

**AUDIT OF  
THE SOCIAL SECURITY  
ADMINISTRATION'S  
FISCAL YEAR 2000  
FINANCIAL STATEMENTS**





## **SOCIAL SECURITY**

Office of the Inspector General

December 1, 2000

To Kenneth S. Apfel  
Commissioner of Social Security

This letter transmits the PricewaterhouseCoopers LLP (PwC) report on the audit of the Fiscal Year (FY) 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 SSA's FY 2000 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.

### **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 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 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 of the organization perpetrate the majority of frauds 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 the Congress 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 the OIG, PwC, an independent certified public accounting firm, performed the audit of SSA's FY 2000 financial statements.

PwC also audited the FY 1999 financial statements, presented in SSA's Accountability Report for FY 2000 for comparative purposes.

PwC issued an unqualified opinion on SSA's FY 2000 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 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:

- Logical access controls at non-headquarters sites;
- Policies and rules governing the operation of firewalls on the SSA network; and
- Technical configuration of a contractor-controlled domain within SSA's Windows NT Network (Corrected by SSA before completion of the audit).

On October 30, 2000, the *Government Information Security Reform Act*, H.R. 5408, was passed. As of the auditor's reporting date, implementation guidance has not been issued. This Act requires an annual independent evaluation of the Agency's information security program by its Inspector General, or the IG's independent evaluator. The Agency's head will send the results, of this evaluation, each year, to the Director of OMB not later than the anniversary date of this legislation. SSA plans to report on its compliance with this law in its FY 2001 Performance and Accountability Report. We believe SSA should also consider the potential impact this legislation may have on how it reports internal control deficiencies under the Federal Managers' Financial Integrity Act of 1982.

In FY 1999, PwC reported a second reportable condition, "SSA Needs to Complete and Fully Test Its Plan for Maintaining Continuity of Operations." In FY 2000, SSA made significant progress to correct this weakness and in the opinion of the auditors, it is no longer a reportable condition. Nonetheless, SSA's work in this area is incomplete and weaknesses remain particularly with regard to business continuity and disaster recovery issues at non-headquarters sites and at the state Disability Determination Service (DDS) offices. These issues will be reported in PwC's FY 2000 Management Letter.

We commend SSA on its progress for improving its plan for continuity of operations, but encourage the Agency to make timely correction of the weaknesses remaining. Continuity of operations and disaster recovery of critical systems is crucial to the overall operations of SSA programs, its service to the public, and the public's confidence in the Government.

One area of particular concern is the timeframe for recovery of critical Agency systems in the event of an interruption or disaster. SSA's improved plan contains a provision for operational recovery of critical systems within 72 hours—a timeframe, which PwC agrees, would not risk material misstatement of the financial reporting of the Agency. However, Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998, requires critical systems to be recovered and operational within 12 hours of recovery plan activation. Although the Agency has improved its ability for

critical systems to become operational within 72 hours, which PwC believes mitigates the risk of material misstatement on financial reporting, SSA is not in compliance with related provisions under PDD 67.

In FY 1999, PwC reported two instances of noncompliance with laws and regulations as follows:

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

In FY 2000, PwC tests of compliance disclosed no instances of non-compliance with laws and regulations that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 01-02. We commend SSA in their efforts to resolve the first non-compliance and encourage the Agency to continue to meet the annual continuing disability review requirements of this law. Nonetheless, we are not in agreement with PwC's opinion that SSA is in compliance with the FFMIA.

With respect to the Federal Financial Management Improvement Act of 1996 (FFMIA), the OIG, in consultation with the General Accounting Office, believes that instances of substantial non-compliance remain due to the continuing reportable condition "SSA Needs to Further Strengthen Controls to Protect Its Information." Computer security is important to ensure the protection of assets and data. A key component of the internal control weakness is the need for an improved Information Security Framework. The lack of such a framework means that important security program controls may not be functioning to ensure that controls are working as management has intended. Thus, SSA's electronic environment could be compromised. FFMIA requires Agency financial management systems to substantially comply with Federal financial management systems requirements. We believe the internal control weaknesses relating to information protection significantly depart from certain requirements in OMB Circular A-130 - *Management of Federal Information Resources* and, as such, constitute instances of substantial non-compliance with Federal financial management systems requirements under FFMIA.

On November 22, 2000, the President signed the Reports Consolidation Bill of 2000 (Act) into law. Under this law, the Head of each Executive Agency with the concurrence of the Director of OMB, may consolidate statutorily required reports described in this Act into a consolidated report. This Act was effective for FY 2000. The reports submitted under this law are due to OMB no later than 180 days after the fiscal year with respect to FY 2000 and FY 2001. This Act also requires a statement prepared by SSA's IG, which summarizes what the IG considers to be the most important management problems facing the Agency and briefly assesses the Agency's progress in addressing those challenges. The Agency head may comment on the IG's statement, but may not modify the statement.

Because the Agency has committed to issuing its FY 2000 report by December 1, 2000, it is not possible to include this statement in the Agency's FY 2000 Accountability Report at this time. We plan to issue this statement to the Agency in the near future, which will allow the Agency to issue an addendum to the FY 2000 Accountability Report, that will include the IG's statement and any comments that the Agency may have thereon. Our statement will be issued in time to allow the Agency to review and prepare any comments it may have on the IG statement and still meet the reporting requirements of the Act.

## 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 2000 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 2000 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 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 internal control weaknesses. We do not concur with PwC's conclusion that the reportable condition on information protection does not constitute an instance of substantial non-compliance with the Federal financial management systems requirements under FFMIA.



James G. Huse, Jr  
Inspector General

## REPORT OF INDEPENDENT ACCOUNTANTS

To Kenneth S. Apfel  
Commissioner of Social Security

In our audit of the Social Security Administration (SSA) for fiscal year 2000, we found that:

- The consolidated 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, 2000 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 financial statements in accordance with accounting principles generally accepted in the United States of America, and the safeguarding of assets against loss from unauthorized acquisition, use or disposal; and
- Our testing identified 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, 2000 and 1999, and the related consolidated statements of net cost, changes in net position, budgetary resources and financing 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 financial statements audited by us and appearing on pages 36 through 49 of this report present fairly, in all material respects, the financial position of SSA at September 30, 2000 and 1999, 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 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 Office of Management and Budget 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 principal statements in accordance with accounting principles generally accepted in the United States of America, and the safeguarding of assets against loss from unauthorized acquisition, use or disposal. Management is responsible for maintaining effectiveness of internal control over financial reporting. Our responsibility is to express an opinion on the effectiveness of internal control 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 the 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, 2000.

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 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. 01-02, requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the principal statements in accordance with accounting principles generally accepted in the United States of America, and the safeguarding of assets against loss from unauthorized acquisition, use or disposal, is fairly stated, in all material respects, as of September 30, 2000.

In addition, with respect to internal control related to those performance measures determined by management to be key and reported on pages 24 to 29, 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. 01-02. 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 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 the 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. An issue raised in our 1999 report, that



SSA needs to complete and fully test its plan for maintaining continuity of operations, is no longer a reportable condition.

### **SSA Needs to Further Strengthen Controls to Protect Its Information**

Over the past year SSA has made notable progress in addressing the information protection issues raised in prior years. Specifically, in FY 2000 the agency has:

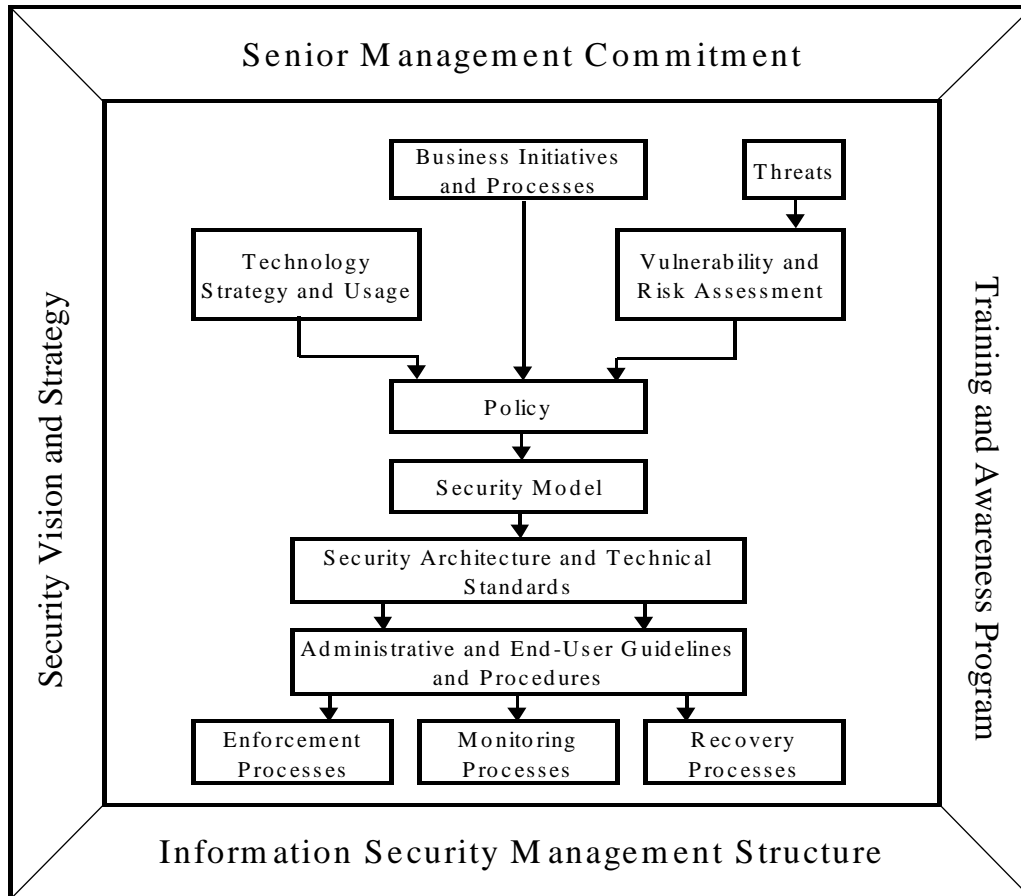
- Issued a security policy, as part of a July 2000 security plan for general support systems, in accordance with the information security requirements included in National Institute of Standards and Technology (NIST) Special Publication 800-18;
- Implemented a process based upon the Security Management Action Report (SMART) for monitoring inappropriate access to SSA mainframe systems;
- Finalized accreditation and certification of systems;
- Strengthened physical access controls over the National Computer Center (NCC);
- Reduced vulnerabilities in the mainframe operating system configuration;
- Implemented network monitoring and alerting tools; and
- Enhanced procedures for removing system access when employees are transferred or leave the agency.

Despite these accomplishments, SSA's systems environment remains threatened by security and integrity exposures impacting key elements of its distributed systems and networks. Because disclosure of detailed information about these exposures 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 exposures occurred included:

- Logical access controls at non-headquarters locations, including SSA's Program Service Centers, Data Operations Center, and selected State Disability Determination Service (DDS) facilities;
- Policies and rules governing the operation of firewalls on the SSA network; and
- Technical configuration of a contractor-controlled domain within SSA's Windows NT network (Corrected by SSA before completion of the audit).

In our view, these exposures occurred primarily because of continuing weaknesses in several components of SSA's overall information protection control structure. The terms italicized in the narrative following the diagram below, describe the various components of that structure are reflected in the Information Security Framework diagram. The Information Security Framework diagram highlights the key system security provisions of OMB Circular A-130, Appendix III, and associated NIST guidelines.

## Information Security Framework



The following examples provide insight into the types of weaknesses we identified in SSA's information protection control structure.

- *Vulnerability and Risk Assessment* - SSA has recently awarded a contract to have a security risk assessment performed for the NCC at agency headquarters. However, we could identify no additional recent risk assessments of components of SSA's network and distributed systems environment.
- *Security Architecture and Technical Standards* – The July 2000 security plan for general support systems (i.e., *Policy*) documents SSA's security goals and objectives for agency networks and distributed systems. However, detailed technical guidance to ensure the consistent accomplishment of those goals and objectives within each technical platform environment (e.g., UNIX, Windows NT, AS-400, etc.) has not yet been developed and/or disseminated. Similarly, although the firewall settings SSA has implemented prevented us from successfully penetrating the network from the outside, firewall policies and rules have not been developed to reflect the decisions SSA has made in defining its *Business Initiatives and Processes*. Until such time as detailed security architecture and technical standards are defined and implemented in line with its July 2000 security plan, SSA's overall *Security Model* will remain incomplete.
- *Administrative and End-User Guidelines and Procedures* - Organizational responsibilities for securing certain processing environments were not clearly defined by SSA. In addition, systems administration personnel at the Data Operations Center in Wilkes Barre, PA were not sufficiently familiar with generally accepted technical approaches for securing a major processing platform at that location.

- *Monitoring Processes* - Monitoring of systems security within SSA's network and distributed systems environment has been inconsistent. SSA's program for monitoring controls over internal modems for dial-in access has been aggressive and effective. However, the effectiveness of the mainframe security monitoring process using the SMART Report needs to be further enhanced. In addition, system security monitoring at non-Headquarters facilities such as SSA's Data Operations Center and State DDS facilities has been minimal and/or ineffective. SSA has not clearly defined roles and responsibilities for monitoring security at the Data Operations Center. Although SSA outlined a monitoring program for the DDS facilities, the regional reviews have not been consistent in execution, content, or reporting.

Until corrected, a weakened or incomplete security framework will continue to impair SSA's ability to mitigate effectively the risk of unauthorized access to, and/or modification or disclosure of, sensitive SSA information. The need for a strong security framework to address threats to the security and integrity of SSA operations will grow as the agency moves ahead with plans to increase its dependence on the Internet and Web-based applications to serve the American public. 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 to enhance information protection by further strengthening its entity-wide security framework as it relates to definition, implementation, enforcement, and monitoring of technical and administrative computer security mechanisms and controls throughout the organization. We recommend that SSA:

- Reevaluate its overall organization-wide security framework;
- Conduct periodic risk assessments to identify inherent vulnerabilities across mainframe, midrange and distributed systems and implement cost-effective countermeasures to mitigate risk to an acceptable level;
- Institutionalize an entity-wide security program that prescribes detailed, platform specific technical guidance to facilitate strengthening of LAN, midrange and distributed systems security;
- Develop and implement an ongoing, entity-wide information security monitoring and compliance program that includes improving the effectiveness of the mainframe monitoring process (SMART Report);
- Assure that the appropriate level of trained resources is in place to develop, implement and monitor the SSA security program; and
- Continue to reassess the security roles and responsibilities assigned throughout the organization's headquarters and non-headquarters office components.

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

## **CONSISTENCY OF OTHER INFORMATION**

Our audit was conducted for the purpose of forming an opinion on the consolidated financial statements of SSA taken as a whole. The other accompanying information included on pages 1 to 6, 35 and 74 to end is presented for purposes of additional analysis and is not a required part of the consolidated financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on it.

The required supplementary information included on pages 7 to 34 and 54 to 55 and the required supplementary stewardship information included on pages 56 to 73 is not a required part of the consolidated financial statements but is supplementary information required by the OMB Bulletin No. 97-01 and the Federal Accounting Standards Advisory Board, respectively. 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 financial statements of SSA taken as a whole. The consolidating information included on pages 51 to 54 is presented for purposes of additional analysis of the consolidated financial statements rather than to present the financial position, changes in net position, budgetary resources and reconciliation of net cost to budgetary resources of the SSA programs. The consolidating information has been subjected to the auditing procedures applied in the audit of the consolidated financial statements and, in our opinion, is fairly stated in all material respects in relation to the consolidated financial statements taken as a whole.

## **OBJECTIVES, SCOPE AND METHODOLOGY**

SSA management is responsible for:

- Preparing the annual financial statements in conformity with accounting principles generally accepted in the United States of America;
- Establishing, maintaining, and assessing internal control that provides reasonable, but not absolute, assurance that the broad control objectives of OMB Bulletin No. 01-02, are met; and
- Complying with applicable laws and regulations.

Our responsibilities are to:

- Express an opinion on SSA's consolidated 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. 01-02, requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the consolidated statements in accordance with accounting principles generally accepted in the United States of America, 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 consolidated financial statements.

In order to fulfill these responsibilities, we:

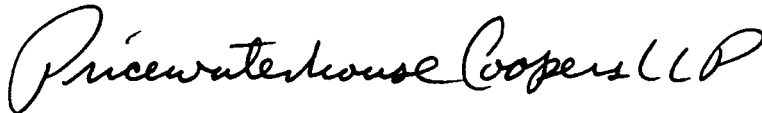
- Examined, on a test basis, evidence supporting the amounts and disclosures in the consolidated financial statements;
- Assessed the accounting principles used and significant estimates made by management;
- Evaluated the overall presentation of the consolidated financial statements;
- Obtained an understanding 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 Performance Goals and Results;
- 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 internal control 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 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.



Arlington, Virginia  
November 30, 2000



# APPENDIX







**SOCIAL SECURITY**  
Deputy Commissioner

November 29, 2000

PricewaterhouseCoopers LLP  
1616 N. Fort Myer Drive  
Arlington, Virginia 22209

Ladies and Gentlemen:

We have reviewed the draft combined report containing the Fiscal Year 2000 Report of Independent Accountants, Report on Management's Assertion About the Effectiveness of Internal Control and the Report on Compliance with Laws and Regulations. We agree with all the findings, recommendations and conclusions contained in the report and our response and comments are enclosed.

We are pleased that the report indicated that the Social Security Administration has improved its plan for maintaining continuity of operations to the extent that this area is no longer a reportable condition and that you acknowledged our notable progress in addressing the remaining reportable condition concerning protection of information. We are also pleased that your testing of compliance with laws and regulations disclosed no instances of noncompliance with the laws and regulations required to be reported under Government Auditing Standards and Office of Management Budget Bulletin Number 01-02.

Please direct any questions on our comments to Thomas G. Staples, Associate Commissioner for Financial Policy and Operations, at (410) 965-3839.

Sincerely,

William A. Halter  
Deputy Commissioner  
of Social Security

Enclosure

**Comments of the Social Security Administration (SSA)**  
**on PricewaterhouseCoopers' Draft Combined Report**  
**Containing the Fiscal Year (FY) 2000 Report of Independent Accountants,**  
**Report on Management's Assertion About the Effectiveness of Internal Control and the**  
**Report on Compliance with Laws and Regulations**

**General Comments**

Thank you for the opportunity to comment on your combined draft report containing the report of independent accountants, the report on management's assertion about the effectiveness of internal control and the report on compliance with laws and regulations. We welcome your opinion that management's assertion that SSA's systems of accounting and internal control are in compliance with the internal control objectives in Office of Management and Budget (OMB) Bulletin No. 01-02 is fairly stated, in all material respects.

We are pleased that there were no new reportable conditions identified since last year's report and that SSA has made improvements such that the reportable condition, reported in your 1999 report, that SSA needs to complete and fully test its plan for maintaining continuity of operations, is no longer a reportable condition. We will continue to make improvements to further strengthen our controls in this area.

We are also pleased that you acknowledged notable progress in addressing the remaining reportable condition that SSA needs to further strengthen controls to protect its information. As this reportable condition continues to become more focused and defined, SSA remains committed to continue making improvements to its overall information protection control structure by completing all planned actions and addressing any issues that emerge.

Furthermore, SSA is pleased that your testing of compliance with laws and regulations disclosed no instances of noncompliance with the laws and regulations required to be reported under Government Auditing Standards and OMB Bulletin No. 01-02. SSA will continue to make corrective actions concerning continuing disability reviews and the requirements referred to in the Federal Financial Management Improvement Act of 1996 so that SSA remains in compliance with the laws and regulations under which instances of noncompliance were previously reported.

SSA agrees with all the recommendations provided concerning the reportable condition that SSA needs to further strengthen controls to protect its information. Below are additional comments on the recommendations.

## **Recommendations**

**We recommend that SSA accelerate and build on its progress to enhance information protection by further strengthening its entity-wide security framework as it relates to definition, implementation, enforcement, and monitoring of technical and administrative computer security mechanisms and controls throughout the organization. We recommend that SSA:**

- **Reevaluate its overall organization-wide security framework;**

### **SSA Comment**

SSA undertook a major initiative in FY 2000 to evaluate its security framework. As a result of that activity, Regional Centers for Security and Integrity were established to elevate the visibility and impact of security functions in SSA field components. The process of reviewing Headquarters security infrastructure is ongoing and SSA executive management will continue to give this area high emphasis based on this recommendation. As SSA continues to reevaluate its organization-wide security framework, detailed technical guidance and implementing documentation will follow.

- **Conduct periodic risk assessments to identify inherent vulnerabilities across mainframe, midrange and distributed systems and implement cost-effective countermeasures to mitigate risk to an acceptable level;**

### **SSA Comment**

SSA has an ongoing risk management program in place and is currently undertaking a risk assessment of its National Computer Center. We are also initiating a vulnerability assessment of key SSA assets based on Presidential Decision Directive 63 initiatives. For application development, SSA's lifecycle has always included risk assessment activity in conjunction with development and implementation of production systems. However, based on this recommendation, SSA is undertaking activity to strengthen its risk assessment activity related to all platforms (mainframe, midrange and distributed).

- **Institutionalize an entity-wide security program that prescribes detailed, platform specific technical guidance to facilitate strengthening of local area network, midrange and distributed systems security;**

### **SSA Comment**

SSA is in the process of developing policy/risk models and technical standards for all SSA platforms. This documentation will identify standard minimal security settings for these systems, monitoring techniques and corrective actions for noncompliance. These models will

form the basis for developing an individual security matrix for each application utilizing the platform security settings and incorporating access, application and other compensating controls to supplement standard settings which will act together to mitigate application specific assessed risks to an acceptable level.

Designated roles and responsibility for implementation and oversight supplement these models. In addition, an agencywide training initiative is incorporated into SSA's strategy to ensure that authorized users having responsibility for managing these platforms fully understand the risks and maintain the security of the platform and application.

- **Develop and implement an ongoing, entity-wide information security monitoring and compliance program that includes improving the effectiveness of the mainframe monitoring process (SMART Report);**

#### **SSA Comment**

SSA is improving its existing compliance infrastructure. In conjunction with this, requirements for improvements to the SMART report have been developed and are expected to be implemented in the near future.

- **Assure that the appropriate level of trained resources is in place to develop, implement and monitor the SSA security program; and**

#### **SSA Comment**

SSA invests significant money and effort, agencywide, in training security personnel. SSA has an aggressive training program for both field and Headquarters personnel. The Agency has been a Computer Security Institute training site since 1994. It is strengthening its existing program by sponsoring Certified Information System Security Practitioner (CISSP) seminars for its security personnel. These seminars train on all 10 security domains and positions SSA attendees for CISSP certification.

In addition, SSA has increased security staffing in FY 2000 through postings and recruitment. These efforts are ongoing in order to ensure that SSA security functions are sufficiently staffed and trained.

- **Continue to reassess the security roles and responsibilities assigned throughout the organization's Headquarters and non-Headquarters office components.**

#### **SSA Comment**

The reassessment of security roles and responsibilities is an ongoing Agency process and is an integral part of the ongoing reevaluation of the overall organizational-wide security framework.