and completeness of Medicare fee-for-service data used for adjudication of claims and ultimately entered into the National Claims History System for programmatic decision support. Additionally, we noted that application changes were being implemented without complete testing and that application change control procedures were not followed at several sites, including the CMS central office. Also, at several sites, application programmers had the ability to directly update production source code for applications, thereby bypassing application change controls.

Systems Software. Systems software is a set of computer programs designed 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 noted numerous weaknesses in systems software settings/controls for network servers.

- ***Changes to systems software.*** Systems software change procedures and/or controls were not in place or consistently followed at many of the sites tested. Failure to control systems software changes can seriously affect the security and effectiveness of data and operations because systems software provides the foundation to operate all of the computers used.

- ***Access to systems software programs and files.*** We noted numerous instances of poor password controls that could allow unauthorized access to systems software programs and files. These weaknesses related to systems software on mainframe, Windows, and Unix systems, as well as firewall and router servers. The lack of security configuration

standards contributed to the weaknesses noted and to the ability to penetrate multiple sites tested.

Service Continuity Planning and Testing. Service continuity relates to the readiness of a site in the case of a system outage or an event that disrupts normal processing of operations. Without approved, documented, and tested business and system continuity plans, there is no assurance that normal operations will be recovered efficiently and timely. We noted incomplete plans and inadequate testing at contractor sites and the CMS central office. Failure to ensure complete, tested, and viable plans could severely affect CMS processing operations.

Conclusions and Recommendations

During FY 2003, CMS made progress by issuing the "Acceptable Risk Safeguards" document. This document provides much greater specificity on security standards and will complement the "Business Partners Systems Security Manual" previously provided to Medicare contractors. CMS has also continued to review the contractors through SAS 70 audits and an extensive contractor self-assessment and reporting process. Additionally, CMS has requested and received system security plans from its contractors and has a promising certification and accreditation program initiative featuring system vulnerability assessments.

Efforts to address the findings noted during our audit within budgetary constraints are challenged by the decentralized nature of Medicare operations and the complexity of fee-for-service processing. CMS has indicated that the President's budget for FY 2004 includes a funding request for information technology modernization. According to CMS officials, its modernization program represents a long-term solution to simplify the application software code and change controls needed for more robust security. CMS has also stated that its contractor reform initiative, including data center consolidation, will shorten the security perimeter by reducing the number of contractors and data centers. We agree that contractor reform and systems modernization will facilitate implementation of an improved systems security posture over the longer term; however, persistent weaknesses in internal controls throughout the Medicare system must be addressed in the interim.

We recommend that ASBTF (1) ensure that CMS identifies and implements corrective actions to address the causes of Medicare systems control weaknesses within current legislative, policy, and budgetary constraints; (2) work with CMS in assessing, and finding ways to address, the shortfall in information technology resource needs; and (3) work with the administration and the Congress to promote Medicare reforms and modernization that will facilitate implementation of improved and cost-effective internal controls. Detailed recommendations are contained in the CMS financial statement audit report, our reports issued pursuant to the Federal Information Security Management Act (FISMA), and the individual reports issued to the Medicare contractors and the CMS central office.

REPORTABLE CONDITION

Departmental Information Systems Controls (Repeat Condition)

As was the case at CMS, we identified a number of significant deficiencies in the design and operation of information systems controls at the other operating divisions. Detailed descriptions of control weaknesses may be found in SAS 70 reports, our FISMA reports, and the management letters issued on each system review.

Our procedures in connection with the financial statement audit process continued to identify general control issues with respect to access controls, application development and change controls, internal vulnerability assessments, entity-wide security program planning and management, and service continuity/disaster recovery. We also found weaknesses in application controls. For example, at one location, supervisory personnel at the local personnel offices did not validate sensitive personnel transactions, such as promotions, before sending the transactions to the central processing point. None of these general or application control issues individually is reportable; however, the nature and extent of weaknesses found throughout the Department indicates that there is much room for improvement.

In addition, during this year's FISMA evaluation, we identified fundamental security program weaknesses that inhibited the Department's ability to create a more mature security environment. Specifically, weaknesses were identified in:

- the integration of security into the system development life cycle,
- capital budgeting to address systems security needs,
- recording and reporting of identified security weaknesses and tracking their resolution through plans of action and milestones,
- the classification of systems as to their mission criticality and sensitivity of data,
- security training and awareness, and
- the security incident response process.

We concluded that the Department did not have an effective information security management structure in place to ensure that sensitive data and critical operations received attention and that appropriate security controls were implemented to protect those operations. Overall, the weaknesses left the Department vulnerable to (1) unauthorized access to and disclosure of sensitive information, (2) malicious changes that could interrupt data processing or destroy data files, (3) improper payments, or (4) disruption of critical operations. In accordance with OMB

criteria, we found a total of 60 deficiencies across the Department, not including CMS. Of the 60 deficiencies, 26 were significant. However, we did not find any evidence that these vulnerabilities had been exploited.

Recognizing that improvements in general controls are necessary, the Department is promulgating updated policies to address areas of concern. Additional efforts to promote effective and continuing compliance with these policies and to expand coverage to application controls may be needed.

Recommendation

We recommend that ASBTF ensure that the operating divisions and service organizations address general and application control weaknesses. Specific recommendations are contained in the individual audit reports.

OTHER MATTERS

Integration of Performance Reporting With Financial Reporting

The Department manages more than 300 programs under its 12 operating divisions and uses more than 650 performance measures to direct program activities and assess progress and achievement. Due to the complexity and volume of the measures, the Department faces significant challenges in meeting the consolidated performance reporting requirements of the Government Performance and Results Act of 1993, OMB Circular A-11, and OMB Bulletin 01-09. Based on OMB guidance on FY 2003 performance reporting, the Department may meet the aforementioned requirements by addressing key performance measures in the FY 2003 "Performance and Accountability Report" with reference to the individual operating divisions' performance reports.

Working with OMB, the Department has taken initial steps toward integrating performance reporting requirements in its FY 2005 One-HHS Action Plan. However, additional effort should be focused on presenting a clearer linkage of the discussion of performance by major goals in the HHS strategic and performance plans to the operating divisions' statements of net cost. Furthermore, the Department should reassess the consistency and data availability of the indicators reported as significant in section II of the "Performance and Accountability Report," as well as the annual performance plans and reports submitted to OMB. For instance, five of the indicators identified as significant in the Management Discussion and Analysis (and section II) are not included in the FY 2004 annual performance plan, and two of the indicators are not included in the draft FY 2005 One-HHS Action Plan. Furthermore, 15 of the indicators identified as significant did not have actual performance results for FY 2003, of which 4 had no actual results for FY 2002 and 1 had no actual results for FY 2001. We were unable to reconcile the supporting documentation provided for some of the indicators.

HHS should continue to work with OMB on consolidated performance reporting requirements and should ensure that measures are clearly linked to the operating divisions reported on the statement of net cost.

Intragovernmental Transactions

Under OMB Bulletin 0l-09, Form and Content of Agency Financial Statements, Government entities are required to reconcile intragovernmental transactions with their trading partners. Some operating divisions were not able to timely and accurately eliminate trading partner information.

Beginning in FY 1966, CMS accrued expenses for Medicaid benefits incurred but not reported. As of September 30, 2003, these accrued expenses exceeded the available unexpended Medicaid appropriations by $8.5 billion. CMS's Office of General Counsel determined that the indefinite authority provision of the Medicaid appropriations allowed the entire accrued expense to be reported as a funded liability. While Department of the Treasury officials agreed that there was a legal basis for recording the accrued benefit liability, they did not agree to recognize the accounting entry on their records.

A somewhat similar problem occurred in the Supplementary Medical Insurance Program, where section 1844 of the Social Security Act authorizes funds to be appropriated to match Medicare beneficiary premiums. The appropriated amount is an estimate calculated annually by CMS. This year's funding estimate was insufficient to match beneficiaries' premiums by $3.4 billion. HHS discussed these issues with OMB officials, who agreed that the longstanding accounting for these issues should continue for FY 2003. OMB asked that HHS seek further clarification with the Federal Accounting Standards Advisory Board on these issues. Until these matters are resolved, differences between records of the operating divisions and the Department of Treasury will remain.

* * * * *

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

Dara Corrigan
Acting Principal Deputy
Inspector General

November 14, 2003
A-17-03-00001

INDEPENDENT AUDITOR REPORT ON COMPLIANCE WITH LAWS AND REGULATIONS

To: The Secretary of Health
and Human Services

We have audited the financial statements of the Department of Health and Human Services (HHS) as of September 30, 2003 and have issued our report, dated November 14, 2003, on those statements. 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 01-02, Audit Requirements for Federal Financial Statements.

The management of HHS is responsible for complying with laws and regulations applicable to HHS. As part of obtaining reasonable assurance about whether the HHS financial statements are free of material misstatement, we performed tests of HHS's 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 with certain other laws and regulations specified in OMB Bulletin 01-02, including the requirements referred to in the Federal Financial Management Improvement Act (FFMIA) of 1996. We limited our tests of compliance to these provisions and did not test compliance with all laws and regulations applicable to HHS.

We were unable to fully test consolidated performance reporting requirements of the Government Performance and Results Act (Public Law 103-62), OMB Circular A-11, and OMB Bulletin 01-09. By letter dated October 30, 2003, OMB said that for FY 2003 performance reporting, HHS should (1) present the significant measures in the Management Discussion and Analysis and Section II of the FY 2003 Performance and Accountability Report with reference to individual operating division plans and (2) issue to the Congress no later than February 27, 2004 a separate FY 2005 annual performance plan combined with the FY 2003 annual performance report. Since the issuance of the operating divisions' plans will be subsequent to the completion of our fieldwork, we were unable to fully assess compliance with the Government Performance and Results Act, OMB Circular A-11, and OMB Bulletin 01-09 as they relate to consolidated performance reporting requirements.

Other than the matter discussed below, the results of our tests of compliance with laws and regulations disclosed no instances of noncompliance under "Government Auditing Standards" and OMB Bulletin 01-02.

Under FFMIA, we are required to report whether HHS financial management systems substantially comply with Federal financial management systems requirements, applicable Federal accounting standards, and the U.S. Government Standard General Ledger 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, described below, in which HHS financial management systems did not substantially comply with certain requirements:

- The financial management systems and processes used by HHS and the operating divisions made it difficult to prepare reliable and timely financial statements. The processes required the use of extensive, time-consuming manual spreadsheets and adjustments in order to report reliable financial information.

  - The Centers for Medicare & Medicaid Services did not have an integrated accounting system to capture expenditures at the Medicare contractor level, and certain aspects of the financial reporting system did not conform to the requirements specified by the Joint Financial Management Improvement Program. Extensive consultant support was needed to establish reliable accounts receivable balances.

  - At most operating divisions, suitable systems were not in place to adequately support sufficient reconciliations and analyses of significant fluctuations in account balances. In addition, some systems were not designed to apply the U.S. Standard General Ledger at the transaction level.

- General and application controls over Medicare financial management systems, as well as systems of certain other operating divisions, were significant departures from requirements specified in OMB Circulars A-127, Financial Management Systems, and A-130, Management of Federal Information Resources.

Our report on internal controls includes information on the financial management systems that did not comply with requirements, relevant facts pertaining to the noncompliance, and recommended remedial actions. HHS has developed a Departmentwide corrective action plan to address FFMIA and other financial management issues. Although certain milestone dates have passed, we recognize that the plan will require periodic updating to reflect changed priorities and available resources.

In connection with our audits, and as further described in our report on internal controls, we identified potential violations of laws and regulations regarding capital leasing activities. Such matters have been referred to the Department for further analysis and resolution as appropriate. Providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit; accordingly, we do not express such an opinion.

* * * * *

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

Dara Corrigan
Acting Principal Deputy
Inspector General

November 14, 2003
A-17-03-00001

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Washington, D.C. 20201

NOV 15 2003

Ms. Dara Corrigan
Acting Principal Deputy Inspector General
Department of Health and Human Services
Washington, DC 20201

Dear Ms. Corrigan:

This letter responds to the opinion submitted by the Office of Inspector General on the Department of Health and Human Services' fiscal year 2003 audited financial statements. We concur with your findings and recommendations.

We are very pleased that, once again, your report reflects an unqualified, or "clean," audit opinion for the Department. Through our joint effort, we were able to achieve both a clean and timely departmental financial statement audit.

We also acknowledge that we continue to have serious internal control weaknesses in our financial systems and processes. The Department's long-term strategic plan to resolve these weaknesses is to replace the existing accounting systems and certain other financial systems within the Department with a Unified Financial Management System (UFMS). HHS is well on its way to implementing this new system. The National Institutes of Health implemented their new general ledger in October 2003. Additionally, the Centers for Medicare & Medicaid Services has begun the implementation process with two of their major Medicare contractors. UFMS will be implemented in accordance with the approved implementation plan allowing HHS to comply with the requirements of the Federal Financial Management Improvement Act by the end of fiscal year 2005. We plan to fully implement the UFMS Departmentwide by 2007.

I would like to thank your office for its continuing professionalism during the course of the audit.

Sincerely,

Kerry Weems
Acting Assistant Secretary for Budget,
Technology, and Finance