SOCIAL SECURITY

Inspector General

November 10, 2003

To: The Honorable Jo Anne B. Barnhart
Commissioner

This letter transmits the PricewaterhouseCoopers LLP (PwC) *Report of Independent Auditors* on the audit of the Social Security Administration's (SSA) Fiscal Year (FY) 2003 and 2002 financial statements. PwC's Report includes the firm's *Opinion on the Financial Statements, Report on Management's Assertion About the Effectiveness of Internal Control,* and *Report on Compliance with Laws and Regulations.*

Objective 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 Office of Management and Budget (OMB) Bulletin 01-02, *Audit Requirements for Federal Financial Statements*. The audit included obtaining an understanding of the internal control over financial reporting and testing and evaluating the design and operating effectiveness of the internal control. Because of inherent limitations in any internal control, there is a risk that errors or fraud may occur and not be detected. The risk of fraud is inherent to many of SSA's programs and operations, especially within the Supplemental Security Income (SSI) program. In our opinion, people outside the organization perpetrate most of the fraud against SSA.

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 the Office of the Inspector General (OIG), PwC, an independent certified public accounting firm, audited SSA's FY 2003 financial statements. PwC also audited the FY 2002 financial statements, presented in SSA's Performance and Accountability Report for FY 2003 for comparative purposes. PwC issued an unqualified opinion on SSA's FY 2003 and 2002 financial statements. PwC also reported that SSA's assertion that its systems of accounting and internal control are in compliance with the internal control objective in OMB Bulletin 01-02 is fairly stated in all material respects. However, the audit identified one reportable condition in SSA's internal control:

SSA Needs to Further Strengthen Controls to Protect Its Information

This is a repeat finding from prior years. It is PwC's opinion that SSA has made notable progress in addressing the information protection issues raised in prior years. Despite these accomplishments, SSA's systems environment remains threatened by security and integrity exposures to SSA operations.

OIG Evaluation of PwC 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 2003 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 workpapers 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 01-02;
- Coordinating the issuance of the audit report; and
- Performing other procedures that we deemed necessary.

PwC is responsible for the attached auditor's report, dated November 7, 2003, and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding PwC's performance under the terms of the contract. Our review, as differentiated from an audit in accordance with applicable auditing standards, was not intended to enable us to express, and accordingly we do not express, an opinion on SSA's financial statements, management's assertions about the effectiveness of its internal control over financial reporting, or SSA's compliance with certain laws and regulations. However, our monitoring review, as qualified above, disclosed no instances where PwC did not comply with applicable auditing standards.

Sincerely,

James G. Huse, Jr.

PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers LLP
1301 K Street, NW
Washington, DC 20005
Telephone (202)414-1000

REPORT OF INDEPENDENT AUDITORS

To the Honorable Jo Anne B. Barnhart
Commissioner
Social Security Administration

In our audit of the Social Security Administration (SSA), we found:

- The consolidated balance sheets of SSA as of September 30, 2003 and 2002, and the related consolidated statements of net cost, of changes in net position, of financing and the combined statements of budgetary resources for the fiscal years then ended are presented fairly, in all material respects, in conformity with accounting principles generally accepted in the United States of America;
- Management fairly stated that SSA's systems of accounting and internal control in place as of September 30, 2003, are in compliance with the internal control objectives in the Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*, requiring that (a) transactions be properly recorded, processed, and summarized to permit the preparation of the consolidated and combined financial statements in accordance with Federal accounting standards and the safeguarding of assets against loss from unauthorized acquisition, use or disposition and (b) transactions are executed in accordance with (i) 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 (ii) any other laws, regulations and governmentwide policies identified in OMB Bulletin No. 01-02;
- No 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, 2003 and 2002, and the related consolidated statements of net cost, of changes in net position, of financing and the combined statements of 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 auditing standards generally accepted in the United States of America, the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and OMB Bulletin No. 01-02. 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 and combined financial statements referred to above and appearing on pages 118 through 139 of this performance and accountability report, present fairly, in all material respects,

the financial position of SSA at September 30, 2003 and 2002, and its net cost, changes in net position, reconciliation of net cost to budgetary resources, and budgetary resources for the fiscal years then ended in conformity with accounting principles generally accepted in the United States of America.

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. 01-02, requiring that (a) transactions be properly recorded, processed, and summarized to permit the preparation of the consolidated and combined financial statements in accordance with Federal accounting standards and the safeguarding of assets against loss from unauthorized acquisition, use or disposition and (b) transactions are executed in accordance with (i) 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 (ii) any other laws, regulations and governmentwide policies identified in OMB Bulletin No. 01-02. SSA's management is responsible for maintaining effective internal controls. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA), the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and OMB Bulletin No. 01-02 and, accordingly, included obtaining an understanding of the internal control, testing and evaluating the design and operating effectiveness of internal control, and performing 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, 2003.

Because of inherent limitations in any internal control, misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of internal control 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. 01-02, requiring that (a) transactions be properly recorded, processed, and summarized to permit the preparation of the consolidated and combined financial statements in accordance with Federal accounting standards and the safeguarding of assets against loss from unauthorized acquisition, use or disposition and (b) transactions are executed in accordance with (i) 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 (ii) any other laws, regulations and governmentwide policies identified in OMB Bulletin No. 01-02, is fairly stated, in all material respects, as of September 30, 2003.

However, we noted certain matters involving the internal control and its operation, set forth below, that we consider to be a reportable condition under standards established by the AICPA and by OMB Bulletin No. 01-02. A reportable condition is a matter coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the Agency's ability to meet the internal control objectives described above.

A material weakness, as defined by the AICPA and OMB Bulletin No. 01-02, 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 consolidated and combined 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 the reportable condition that follows is not a material weakness as defined by the AICPA and OMB Bulletin No. 01-02.

SSA Needs to Further Strengthen Controls to Protect Its Information:

Over the past year, SSA has made significant progress in addressing the information protection issues raised in prior years. Specifically, during fiscal year 2003 SSA has:

- Implemented "risk models" to standardize platform security configuration settings for the Windows NT, Windows 2000, AS 400, Unix and WANG platforms;
- Enhanced the risk models to further strengthen the security settings for new security weaknesses;
- Implemented new tools and procedures to monitor adherence to platform security configuration standards for the Windows NT, Windows 2000, AS 400, Unix and WANG platforms;
- Reduced the number of Windows NT, Windows 2000, AS 400, Unix, and servers with known high risk security weaknesses;
- Maintained strong access-based rule settings and standardized monitoring and logging procedures for firewalls;
- Continued progress on the Standard Security Profile Project (SSPP - the project consists of a full scale comparison of system user access assignments to job responsibilities to ensure accuracy) and expanded the SSPP to include non-IT employees;
- Continued progress on the Dataset Naming Standards project, including setting naming conventions, determining tools for compliance and enforcement, and establishing data ownership;
- Improved and implemented new reports and procedures for enhanced review of security violations on the mainframe; and,
- Continued progress in the area of continuity of operations planning for the Regional Offices (RO)/Program Service Centers (PSC) and state Disability Determination Services (DDS) sites.

Although significant progress has been made regarding logical security controls, we note the need for further progress regarding (a) the review of security access assignments, including vetting of assignments for access to transactions and data, (b) the establishment and full use of dataset naming conventions, (c) the establishment of a dataset dictionary for existing datasets and transactions, and (d) the enforcement of the new dataset naming rules and standards for sensitive systems. We also note the need to test the newly drafted high level procedures to move workloads between RO/PSC and DDS sites to maintain continuity of operations by testing the processes and procedures up to the actual transfer of the workloads. Disclosure of more detailed information about these exposures might further compromise controls and is therefore not provided in this report. Rather, the specific details of weaknesses noted are presented in a separate, limited-distribution management letter.

Management has made concerted efforts to address these issues; however, the completion of the SSPP is a time consuming task that will require substantial resources to complete. Further, the physical controls over the state DDS sites continue to be a challenge because many of the sites are co-located with state agencies, or are housed in buildings with inherent physical security issues.

The need for a strong security program to address threats to the security and integrity of SSA operations continues to grow as the Agency continues to progress with plans to increase dependence on the Internet and Web-based applications to serve the American public. Clear progress has been made towards the implementation of a strong overall security program. However, to more fully protect SSA from risks associated with the loss of data, loss of other resources and/or compromised privacy of information associated with SSA's enumeration, earnings, retirement, and disability processes and programs, SSA must complete the strengthening of its security program in the areas of assigning access to transactions and data and physical security over DDS sites.

Recommendations

We recommend that SSA implement the remaining portions of its entity-wide security program. Specifically, we recommend that SSA:

- Continue the SSPP program to ensure that sensitive systems, as defined by the SSA systems accreditation and certification process, are adequately addressed regarding proper access assignments, dataset naming standards, and inclusion in the dataset dictionary;
- Continue to improve physical security controls for the DDS sites; and
- Continue to enhance continuity of operations activities, including testing of newly developed procedures for RO/PSC and DDS sites.

More specific recommendations addressing the individual exposures we identified are included in a separate, limited-distribution management letter.

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

REPORT ON COMPLIANCE WITH LAWS AND REGULATIONS

We conducted our audit in accordance with auditing standards generally accepted in the United States of America, the standards applicable to financial audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States, and OMB Bulletin No. 01-02.

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 Agency's 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. 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 we did not test compliance with all laws and regulations applicable to SSA.

The results of our tests of compliance disclosed no instances of noncompliance with laws and regulations discussed in the preceding paragraph exclusive of FFMIA that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 01-02.

Under FFMIA, we are required to report whether SSA's financial management systems substantially comply with the 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 no instances in which SSA's financial management systems did not substantially comply with the three requirements discussed in the preceding paragraph.

The objective of our audit of the financial statements was not to provide an opinion on overall compliance with such provisions of laws and regulations and, accordingly, we do not express such an opinion.

INTERNAL CONTROL RELATED TO KEY PERFORMANCE MEASURES

With respect to internal control related to those performance measures determined by management to be key and included on pages 29 to 54 of this performance and accountability report, we obtained an understanding of the design of significant internal control relating to the existence and completeness

assertions, as required by OMB Bulletin No. 01-02. Our procedures were not designed to provide assurance on the internal control over reported performance measures, and accordingly, we do not express an opinion on such control.

OTHER INFORMATION

Our audit was conducted for the purpose of forming an opinion on the consolidated and combined financial statements of SSA taken as a whole. The Schedule of Budgetary Resources, included on page 144 of this performance and accountability report, is not a required part of the consolidated and combined financial statements but is supplementary information required by OMB Bulletin No. 01-09*, Form and Content of Agency Financial Statements*. This information, and the consolidating and combining information included on pages 140 to 143 of this performance and accountability report are presented for purposes of additional analysis of the consolidated and combined financial statements rather than to present the financial position, changes in net position, reconciliation of net cost to budgetary resources, and budgetary resources of the individual SSA programs. Such information has been subjected to the auditing procedures applied in the audit of the consolidated and combined financial statements and, in our opinion, is fairly stated in all material respects in relation to the consolidated and combined financial statements taken as a whole.

The required supplementary information included on pages 1 and 2, 6 to 64, 115 to 117 and 145 of this performance and accountability report and the required supplementary stewardship information included on pages 146 to 163 of this performance and accountability report, are not required parts of the financial statements but are supplementary information required by OMB Bulletin No. 01-09 and the Federal Accounting Standards Advisory Board. We have applied certain limited procedures to such information, which consisted principally of inquiries of management regarding the methods of measurement and presentation of the supplementary information. However, we did not audit the information and express no opinion on it.

The other accompanying information included on pages 3 to 5, 65 to 114, 164 to 166 and 172 to the end of this performance and accountability report, are presented for purposes of additional analysis and are not a required part of the financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the consolidated and combined financial statements and, accordingly, we express no opinion on it.

* * * * *

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

PricewaterhouseCoopers LLP

November 7, 2003