



SOCIAL SECURITY

Office of the Inspector General

November 19, 1999

To Kenneth S. Apfel
Commissioner of Social Security

This letter transmits the PricewaterhouseCoopers LLP (PwC) report on the audit of the Fiscal Year (FY) 1999 financial statements of the Social Security Administration (SSA) and the results of the Office of the Inspector General's (OIG) review thereon. PwC's report includes the firm's opinion on SSA's FY 1999 financial statements, its report on SSA management's assertion about the effectiveness of internal control, and its report on SSA's compliance with laws and regulations.

Objectives of a Financial Statement Audit

The objective of a financial statement audit is to determine 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.

PwC's examination was made in accordance with generally accepted auditing standards, *Government Auditing Standards* issued by the Comptroller General of the United States, and the Office of Management and Budget (OMB) Bulletin No. 98-08, as amended. The audit includes obtaining an understanding of the internal control over financial reporting, and testing and evaluating the design and operating effectiveness of the internal control. Due to inherent limitations in any internal control, there is a risk that error or fraud may occur and not be detected.

The risk of fraud is inherent to SSA's programs and operations, especially within the Supplemental Security Income program. In our opinion, individuals outside of the organization perpetrate the majority of fraud against SSA. A discussion of fraud issues affecting SSA and the activities of the OIG to address fraud is presented in the Inspector General's Report to Congress, a separate section within this accountability report.

Audit of Financial Statements, Effectiveness of Internal Control, and Compliance with Laws and Regulations

The Chief Financial Officers (CFO) Act of 1990 (P.L. 101-576), as amended, requires SSA's Inspector General (IG) or an independent external auditor, as determined by the IG, to audit SSA's financial statements in accordance with applicable standards. Under a contract monitored by OIG, PricewaterhouseCoopers LLP, an independent certified public accounting firm, performed the audit of SSA's FY 1999 financial statements. PwC also audited the FY 1998 financial statements, presented in SSA's Accountability Report for FY 1999 for comparative purposes.

PwC issued an unqualified opinion on SSA's FY 1999 financial statements. PwC also reported that SSA's assertion that its systems of accounting and internal control are in compliance with the internal control objectives in OMB Bulletin No. 98-08. However, the audit identified two reportable conditions in SSA's internal control. The control weaknesses identified are:

1. SSA Needs to Further Strengthen Controls to Protect Its Information
2. SSA Needs to Complete and Fully Test Its Plan for Maintaining Continuity of Operations

In FY 1998 PwC reported a third reportable condition, "SSA Can Improve Controls Over Separation of Duties". In FY 1999, SSA made significant progress to correct this weakness and in the opinion of the auditors, it is no longer a reportable condition. We commend SSA on its progress, but encourage the organization to continue its efforts in this area. Strong internal control, including proper separation of duties, are important to mitigate the risk of fraud.

PwC also reported instances of noncompliance with laws and regulations as follows:

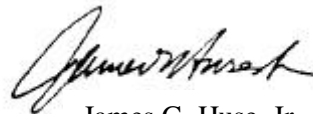
1. Section 221(i) of the Social Security Act, which requires periodic continuing disability reviews for title II beneficiaries; and
2. The Federal Financial Management Improvement Act of 1996 (FFMIA) for the cumulative effect of the two internal control weaknesses listed above.

OIG Evaluation of PwC's Audit Performance

To fulfill our responsibilities under the CFO Act and related legislation for ensuring the quality of the audit work performed, we monitored PwC's audit of SSA's FY 1999 financial statements by:

- Reviewing PwC's approach and planning of the audit;
- Evaluating the qualifications and independence of its auditors;
- Monitoring the progress of the audit at key points;
- Examining its working papers related to planning the audit and assessing SSA's internal control;
- Reviewing PwC's audit report to ensure compliance with *Government Auditing Standards* and OMB Bulletin No. 98-08, as amended;
- Coordinating the issuance of the audit report; and
- Performing other procedures that we deemed necessary.

Based on the results of our review, we determined that PwC planned, executed, and reported the results of its audit of SSA's FY 1999 financial statements in accordance with applicable standards. Therefore, it is our opinion that PwC's work provides a reasonable basis for the firm's opinion on SSA's FY 1999 financial statements and SSA management's assertion on the effectiveness of its internal control and compliance with laws and regulations. Based on our review of the audit, we concur with PwC's finding of reportable conditions related to internal control weaknesses and instances of noncompliance with section 221(i) of the Social Security Act and the FFMIA.



James G. Huse, Jr.
Inspector General

SOCIAL SECURITY ADMINISTRATION BALTIMORE MD 21235-0001

REPORT OF INDEPENDENT ACCOUNTANTS

To Kenneth S. Apfel
Commissioner of Social Security

In our audit of the Social Security Administration (SSA) for fiscal year 1999, we found that:

- The principal financial statements were fairly stated in all material respects;
- Management fairly stated that SSA's systems of accounting and internal control in place as of September 30, 1999 are in compliance with the internal control objectives in Office of Management and Budget (OMB) Bulletin No. 98-08, as amended, *Audit Requirements for Federal Financial Statements*, requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the principal statements in accordance with generally accepted accounting principles, and the safeguarding of assets against loss from unauthorized acquisition, use or disposal; and
- Our testing identified two reportable instances of noncompliance with the laws and regulations we tested.

The following sections outline each of these conclusions in more detail.

OPINION ON THE FINANCIAL STATEMENTS

We have audited the accompanying consolidated balance sheets of SSA as of September 30, 1999 and 1998, and the related consolidated statements of net cost, changes in net position, financing, and budgetary resources for the fiscal years then ended. These financial statements are the responsibility of SSA's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with generally accepted auditing standards, *Government Auditing Standards* issued by the Comptroller General of the United States, and OMB Bulletin No. 98-08, as amended. Those 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 financial statements audited by us and appearing on pages 29 through 41 of this report present fairly, in all material respects, the financial position of SSA at September 30, 1999 and 1998, and its consolidated net cost, changes in net position, budgetary resources and reconciliation of net cost to budgetary resources for the fiscal years then ended in conformity with generally accepted accounting principles.

REPORT ON MANAGEMENT'S ASSERTION ABOUT THE EFFECTIVENESS OF INTERNAL CONTROL

We have examined management's assertion that SSA's systems of accounting and internal control are in compliance with the internal control objectives in OMB Bulletin No. 98-08, as amended, requiring management to establish internal accounting and administrative controls to provide reasonable assurance that transactions are properly recorded, processed, and summarized to permit the preparation of the principal statements in accordance with generally accepted accounting principles, and the safeguarding of assets against loss from unauthorized acquisition, use or disposal.

Our examination was made in accordance with standards established by the American Institute of Certified Public Accountants (AICPA), *Government Auditing Standards* issued by the Comptroller General of the United States, and OMB Bulletin No. 98-08, as amended and, accordingly, included obtaining an understanding of the internal control over financial reporting, testing and evaluating the design and operating effectiveness of the internal control, and such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Our examination was of the internal control in place as of September 30, 1999.

Because of inherent limitations in any internal control, misstatement due to errors or fraud may occur and not be detected. Also, projections of any evaluation of the internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, management's assertion that SSA's systems of accounting and internal control are in compliance with the internal control objectives in OMB Bulletin No. 98-08, as amended, requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the principal statements in accordance with generally accepted accounting principles, and the safeguarding of assets against loss from unauthorized acquisition, use or disposal, is fairly stated, in all material respects.

In addition, with respect to the internal control related to those performance measures determined by management to be key and reported in the Overview and Supplemental Financial and Management Information, we obtained an understanding of the design of significant internal control relating to the existence and completeness assertions and determined whether it has been placed in operation, as required by OMB Bulletin No. 98-08, as amended. Our procedures were not designed to provide assurance on the internal control over reported performance measures, and accordingly, we do not provide an opinion on such control.

However, we noted certain matters involving the internal control and its operation that we consider to be reportable conditions under standards established by the AICPA and by OMB Bulletin No. 98-08, as amended. Reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of the internal control that, in our judgment, could adversely affect the agency's ability to meet the internal control objectives described above. The reportable conditions we noted were: SSA needs to further strengthen controls to protect its information and SSA needs to complete and fully test its plan for maintaining continuity of operations.

A material weakness, as defined by the AICPA and OMB Bulletin No. 98-08, as amended, is a reportable condition 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 in relation to the principal financial statements being audited or to a performance measure or aggregation of related performance measures may occur and not be detected within a timely period by employees in the normal course of performing their assigned duties. We believe that neither of the two reportable conditions that follow is a material weakness as defined by the AICPA and OMB Bulletin No. 98-08, as amended. One of the issues raised in our 1998 report, that SSA can improve controls over separation of duties, is no longer a reportable condition.

1. SSA Needs to Further Strengthen Controls to Protect Its Information

SSA has made notable progress in addressing the information protection issues raised in prior years. Specifically, the agency has:

- Developed a System Security Bulletin that provides a security framework for processing in the mainframe and distributed environments;
- Established a mainframe security monitoring process through the development of the Security Management Action Report (SMART) that is used to monitor inappropriate access to SSA systems;
- Improved physical security at the National Computer Center (NCC) by implementing tighter controls over physical access to the facility and increasing security awareness of the guard force; and
- Continued to improve security monitoring procedures and practices in the local area network (LAN) environment at Headquarters, including an ongoing process to identify unauthorized modems and immediately removing unauthorized modem access.

Our audit in 1999 found that SSA's systems environment remains threatened by weaknesses in several components of its information protection control structure. Because disclosure of detailed information about these weaknesses might further compromise controls, we are providing no further details here. Instead, the specifics are presented in a separate, limited-distribution management letter. The general areas where weaknesses were noted are:

- The entity-wide security program and associated weaknesses in developing, implementing and monitoring LAN and distributed systems security;
- SSA's mainframe computer security and operating system configuration;
- Physical access controls at non-headquarters locations; and
- Certification and accreditation of certain general support and major application systems.

Until corrected, these weaknesses will continue to increase the risks of unauthorized access to, and modification or disclosure of, sensitive SSA information. In turn, unauthorized access to sensitive data can result in the loss of data, loss of Trust Fund resources, and compromised privacy of information associated with SSA's enumeration, earnings, retirement, and disability processes and programs.

Recommendations

We recommend that SSA accelerate and build on its progress in 1999 to enhance information protection by further strengthening its entity-wide security as it relates to implementation of physical and technical computer security mechanisms and controls throughout the organization. In general, we recommend that SSA:

- Reevaluate its overall organization-wide security architecture;
- Reassess the security roles and responsibilities throughout the organization's central and regional office components;
- Assure that the appropriate level of trained resources are in place to develop, implement and monitor the SSA security program;

- Enhance and institutionalize an entity-wide security program that facilitates strengthening of LAN and distributed systems' security;
- Review and certify system access for all users;
- Enhance procedures for removing system access when employees are transferred or leave the agency;
- Decrease vulnerabilities in the mainframe operating system configuration;
- Implement the mainframe monitoring process (SMART Report);
- Finalize accreditation and certification of systems;
- Develop and implement an ongoing entity-wide information security compliance program; and
- Strengthen physical access controls at non-headquarters sites.

More specific recommendations are included in a separate, limited-distribution management letter.

2. SSA Needs to Complete and Fully Test Its Plan for Maintaining Continuity of Operations

SSA has made notable progress since 1998 in implementing improvements to its disaster recovery plan for computer operations. For example, SSA has scheduled testing for all of its 13 originally identified critical workloads for fiscal year 2000. In addition, SSA established a special workgroup that validated the original critical workloads and identified potential additional critical workloads. SSA further developed its draft plan for moving computer operations from its designated "hot-site" (a facility that already has computer equipment and an acceptable computing environment in place to provide processing capabilities on short notice) to a "cold-site" in the event of a longer-term disruption of processing operations. In an effort to eliminate the need for a hot-site to cold-site transition plan and provide for long term outages of up to 12 months, SSA has negotiated with the hot-site vendor via the General Services Administration (GSA) to provide maximum EDP operational capability after disaster declaration. Furthermore, an Interagency Agreement between SSA and GSA has been established so funds and resources will be available in a time of disaster. Finally, SSA initiated efforts to establish a continuity of operations planning workgroup to bring an agency-wide focus to its efforts in this area.

While SSA has many components of a contingency plan in place, we identified a number of deficiencies that, in our opinion, would impair SSA's ability to respond effectively to a disruption in business operations as a result of a disaster or other long-term crisis. Although SSA has performed a Business Impact Analysis, its list of critical workloads is still being finalized and recovery time objectives (RTOs) have not yet been established for each of the critical workloads. Consequently, SSA has not established recovery priorities for all of its systems in the mainframe and distributed environments. Furthermore, the plan for recovering the critical workloads still needs to be fully tested. In addition, SSA has not fully updated the contingency plans for the headquarters site or finalized and tested contingency plans for non-headquarters sites.

SSA also needs to take additional actions to ensure its approach for obtaining alternate processing facilities will be successful. As with other agreements for continuity services, availability of SSA's designated hot-site is dependent upon whether other customers of the hot-site vendor have already declared a disaster, since use of the hot-site is on a "first come, first served" basis. Under the current hot-site arrangement, SSA will be provided with the choice of two Mainframe/Midrange Recovery Centers (MRCs) and two Workarea Recovery Centers (WRCs) for recovering EDP operations. Vendor facilities in North Bergen, NJ and Columbia, MD, respectively, have been identified for SSA use. SSA needs to have the hot-site vendor

identify the secondary MRC and WRC in the event that SSA is not the first customer to declare a disaster and therefore cannot be serviced by the North Bergen and/or Columbia facilities. Once the secondary facilities have been identified, SSA needs to perform recovery tests at these locations to ensure that the resources are adequate to enable recovery of EDP operations.

While we are encouraged by the attention and level of effort SSA has directed to this issue thus far, and senior level agency management is committed to completing and fully testing a comprehensive plan, SSA remains focused on the systems aspect of continuity planning. SSA needs to ensure it includes contingency planning for operations as well as for systems in its overall plan.

Recommendations

We recommend that SSA:

- Finalize the list of critical SSA workloads and fully test the plans for recovering each workload;
- Establish RTOs for each critical workload;
- Establish recovery priorities for all systems and applications (mainframe and distributed);
- Update contingency plans for headquarters;
- Finalize and test contingency plans for non-headquarters sites;
- Have its hot-site vendor identify secondary facilities (MRC and WRC) for recovering EDP operations; and
- Finalize and test SSA's ultimate strategy for implementing and maintaining alternate processing facilities.

REPORT ON COMPLIANCE WITH LAWS AND REGULATIONS

We conducted our audit in accordance with generally accepted auditing standards, 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. 98-08, as amended.

The management of SSA is responsible for complying with laws and regulations applicable to the agency. As part of obtaining reasonable assurance about whether the financial statements are free of material misstatement, we performed tests of SSA's compliance with certain provisions of applicable laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts and certain other laws and regulations specified in OMB Bulletin No. 98-08, as amended, including the requirements referred to in the Federal Financial Management Improvement Act (FFMIA) of 1996. However, the objective of our audit of the financial statements was not to provide an opinion on overall compliance with such provisions and, accordingly, we do not express such an opinion.

The results of our tests of compliance with the laws and regulations described in the preceding paragraph disclosed instances of noncompliance with the following laws and regulations that are required to be reported under *Government Auditing Standards* and OMB Bulletin No. 98-08, as amended.

- SSA is not in full compliance with Section 221(i) of the Social Security Act which requires periodic Continuing Disability Reviews (CDRs) for Title II beneficiaries. If CDRs are not performed timely, beneficiaries who are no longer eligible for disability may inappropriately continue to receive benefits,

including Medicare benefits. Prior to our report date, SSA was unable to provide an estimate of the total backlog of Title II cases yet to be reviewed for continuing eligibility as of September 30, 1999.

- Under FFMIA, we are required to report whether the agency's financial management systems substantially comply with Federal financial management systems requirements, Federal accounting standards, and the United States Standard General Ledger at the transaction level. To meet this requirement we performed tests of compliance using the implementation guidance for FFMIA included in Appendix D of OMB Bulletin No. 98-08, as amended. We found weaknesses in information protection and business continuity planning, as described above. We believe these weaknesses are significant departures from certain of the requirements of OMB Circulars A-127, *Financial Management Systems*, and A-130, *Management of Federal Information Resources*, and are therefore instances of substantial noncompliance with the Federal financial management systems requirements under FFMIA. SSA should assign a high priority to the corrective actions consistent with the requirements of OMB Circular No. A-50 Revised, on audit follow-up.

Except as noted in the previous paragraph, the results of our tests of compliance disclosed no instances of noncompliance with other laws and regulations that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 98-08, as amended.

OBJECTIVES, SCOPE AND METHODOLOGY

SSA management is responsible for:

- Preparing the annual financial statements in conformity with generally accepted accounting principles;
- Establishing, maintaining, and assessing internal control that provides reasonable, but not absolute, assurance that the broad control objectives of OMB Bulletin No. 98-08, as amended are met; and
- Complying with applicable laws and regulations.

Our responsibilities are to:

- Express an opinion on SSA's principal financial statements;
- Obtain reasonable assurance about whether management's assertion about the effectiveness of the internal control is fairly stated, in all material respects, based upon the internal control objectives in OMB Bulletin No. 98-08, as amended, *Audit Requirements for Federal Financial Statements*, requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the principal statements in accordance with generally accepted accounting principles, and the safeguarding of assets against loss from unauthorized acquisition, use or disposal; and
- Test SSA's compliance with selected provisions of laws and regulations that could materially affect the principal financial statements.

In order to fulfill these responsibilities, we:

- Examined, on a test basis, evidence supporting the amounts and disclosures in the principal financial statements;
- Assessed the accounting principles used and significant estimates made by management;
- Evaluated the overall presentation of the principal financial statements;

- Obtained an understanding of the internal control related to safeguarding assets, compliance with laws and regulations including the execution of transactions in accordance with budget authority, financial reporting, and certain performance measures determined by management to be key and reported in the Overview of SSA and Supplemental Financial and Management Information;
- Tested relevant internal control over safeguarding, compliance, and financial reporting and evaluated management's assertion about the effectiveness of the internal control; and
- Tested compliance with selected provisions of laws and regulations.

We did not evaluate all the internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act, such as those controls relevant to preparing statistical reports and ensuring efficient operations. We limited our internal control testing to those controls necessary to achieve the objectives outlined in our report on management's assertion about the effectiveness of the internal control.

* * * * *

We noted other matters involving the internal control and its operation that we will communicate in a separate letter.

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

PriceWaterhouseCoopers LLP

Arlington, Virginia
November 18, 1999