that improved financial information will provide for better decision-making, potential cost savings, and a means to meet current Federal accounting and budgetary reporting requirements. However, the system is not expected to be fully operational until 2005.

Administration for Children and Families. The ACF, the second largest operating division with net budget outlays of $37.5 billion, prepared its financial statements more accurately and more timely than last year, largely as a result of having performed many of the required reconciliations and analyses during the year. But many "Fund Balance with Treasury" reconciliations were performed late, and most of the required budgetary account reconciliations were not performed until yearend to prepare the financial statements.

Fund Balance with Treasury reconciliations deserve particular mention because the differences between the general ledger and the Department of the Treasury's records were so great. At various times, the difference ranged from $200 million to $6.3 billion. This suggests that ACF did not post transactions timely or accurately; in our testing, we found instances of this problem. For example, we noted that a $143 million transaction had been posted to the wrong appropriation and remained uncorrected for over a year.

Recommendations. We recommend that the Assistant Secretary for Management and Budget (ASMB):

- direct each operating division to establish controls to identify and report significant accounting anomalies to top management;
- direct the CFO of the Program Support Center to communicate accounting and control problems more effectively to the CFOs of serviced entities;
- direct that operating division CFOs work with their program office counterparts to develop procedures for analyzing and explaining unusual changes in account balances;
- oversee and maintain close liaison with entities serviced by the Program Support Center and CFO offices during the installation of new systems or the revision of operating procedures;
- continue to support the development of the HCFA Integrated General Ledger Accounting System and oversee its implementation;

- monitor HCFA's corrective actions to strengthen regional office and contractor monitoring of accounts receivable and to ensure that key financial reconciliations are performed timely;

- consider directing operating division CFOs to prepare and analyze interim financial statements, particularly the statements of net cost, budgetary resources, and financing, as an aid in the reconciliation and analysis process; and

- require each operating division to prepare quarterly reports on the status of corrective actions on recommendations in the specific CFO reports on internal controls. The ASMB, in turn, should summarize and report quarterly on these actions to the Deputy Secretary and OIG.

2. Medicare Electronic Data Processing (Repeat Condition)

The HCFA relies on extensive electronic data processing (EDP) operations at both its 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 critical data while reducing the risk of errors, fraud, and other illegal acts.

The HCFA central office systems maintain administrative data, such as Medicare enrollment, eligibility, and paid claims data, and process all payments for managed care. In FY 2000, managed care payments totaled about $39.8 billion. The Medicare contractors and data centers use several "shared" systems to process and pay fee-for-service claims. All of the shared systems interface with HCFA's Common Working File (CWF) to obtain authorization to pay claims and to coordinate Medicare Part A and Part B benefits. This network accounted for and processed $173.6 billion in Medicare expenditures during FY 2000.

Our review of EDP internal controls covered general and application controls. General controls involve the entity-wide security program, access controls, application development and program change controls, segregation of duties, operating system software, and service continuity. General controls affect the integrity of all applications operating within a single data processing facility and are critical to ensuring the reliability, confidentiality, and availability of HCFA data. Application controls involve input, processing, and output controls related to specific EDP applications.

We completed general control reviews at nine Medicare data processing facilities that support the Medicare contractors sampled. In addition, we assessed application controls of the Fiscal Intermediary Shared System (FISS), the Multi-Carrier System, and the CWF at three separate

contractors. At the HCFA central office, we updated the status of prior-year findings concerning general controls.

We found numerous EDP general control weaknesses, primarily at the Medicare contractors. Such weaknesses do not effectively prevent (1) unauthorized access to and disclosure of sensitive information, (2) malicious changes that could interrupt data processing or destroy data files, (3) improper Medicare payments, or (4) disruption of critical operations. Further, weaknesses in the contractors' entity-wide security structure do not ensure that EDP controls are adequate and operating effectively.

As noted in the following table, a total of 124 weaknesses were identified. The majority were found at the Medicare contractors, and most (about 80 percent) involved three types of controls: access controls, entity-wide security programs, and systems software. While individually the conditions found are not material, the cumulative effect is material.

General Control Audit Areas	Number of Weaknesses		Total
	Central Office	Medicare Contractors	
Access controls	2	55	57
Entity-wide security programs	4	17	21
Systems software	1	20	21
Service continuity/contingency planning	-	11	11
Segregation of duties	1	7	8
Application software development and change controls	1	5	6
Total	**9**	**115**	**124**

Access controls. Access controls ensure that critical systems assets are physically safeguarded and that logical access to sensitive computer programs and data is granted only when authorized and appropriate. Closely related to these controls are those over computer operating systems and data communications software. These controls further ensure that only authorized staff and computer processes 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. However, access control weaknesses represented the largest problem area. Of the 124 EDP control weaknesses reported, 57, or 46 percent, related to access controls.

- ***Administration of access controls*** (29 conditions: 27 at 11 Medicare contractor sites and 2 at the HCFA central office). In numerous instances, passwords were not properly administered, systems security software was not implemented effectively, or access privileges were not reviewed frequently enough to ensure their continuing validity.

- ***Access to computer programs and system files*** (5 conditions at 5 Medicare contractor sites). At some sites, installation-level controls over critical system software libraries were inadequate, and programmers were inappropriately allowed access to production software program libraries. We also noted cases in which programmers had inappropriate access to system logs; this provided an opportunity to conceal improper actions and obviated the logs' effectiveness as a detect control. At another site, the computer operator could override installation system security precautions when restarting the mainframe computer system.

- ***Access to sensitive data*** (15 conditions at 9 Medicare contractor sites). These are instances in which computer programmers and/or other technical support staff had inappropriate access to the data files used in the claim process. At several sites, programmers had inappropriate access to beneficiary history files. Under these conditions, the CWF system was vulnerable to inappropriate use. At several other sites, programmers had inappropriate access rights to production files, including beneficiary history and other sensitive data. Also, users of one contractor's local area network could access Medicare program data without adequate controls. During vulnerability testing at three Medicare contractor sites, excessive remote access attempts were permitted and more information about the computers being tested was disclosed than necessary. Such weaknesses increase the risk of unauthorized remote access to sensitive Medicare systems.

- ***Physical access*** (8 conditions at 5 Medicare contractor sites). These include weaknesses in controls over access to sensitive facilities and media within those facilities. For example, at one contractor, inappropriate individuals had access to the computer center's command post. At another, the computer production control area was not secured during normal business hours.

Entity-wide security programs. These programs are intended to ensure that security threats are identified, risks are assessed, control objectives are formulated, control techniques are developed, and management oversight is applied to ensure the overall effectiveness of security measures. Programs typically include policies on how and which sensitive duties should be separated to avoid conflicts of interest. Likewise, 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, computer-based operations. Of the 124 EDP control weaknesses reported, 21, or 17 percent, related to security program weaknesses.

- ***Entity-wide plans*** (8 conditions at 8 Medicare contractor sites). Eight contractor sites lacked fully documented, comprehensive entity-wide security plans that addressed all aspects of an adequate security program. One site also had no mechanism for ensuring that system audit findings were effectively addressed and resolved.

- ***Implementation of entity-wide plans*** (13 conditions: 9 at 6 Medicare contractor sites and 4 at the HCFA central office). Inadequate risk assessments, a lack of comprehensive security awareness programs, and inadequate policies were among the weaknesses reported at the contractors. At the HCFA central office, four conditions remained reportable: no security assessment of, or security plans for, significant application systems; deficiencies in the security plan accreditation process; insufficient security oversight of the Medicare contractors; and no formal process to remove system access of terminated HCFA employees and contractors.

Systems software controls. Systems software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, it is used to support and control a variety of applications that may run on the same computer hardware. Systems software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system. Some systems software can change data and programs on files without leaving an audit trail. Of the 124 EDP control weaknesses, 21, or 17 percent, related to weaknesses in systems software controls (20 at 7 Medicare contractor locations and 1 at the HCFA central office). Problems related to managing routine changes to systems software to ensure their appropriate implementation and configuring controls associated with the operating system to ensure their effectiveness. Such problems could weaken critical controls over access to sensitive Medicare data files and operating system programs.

Shared system weaknesses. We found that the prior control weakness related to the Medicare data centers' having full access to the FISS source code remained unresolved. This weakness has been expanded to include the CWF system, since the design of the CWF software provides for programmer update access to CWF data files to meet operational needs. As we previously reported, Medicare data centers had access to the FISS source code and were able to implement local changes to FISS programs. Such access may be abused, resulting in the implementation and processing of unauthorized programs at contractor data centers. While HCFA requires

contractors to restrict local changes to emergency situations, local changes are often not subjected to the same controls that exist in the standard change control process.

HCFA central office. Our followup work found that the HCFA central office had resolved the prior-year deficiency in mainframe database access controls. The central office has also continued to implement enhanced control procedures, specifically in access controls and application development and program change controls. However, actions were still underway as of the end of FY 2000. Improvements not yet completed included:

- issuance of task orders to various contractors to address issues related to risk assessment, security policies and procedures, independent verification and validation of entity-wide security plans, and related procedures for significant systems and

- migration to enterprise-wide program change management software, with full implementation planned during FY 2001.

Recommendation. We recommend that ASMB oversee HCFA's identification and implementation of corrective actions to address the fundamental causes of Medicare EDP control weaknesses. Detailed recommendations are contained in the HCFA audit report.

REPORTABLE CONDITIONS

1. Medicaid Estimated Improper Payments (Repeat Condition)

The Medicaid program, enacted in 1965 under Title XIX of the Social Security Act, is a grant-in-aid medical assistance program largely for the poor, the disabled, and persons with developmental disabilities requiring long-term care. Funded by Federal and State dollars, the program is administered by HCFA in partnership with the States via approved State plans. Under these plans, States reimburse providers for medical assistance to eligible individuals, who numbered more than 33 million in 2000. In FY 2000, Federal and State Medicaid outlays totaled $207.1 billion; Federal expenses were $118.7 billion.

We found that HCFA still lacked a methodology to estimate the extent of improper Medicaid payments on a national level. For the last 5 years, OIG reviewed a statistical sample of Medicare claims and estimated the extent of payments that did not comply with laws and regulations. The majority of errors fell into four broad categories: unsupported services, medically unnecessary services, incorrect coding, and noncovered services. This information helped HCFA to monitor and reduce improper Medicare payments. Because HCFA has not established a similar methodology for the Medicaid program, it cannot reach conclusions on the extent of Medicaid

payment errors. We recognize that Medicaid is a State-administered program, so estimates of improper payments will require the cooperation of States.

Our prior report recommended that HCFA work with the States to develop procedures and implement a methodology for determining the extent of improper Medicaid payments. We noted some recent progress in this area. A project coordinator has begun requesting State participation in a pilot error rate project.

Recommendation. We recommend that ASMB and HCFA continue to work with the States to develop procedures and implement a methodology for determining the extent of improper Medicaid payments.

2. Departmental Electronic Data Processing (Repeat Condition)

The following summarizes some of the systemic EDP control weaknesses identified in audits of operating division financial statements and service organization operations. Other weaknesses are reported in the individual reports on these entities. We note that NIH has resolved the previous year's reportable findings related to systems access controls.

Division of Financial Operations. The Program Support Center's DFO uses several automated systems to provide financial services to certain operating divisions. While DFO continues to strengthen controls over these systems, further improvements are needed.

- The DFO entity-wide security program lacked a formal risk assessment, a formal security plan, and adequate personnel security policies. In addition, the security features of the DFO accounting system (CORE) were not accredited as required by OMB Circular A-130. Such weaknesses in the entity-wide security structure limited assurance that EDP controls were adequate and operating effectively.

- The DFO policy for application change control included no formal test procedures and lacked adequate emergency change procedures, as well as adequate library management software. Additionally, DFO did not consistently follow its documented application change control procedures. For example, change request forms, used to ensure that software changes are approved and documented, were not always complete; supervisory approval of program modifications was not consistently documented; and "before and after" images of program code were not compared to ensure that only approved changes were made to the CORE application.

- A penetration test of the DFO internal network and computing resources to assess the security of systems and to identify vulnerabilities determined that user account policies and administrative passwords on servers were weak. This type of weakness increases to a high level the risk that the system will be compromised by unauthorized users.

Food and Drug Administration. In FY 1999, FDA had several findings under each of the six major categories of general controls. Although FDA resolved many of these findings, some were still outstanding this year. When viewed in the aggregate, these exceptions constituted a reportable condition. Areas still in need of improvement included the entity-wide security program, access controls, software application change controls, and service continuity.

Recommendation. We recommend that ASMB oversee the efforts of the operating divisions and service organizations to improve security issues, system access controls, application change controls, and service continuity plans. Specific recommendations are covered in the individual audit reports.

OTHER MATTERS

FMFIA Reporting

As part of our audit, we also obtained an understanding of management's process for evaluating and reporting on internal control and accounting systems, as required by the Federal Managers' Financial Integrity Act (FMFIA), and compared the material weaknesses reported in the HHS FY 2000 FMFIA report relating to the financial statements under audit with the material weaknesses noted in our report on internal controls. Under OMB guidelines for FMFIA reporting, HHS reports as a material weakness any deficiency the Secretary determines to be significant enough to be disclosed outside the agency. This designation requires HHS management to judge the relative risk and significance of deficiencies. In making this judgment, HHS management pays particular attention to the views of the HHS Inspector General. The HHS management agrees with the HHS Inspector General in reporting to the President and the Congress the two material weaknesses described in this report.

Medicare National Error Rate

At HCFA's request, we developed a national error rate of the extent of improper Medicare fee-for-service payments for FY 2000. As discussed in detail in our separate report (CIN: A-17-00-02000), and based on our statistical sample, we estimate that improper Medicare benefit payments made during FY 2000 totaled $11.9 billion, or about 6.8 percent of the $173.6 billion

in processed fee-for-service payments reported by HCFA. This year's estimate of improper payments is the lowest estimate to date and about half the $23.2 billion that we estimated for FY 1996. There is convincing evidence that this reduction is statistically significant. However, we cannot conclude that this year's estimate is statistically different from the estimates for FY 1999 ($13.5 billion) or 1998 ($12.6 billion). The decrease this year may be due to sampling variability; that is, selecting different claims with different dollar values and errors will inevitably produce a different estimate of improper payments.

As in past years, these improper payments could range from inadvertent mistakes to outright fraud and abuse. We cannot quantify what portion of the error rate is attributable to fraud. The overwhelming majority (92 percent) of these improper payments were detected through medical record reviews coordinated by OIG. When these claims were submitted for payment to Medicare contractors, they contained no visible errors. Although HCFA has made substantial progress since FY 1996 in reducing improper payments in the Medicare program, continued efforts are needed.

****

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.

February 26, 2001

REPORT ON COMPLIANCE WITH LAWS AND REGULATIONS

We have audited the principal financial statements of HHS as of and for the year ended September 30, 2000, and have issued our report thereon dated February 26, 2001. 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 OMB Bulletin 01-02, *Audit Requirements for Federal Financial Statements*.

The HHS management is responsible for complying with applicable laws and regulations. As part of obtaining reasonable assurance about whether the HHS financial statements are free of material misstatement, we performed tests of management 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.

The results of our tests of compliance with laws and regulations described in the preceding paragraph, exclusive of FFMIA, disclosed no instances of noncompliance required to be reported under *Government Auditing Standards* or 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 United States 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 Federal financial management system requirements.

- The financial management systems and processes used by HHS and the operating divisions were not adequate to prepare reliable, timely financial statements. Because the Department is decentralized, operating divisions must have efficient and effective systems and processes to report financial results.

  - At HCFA, extensive consultant support was needed to establish reliable accounts receivable balances and to oversee Medicare contractors.

  - The Payment Management System, an application for processing grant payments, did not record and report grant transactions properly.

- At most operating divisions, suitable systems were not in place to adequately explain significant fluctuations in grant transactions.

- At NIH, an integrated accounting system was not in place to consolidate the accounting results of transactions by the Institutes. Extensive, time-consuming manual adjustments were needed before reliable financial statements could be prepared.

❑ The EDP internal control weaknesses identified at the sampled Medicare contractors were significant departures from requirements in OMB Circulars A-127, *Financial Management Systems*, and A-130, *Management of Federal Information Resources*.

The results of our tests disclosed no instances in which the HHS financial management systems did not substantially comply with applicable Federal accounting standards or the U.S. Government Standard General Ledger.

The HHS CFO prepared a 5-year 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.

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.

Michael Mangano

Michael F. Mangano
Acting Inspector General
Department of Health and Human Services

February 26, 2001
CIN: A-17-00-00014

Appendix I

FISCAL YEAR 2000 CFO REPORTS ON HHS OPERATING DIVISIONS AND SERVICE ORGANIZATIONS

Nine separate financial statement audits of HHS operating divisions were conducted in FY 2000:

- Administration for Children and Families *(CIN: A-17-00-00001)*
- Centers for Disease Control and Prevention *(CIN: A-17-00-00008)*
- Food and Drug Administration *(CIN: A-17-00-00006)*
- Health Care Financing Administration *(CIN: A-17-00-02001)*
- Health Resources and Services Administration *(CIN: A-17-00-00003)*
- Indian Health Service *(CIN: A-17-00-00004)*
- National Institutes of Health *(CIN: A-17-00-00007)*
- Program Support Center *(CIN: A-17-00-00005)*
- Substance Abuse and Mental Health Services Administration *(CIN: A-17-00-00002)*

Four Statement on Auditing Standards 70 examinations were conducted:

- Center for Information Technology, NIH *(CIN: A-17-00-00010)*
- Central Payroll and Personnel System, Program Support Center *(CIN: A-17-00-00012)*
- Division of Financial Operations, Program Support Center *(CIN: A-17-00-00009)*
- Payment Management System, Program Support Center *(CIN: A-17-00-00011)*

Appendix II

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Washington, D.C. 20201

FEB 26 2001

Michael F. Mangano
Acting Inspector General
Department of Health and Human Services
Washington, D.C. 20201

Dear Mr. Mangano:

This letter responds to the Office of Inspector General opinion of the FY 2000 audited financial statements of the Department of Health and Human Services. We concur with your findings and recommendations.

We are tremendously pleased that, once again, your report reflects an unqualified, or "clean", audit opinion for the Department. Through our joint efforts, we were able to reach the goal of both a clean and timely Departmental financial statement audit.

We also acknowledge that significant internal control weaknesses remain. In addition to the incremental progress we have made on these weaknesses over the last year, we have greatly accelerated our efforts to improve our financial systems to ultimately resolve these material weaknesses.

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

Sincerely,

Dennis P. Williams
Acting Assistant Secretary for Management and
Budget/Chief Financial Officer