AUDIT OF THE SOCIAL SECURITY ADMINISTRATION'S FISCAL YEAR 2001 FINANCIAL STATEMENTS

SOCIAL SECURITY

Office of the Inspector General

December 11, 2001

To: Jo Anne B. Barnhart
Commissioner

This letter transmits the PricewaterhouseCoopers LLP (PwC) report on the audit of the Fiscal Years (FY) 2001 and 2000 financial statements of the Social Security Administration (SSA) and the results of the Office of the Inspector General's (OIG) review thereof. PwC's report includes the firm's *Opinion on the Financial Statements*, its *Report on Management's Assertion About the Effectiveness of Internal Control*, and its report on SSA's *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 is required to be 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. 01-02. 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 many of SSA's programs and operations, especially within the Supplemental Security Income (SSI) program. In our opinion, people outside of the organization perpetrate the majority of frauds 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 OIG, PwC, an independent certified public accounting firm, performed the audit of SSA's FY 2001 financial statements. PwC also audited the FY 2000 financial statements, presented in SSA's Performance and Accountability Report for FY 2001 for comparative purposes. PwC issued an unqualified opinion on SSA's FY 2001 and 2000 financial statements. PwC also reported that SSA management's assertion, that its systems of accounting and internal control are in compliance with the internal control objectives in OMB Bulletin No. 01-02, is fairly stated in all material respects. However, the audit identified one reportable condition in SSA's internal control. The control weakness identified is: ***SSA Needs to Further Strengthen Controls to Protect Its Information.***

This is a repeat finding from prior years. It is the opinion of PwC 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 impacting key elements of its distributed systems and networks. The general areas where exposures occurred included:

- Implementation, enforcement, and ongoing monitoring of technical security configuration standards;
- Implementation, enforcement, and ongoing monitoring of technical standards and rules governing the operation of firewalls on the SSA network;
- Monitoring controls over security violation, periodic review of user access, and firewall logs; and
- Physical access controls at non-headquarters locations.

The results of PwC's tests of compliance disclosed no instances of noncompliance with laws and regulations that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 01-02.

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 2001 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 No. 01-02;
- 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 2001 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 2001 and 2000 financial statements and SSA management's assertion on the effectiveness of its internal control. Based on our oversight of the audit, we concur with PwC's finding of a reportable condition related to a weakness in internal control.

James G. Huse, Jr
Inspector General of Social Security

PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers LLP
1616 N. Fort Myer Dr.
Arlington VA 22209-3195
Telephone (703) 741 1000
Facsimile (703) 741 1616

REPORT OF INDEPENDENT ACCOUNTANTS

To Ms. Jo Anne B. Barnhart
Commissioner of Social Security

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

- The consolidated balance sheets of SSA as of September 30, 2001 and 2000, and the related consolidated statements of net cost, consolidated statements of changes in net position, combined statements of budgetary resources, consolidated statements of financing, and statements of custodial activity 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, 2001 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 transactions be properly recorded, processed, and summarized to permit the preparation of the consolidated and combined financial statements in accordance with accounting principles generally accepted in the United States of America and that assets be safeguarded against loss from unauthorized acquisition, use or disposal; and
- 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, 2001 and 2000, and the related consolidated statements of net cost, consolidated statements of changes in net position, combined statements of budgetary resources, consolidated statements of financing, and statements of custodial activity 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 65 through 85 of this performance and accountability report, present fairly, in all material respects, the financial position of SSA at September 30, 2001 and 2000, and its net cost, changes in net position, budgetary resources, reconciliation of net cost to budgetary resources, and custodial activity for the fiscal years then ended in conformity with accounting principles generally accepted in the United States of America.

PRICEWATERHOUSECOOPERS

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 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 consolidated and combined financial statements in accordance with accounting principles generally accepted in the United States of America and that assets be safeguarded against loss from unauthorized acquisition, use or disposal. SSA's management is responsible for maintaining effective internal control over financial reporting. 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 over financial reporting, 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, 2001.

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 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. 01-02, requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the consolidated and combined financial statements in accordance with accounting principles generally accepted in the United States of America and that assets be safeguarded against loss from unauthorized acquisition, use or disposal, is fairly stated, in all material respects, as of September 30, 2001.

However, we noted certain matters involving the internal control and its operation 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. The reportable condition we noted is that SSA needs to further strengthen controls to protect its information.

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

PRICEWATERHOUSECOOPERS

SSA Needs to Further Strengthen Controls to Protect Its Information

SSA has continued to make progress in addressing the information protection issues raised in prior years. Specifically, in FY 2001 the agency has:

- Conducted a risk assessment to identify critical assets and vulnerabilities as part of the Critical Infrastructure Protection project;
- Issued a final security policy for the State Disability Determination Service (DDS) sites in accordance with the information security requirements included in the National Institute of Standards and Technology (NIST) Special Publication 800-18;
- Established and published technical security configuration standards for NT, Unix, AS 400, and firewall servers;
- Completed updates for accreditation and certification of key systems; and
- Further strengthened physical access controls over the National Computer Center (NCC).

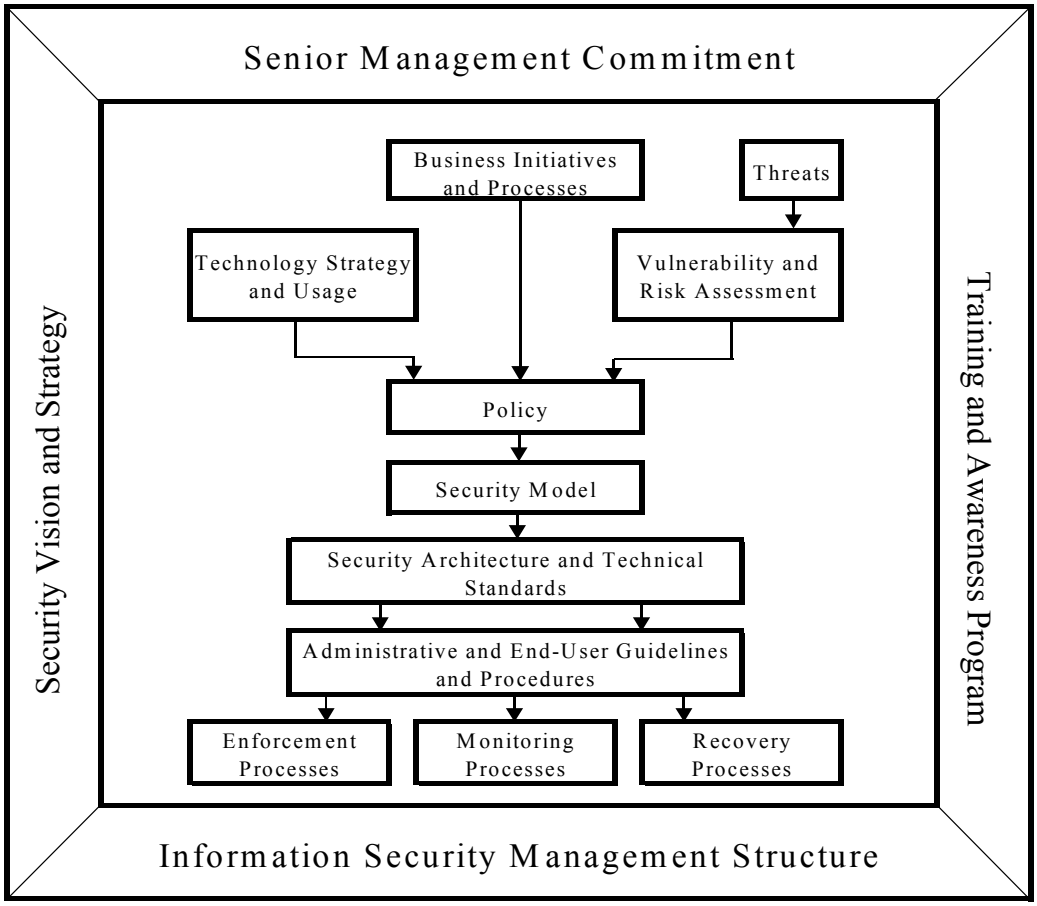
Although SSA has made improvements to its entity-wide security program and standards, we identified weaknesses in controls that expose key elements of SSA's distributed systems and networks to unauthorized access to sensitive data. The general areas where exposures occurred included:

- Implementation, enforcement, and ongoing monitoring of technical security configuration standards throughout the SSA environment, including systems housed in the NCC and off-site housed systems;
- Implementation, enforcement, and ongoing monitoring of technical standards and rules governing the operation of firewalls on the SSA network;
- Monitoring controls over security violations, periodic reviews of user access, and firewall logs; and
- Physical access controls at non-headquarters locations, including SSA's Regional Offices, Program Service Centers, and selected State DDS facilities.

These exposures exist primarily because SSA is in the process of implementing its enterprise-wide security program. The following diagram represents a framework for a fully integrated and functional enterprise-wide security program. This information security framework diagram incorporates the key system security provisions of OMB Circular A-130, Appendix III, and associated NIST guidelines.

PRICEWATERHOUSECOOPERS

Information Security Framework



During fiscal year 2001, SSA has made progress in certain elements of this information security framework; however, the weaknesses we identified show that elements of the framework related to the implementation, enforcement, and monitoring of security policies and technical security standards need to be addressed. Disclosure of detailed information about these weaknesses might further compromise controls. Rather than provide such details in this report, we present them in a separate, limited-distribution management letter, and we present in this report the following examples, which provide an overview of the types of weaknesses we identified.

- *Technical Standards Implementation and Ongoing Enforcement* - Security configurations for four technical environments were inconsistent with SSA guidelines for system configurations. These inconsistencies represent weaknesses in controls over these systems, which could be exploited to improperly access sensitive SSA systems and data. Further, no process has been established to monitor configurations to determine that they remain consistent with the technical configuration standards once implemented. Finally, a configuration standard has not been established to consistently address security for one of the SSA platforms.
- *Monitoring Processes* - Monitoring of systems security within SSA's network and distributed systems environment has been inconsistent. Although SSA's program for monitoring controls over internal modems for dial-in access has been effective, its use of violation reports to monitor the effectiveness of the mainframe security requires enhancement. Mainframe system security monitoring at headquarters and non-headquarters facilities, such as SSA's Regional Offices and Program Service Center sites and State DDS facilities, was weak. Also, the monitoring of employees' access to systems has not been

periodically performed. Finally, the review of firewall logs is not consistently performed for the SSA firewalls.

- *Physical Security Enforcement* Processes - Enforcement of security policies and procedures for physical access to information resources at non-headquarters locations, including SSA's Regional Offices, Program Service Centers and selected State DDS facilities was not sufficient. We noted weaknesses in physical security at these sites that could allow unauthorized employees or visitors to access sensitive SSA information.

Until a complete security framework is implemented and maintained, SSA's ability to mitigate effectively the risk of unauthorized access to, and/or modification or disclosure of, sensitive SSA information will be impaired. Unauthorized access to sensitive data can result in the loss of data, loss of Trust Fund assets, and/or compromised privacy of information associated with SSA's enumeration, earnings, benefit payment processes and programs. The need for a strong security framework to address threats to the security and integrity of SSA operations will grow as the agency continues to implement Internet and Web-based applications to serve the American public.

Recommendations

We recommend that SSA continue its efforts to fully implement the information security framework by:

- Assigning specific resources to complete the full information security framework, with priority given to implementation, enforcement, and monitoring of technical security standards;
- Fully implementing technical security configuration standards;
- Establishing a process to determine that configuration standards remain consistently enforced;
- Establishing and enforcing effective procedures for monitoring security violations, periodic review of access assignments and firewall log reviews; and,
- Consistently enforcing policies and procedures for physical access to information resources based on the concept of access required to perform assigned job responsibilities.

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 that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 01-02.

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 36 to 51 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.

CONSISTENCY OF 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 other accompanying information included on pages 1 to 6, and 111 to the end of this performance and accountability report, is presented for purposes of additional analysis and is not a required part of the consolidated and combined 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.

The required supplementary information included on pages 7 to 62, and 90 of this performance and accountability report and the required supplementary stewardship information included on pages 91 to 110 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 and the Federal Accounting Standards Advisory Board. We have applied certain limited procedures, 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.

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 consolidating and combining information included on pages 86 to 88 of this performance and accountability report, is presented for purposes of additional analysis of the consolidated and combined financial statements rather than to present the financial position, changes in net position, and reconciliation of net cost to budgetary resources of the SSA programs. The consolidating and combining 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.

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 required supplementary information, Schedule of Budgetary Resources, included on page 89 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. This information is also presented for purposes of additional analysis of the consolidated and combined financial statements rather than to present the budgetary resources of the SSA programs. This 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.

* * * * *

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

PRICEWATERHOUSECOOPERS

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 30, 2001