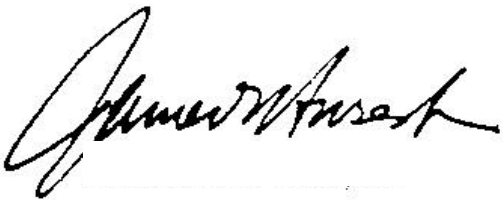
Office of the Inspector General

Message From the Acting Inspector General

I am pleased to present the opinion on the Social Security Administration's financial statements and the Office of the Inspector General's Report to the Congress for FY 1998. We continue our cooperative effort with the Agency to streamline and consolidate these reports within the Agency's Accountability Report. These reports satisfy the requirements of the Federal Managers' Financial Integrity Act and the Inspector General Act of 1978, as amended.

In FY 1998, our Office of Audit issued 56 reports with recommendations that about $2.1 billion in Federal funds could be put to better use. Our Office of Investigations worked with other Federal agencies and local law enforcement departments to obtain 6,291 criminal convictions that resulted in over $94 million in scheduled restitution, judgments, recoveries, fines, and savings. As in previous years, the dollars gained as a result of our work exceed our $48,424,000 FY 1998 budget.

I intend for the Office of the Inspector General to maintain independence and objectivity and foster a positive cooperative relationship with the Commissioner and Social Security Administration management. I will balance our need for independence with an equal responsibility to be considered a fair and valued resource to the Social Security Administration. As we continue our work to contribute to the solvency efforts by preventing fraud against the Social Security Administration's programs, we look forward to the continued support of the Commissioner and the Congress.



James G. Huse, Jr.
Acting Inspector General

Audit of the Social Security Administration's Fiscal Year 1998 Financial Statements

SOCIAL SECURITY

Office of the Inspector General

November 20, 1998

To Kenneth S. Apfel
Commissioner of Social Security

This letter transmits the PricewaterhouseCoopers LLP report on the audit of the Fiscal Year (FY) 1998 financial statements of the Social Security Administration (SSA) and the results of the Office of the Inspector General's (OIG) review thereon. PricewaterhouseCooper's report includes the firm's opinion on SSA's FY 1998 financial statements, its report on SSA management's assertion about the effectiveness of internal controls, and its report on SSA's compliance with laws and regulations.

Audit of Financial Statements, Effectiveness of Internal Controls, 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. The audit is to be performed in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States, Office of Management and Budget (OMB) Bulletin No. 98-08, *Audit Requirements for Federal Financial Statements*, and other applicable requirements. Under a contract monitored by OIG, PricewaterhouseCoopers (formerly known as Price Waterhouse), an independent certified public accounting firm, performed the audit of SSA's FY 1998 financial statements. PricewaterhouseCoopers also audited the FY 1997 financial statements, presented in SSA's Accountability Report for Fiscal Year 1998 for comparative purposes.

PricewaterhouseCoopers issued an unqualified opinion on SSA's FY 1998 financial statements and an unqualified opinion on SSA's assertion that its systems of accounting and internal control are in compliance with the internal control objective in OMB Bulletin No. 98-08. However, the audit identified three reportable conditions in SSA's internal controls. The control weaknesses identified are:

1. SSA can further strengthen controls to protect its information;
2. SSA needs to accelerate efforts to improve and fully test its plan for maintaining continuity of operations; and
3. SSA can improve controls over separation of duties.

In its FY 1997 report, PricewaterhouseCoopers recommended SSA report the above reportable conditions as material internal control weaknesses under the Federal Managers' Financial Integrity Act of 1982 (FMFIA). Reportable conditions are matters that, in the auditor's judgement, should be communicated because they represent significant deficiencies in the design or function of internal controls with potential adverse effects on SSA's ability to meet its internal control objectives. Except for a change in reporting requirements in OMB Bulletin No. 98-08 from the prior audit bulletins, the circumstances supporting last year's recommendation have not changed significantly. While OMB Bulletin 98-08 does not require auditors to recommend that reportable conditions be reported as material weaknesses under FMFIA, we still believe these deficiencies warrant inclusion in SSA's FMFIA report as material internal control weaknesses of the Agency.

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

1. SSA did not perform periodic continuing disability reviews for Title II beneficiaries as required by Section 221(i) of the Social Security Act; and
2. The cumulative effect of the three internal control weaknesses listed above resulted in a non-compliance with the Federal Financial Management Improvement Act of 1996 (FFMIA).

OIG Evaluation of PricewaterhouseCooper'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 PricewaterhouseCooper's audit of SSA's FY 1998 financial statements by:

- Reviewing PricewaterhouseCooper'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 controls;
- Reviewing PricewaterhouseCooper's audit report to ensure compliance with *Government Auditing Standards* and OMB Bulletin No. 98-08;
- 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 PricewaterhouseCoopers planned, executed and reported the results of its audit of SSA's FY 1998 financial statements in accordance with applicable standards. Therefore, it is our opinion that PricewaterhouseCooper's work generally provides a reasonable basis for the firm's opinion on SSA's FY 1998 financial statements and SSA management's assertion on the effectiveness of its internal controls and the agency's compliance with laws and regulations. Based on our review of PricewaterhouseCooper's audit, we concur with the 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
Acting Inspector General

SOCIAL SECURITY ADMINISTRATION BALTIMORE MD 21235

PRICEWATERHOUSECOOPERS

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

REPORT OF INDEPENDENT ACCOUNTANTS

To Kenneth S. Apfel
Commissioner of Social Security Administration

In our audit of the Social Security Administration (SSA) for fiscal year 1998, we found that:

- The principal financial statements were fairly stated in all material respects;
- Management fairly stated that SSA's systems of accounting and the internal control in place as of September 30, 1998 are in compliance with the internal control objectives in Office of Management and Budget (OMB) Bulletin No. 98-08, *Audits of Federal Financial Statements*, requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the principal statements in accordance with Federal accounting standards, 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, 1998 and 1997, 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. 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.

These financial statements were prepared on the basis of accounting described in Note 1 to the financial statements, which is a comprehensive basis of accounting other than generally accepted accounting principles.

In our opinion, the consolidated financial statements audited by us and appearing on pages 27 through 39 of this report present fairly, in all material respects, the financial position of SSA as of September 30, 1998 and 1997, and its consolidated net cost, changes in net position, budgetary resources and reconciliation of net costs to budgetary obligations for the fiscal years then ended, on the basis of accounting described in Note 1.

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. 98-08 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 Federal accounting standards, 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 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, 1998.

Because of inherent limitations in any internal control, 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 requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the principal statements in accordance with Federal accounting standards, 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. 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. 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 can further strengthen controls to protect its information; SSA needs to accelerate efforts to improve and fully test its plan for maintaining continuity of operations; and SSA can improve controls over separation of duties.

A material weakness, as defined by the AICPA and OMB Bulletin No. 98-08, 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 none of the three reportable conditions that follows is a material weakness as defined by the AICPA and OMB Bulletin No. 98-08. Two of the issues raised in our 1997 report are no longer reportable conditions: SSA needs to improve its software application development and change control policies and procedures; and SSA's quality control activities need improvement.

1. SSA Can Further Strengthen Controls to Protect Its Information

SSA has made noteworthy progress in addressing the information protection weaknesses raised in prior years, especially those impacting its mainframe computer processing environment. Specifically, the agency has:

- Strengthened mainframe system security by decreasing certain vulnerabilities in the mainframe operating system configuration, developing policies and procedures for better password controls, and placing access to several key system resources under the control of SSA's mainframe security software package;

- Substantially improved network monitoring procedures and practices by implementing an ongoing process to identify unauthorized modems and immediately removing access for any such unauthorized modems discovered;

- Enhanced security awareness through an increased emphasis on user training and the issuance of employee bulletins; and

- Increased its focus on entity-wide security in the distributed computing environment. SSA is currently developing an in-house automated tool that will help integrate security controls throughout the entity.

Our audit in 1998 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 local area network (LAN) and distributed systems security;

- SSA's mainframe computer security (controlling access to sensitive information);

- Physical access controls; 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 its efforts 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, the needed corrective actions include:

- Enhancing and institutionalizing the entity-wide security program;

- Further strengthening LAN and distributed systems security;

- Improving mainframe security monitoring practices;

- Reviewing and certifying system access for all users;
- Enhancing procedures for removing system access when employees are transferred or leave SSA;
- Continuing to focus on strengthening physical access controls;
- Completing certification and accreditation of SSA systems; and
- Developing and implementing an ongoing program for measuring user compliance with SSA security policies and procedures.

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

2. SSA Needs to Accelerate Efforts to Improve and Fully Test Its Plan for Maintaining Continuity of Operations

During 1998, SSA made noteworthy progress in strengthening its contingency/disaster recovery strategy for ensuring continuity of computer processing operations. For example, SSA's Principal Deputy Commissioner has directed the formation of an agency-wide inter-component workgroup, under the leadership of the Deputy Commissioner for Operations, to oversee the updating of its existing Business Impact Analysis for assessing the threats posed by a major disruption. In addition, the agency has drafted a 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 capability on short notice) to a "cold site" in the event of a longer-term disruption of processing operations, but this plan is not yet fully developed. During its most recent (June 1998) annual disaster recovery test, SSA successfully tested 10 of the current 13 critical workloads, and has begun the procurement process for further expanding its test capability (from 64 hours to 120 hours in 1999) and extending the test period so that all critical workloads can be tested by the year 2000. Finally, SSA has further updated its Emergency Response Procedures for the National Computer Center and confirmed plans to test those procedures on a quarterly basis.

While SSA has many components of a contingency/disaster recovery plan in place, we identified a number of deficiencies in those components that, in our view, would impair SSA's ability to respond effectively to a disruption in business operations as a result of a disaster or other long-term emergency. First, SSA's existing Business Impact Analysis is outdated and thus cannot be used to validate critical workloads. Second, the "cold site" implementation plan, to be used in the event of an extended outage, has not been finalized or appropriately tested. Third, while SSA has successfully tested 10 of the current 13 critical workloads, we still emphasize the need to test all critical workloads together. Finally, SSA has not adopted procedures to continuously test its contingency/disaster recovery plan and update related documentation.

While we are encouraged by the attention and level of effort SSA has directed to this issue thus far, SSA remains vulnerable should a near-term disaster occur. The agency needs to implement the following recommendations to sufficiently reduce the risks posed to continuity of operations by the previously identified deficiencies.

Recommendations

We recommend that SSA:

- Complete the Business Impact Analysis update and use the results to validate all critical workloads;
- Finalize and test as appropriate the draft "cold site" implementation plan;
- Expedite the current schedule for achieving successful testing of all critical workloads; and
- Continue to periodically test all contingency planning procedures and update the associated documentation accordingly.

3. SSA Can Improve Controls Over Separation of Duties

SSA's modernization and streamlining efforts to improve service delivery have reduced controls by giving staff the ability to perform incompatible, and thus typically segregated, functions, particularly in customer service staff positions and in the data operations environment. For example, field office staff in many cases have the responsibility and access capabilities to perform all functions related to a claims case, including initiating and adjudicating claims, establishing Social Security numbers, amending earnings records, processing death records, and other transactions. Security administrators likewise have both security and operational responsibility and associated access capability in many cases. SSA's simplified process for creating, modifying and administering access profiles for employees does not reinforce adequate control and oversight by managers of the key processes, or require a formal assessment of the risk associated with combining multiple sets of access permissions for a given individual.

To enhance its ability to meet its customer service goals, SSA has chosen to mitigate these risks through a combination of compensating controls. For example, for key transactions and processes that it considers to be at higher risk of error, SSA requires 2-PIN approval in which two different employees review and confirm these high-risk automated transactions using their personal identification number (PIN) for accessing the system. In addition, SSA has implemented reporting systems designed to detect risky or unusual transactions and produce exception reports.

SSA has made progress in implementing key recommendations from prior audit reports to further strengthen compensating controls. In 1998, SSA expanded use of the 2-PIN control process. Also, SSA is closer to initial implementation of its Comprehensive Integrity Review Process System (CIRPS). Upon implementation, and used proactively, CIRPS could enable substantial expansion and improvement of claims and security/integrity reviews, and significantly augment Audit Trail System (ATS) as a tool for detecting errors or unauthorized activity.

While these actions have improved SSA's compensating controls, they still do not sufficiently mitigate the risk associated with inadequate separation of duties. For example, according to customer service staff, the current 2-PIN process is viewed more as an impediment to efficient operations than as a preventive control. As a result, second PINs are often provided without sufficient scrutiny, and the 2-PIN process is frequently a peer-to-peer review. Similarly, weaknesses still exist in several of the most significant compensating control mechanisms, such as the ATS, that in our view substantially reduce their reliability.

Recommendations

We recommend that SSA:

- Strengthen the use of the 2-PIN control process. Second-PIN providers should receive additional training on how to exercise the appropriate oversight to reduce the risk of error, fraud, waste, and abuse. In addition, for the most sensitive transactions and functions, the provision of a second PIN should be provided by higher-level SSA personnel or personnel from a separate organizational unit, which may be in a remote location.

- Maximize the benefits offered by detective tools such as ATS and CIRPS, by using them proactively. To do so, SSA should first develop tolerance level standards and metrics for high-risk transactions and risky transaction combinations. Next, SSA should actively detect and measure the occurrence of high-risk transactions, such as, by job function and field office size and assess their significance using an analytical model. Finally, SSA should create formal mechanisms to provide feedback on these results and incorporate that feedback into the process for making internal control decisions. The results of these measurement and analysis activities may indicate that SSA needs to improve the current methodology for creating, modifying, and administering access control software profiles. If so, process-wide oversight should be made a part of the methodology, enabling more proactive profile management and formal acknowledgement of risk acceptance.

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.

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, 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.

- 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. SSA's management estimated the total backlog of Title II cases yet to be reviewed for continuing eligibility at 1.6 million cases. If CDRs are not performed timely, beneficiaries who are no longer eligible for disability may inappropriately continue to receive benefits, including Medicare benefits.

- 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. We found weaknesses in information protection, business continuity planning and separation of duties, 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.

OBJECTIVES, SCOPE AND METHODOLOGY

SSA management is responsible for:

- Preparing the annual financial statements in conformity with the basis of accounting described in Note 1;
- Establishing, maintaining, and assessing internal control that provide reasonable, but not absolute, assurance that the broad control objectives of OMB Bulletin No. 98-08 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, *Audits of Federal Financial Statements*, requiring that transactions be properly recorded, processed, and summarized to permit the preparation of the principal statements in accordance with Federal accounting standards, 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 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.

PRICEWATERHOUSECOOPERS

We did not evaluate all the 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 the internal control.

* * * * *

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

This report is intended for the information of the management and the Inspector General of SSA, OMB and the Congress. However, this report is a matter of public record and its distribution is not limited.

PricewaterhouseCoopers LLP

Arlington, Virginia
November 20, 1998

APPENDIX

SOCIAL SECURITY
Office of the Commissioner

November 13, 1998

PricewaterhouseCoopers
1616 N. Fort Myer Drive
Arlington, Virginia 22209

Ladies and Gentlemen:

We have reviewed the 1998 draft report on management's assertion about the effectiveness of the Social Security Administration's (SSA) internal controls and compliance with laws and regulations and generally agree with all findings and recommendations except as noted in our attached comments.

We are pleased that sufficient improvement was made in the software development and quality assurance areas so that they were not reported again in this year's report. We were also pleased that you reported significant progress in the three reportable conditions addressed in this report. We will continue to work with you to correct the remaining conditions as quickly as possible. Please direct any questions on our comments to Steven L. Schaeffer at extension 53927.

Sincerely,

John R. Dyer
Acting Principal Deputy Commissioner
of Social Security

Enclosure

cc:
Pamela J. Gardiner (OIG)
Debbie Sebastian (GAO)

SOCIAL SECURITY ADMINISTRATION BALTIMORE MD 21235-0001

Comments of the Social Security Administration (SSA) on PricewaterhouseCoopers' Draft Report on Management's Assertion About the Effectiveness of SSA's Internal Controls and Compliance with Laws and Regulations

General Comments

Thank you for the opportunity to comment on your draft report on the effectiveness of SSA's internal controls and compliance with laws and regulations. We welcome your opinion that management's assertion that SSA's systems of accounting and internal controls are in compliance with the internal control objective in Office of Management and Budget (OMB) Bulletin 98-08 is fairly stated in all material respects.

We are pleased that there were no new reportable conditions identified since last year's audit and that sufficient progress was made in the areas of software development and change control and quality assurance to no longer identify those two reportable conditions from fiscal year (FY) 1997 as reportable conditions in FY 1998. We will continue to make improvements in those two areas until all of our plans for corrective action have been implemented.

We are also pleased that you reported significant progress in the three reportable conditions addressed in this report, i.e., protection of data, continuity of operations and separation of duties. At this point, we have completed corrective action on the majority of the recommendations in these three areas from last year's report and will continue making improvements until all planned actions are completed.

Report on Management's Assertion About the Effectiveness of Internal Controls

Finding 1, SSA Can Further Strengthen Controls to Protect Its Information

Recommendations:

We recommend that SSA accelerate its efforts 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, the needed corrective actions include:

- **Enhancing and institutionalizing the entity-wide security program;**

SSA Comment

SSA agrees with this recommendation and has made substantial progress in this area in the last year, including: the issuance of new password guidelines requiring the password length to be a minimum of six characters and implementation of the software changes necessary to enforce this new policy; the conversion of the Financial ACcounTing System (FACTS) to the Integrated Database Management System enabling it to be fully controlled by TOP SECRET; the coverage of the national FALCON region under TOP SECRET; and, the expansion and improvement of the Agency's security awareness program, including frequent reminders of employees' responsibilities. SSA will continue to enhance and institutionalize the entity-wide security program through a series of actions, including:

1. Implement Enterprise Security Interface (ESI) throughout the enterprise which will integrate user authentication and functional level security for WIN-NT distributed applications with the mainframe TOP SECRET security policies and rules. The ESI rollout is on target and will be accomplished on a flow basis over the next 1-2 years.

2. Install a commercial enterprise management software product, CA-UNICENTER TNG, on all UNIX platforms.

3. Convert Processing Center FALCON regions to TOP SECRET in the next 1-2 years.

- **Further strengthening Local Area Network and distributed systems security;**

SSA Comment

SSA agrees with this recommendation and will continue to make improvements, with emphasis on controlling unauthorized access.

In the last year, SSA has made significant progress in improving this area, particularly in the reassessment of dial-in access to systems resources and the development of safeguards in this area. Modems not approved by the Agency have been removed and a nationwide registration, approval and monitoring procedure was implemented in the last year. In addition, SSA took action to ensure that all users disable the automatic logon features in the WIN-NT configuration, that all passwords meet SSA's new standards and that workstation passwords are changed regularly. SP3 was implemented for the WIN-NT network on installed platforms and it will be included in all future installations. The current VISN system now employs a dial-in history file and an audit trail log of password encrypted files sent to each customer. A firewall and other architectural modifications have been made to the Bulletin Board system.

As mentioned earlier, SSA plans to further improve the security of its distributed environment by implementing ESI over the next 1-2 years and installing a commercial management software product on all UNIX platforms. Additionally, SSA will install "stealth" devices at each of the major network nodes that connect to the enterprise environment to detect hacker attacks. These devices will provide an additional level of monitoring and real-time alerts in the event that a break-in occurred from one of the remote offices.

- **Improving mainframe security monitoring practices;**

SSA Comment

SSA agrees with this recommendation and will work with the auditors to improve our mainframe security monitoring practices. SSA is planning a mechanism which will focus the security violation reports and make them available to the appropriate level manager. Requirements have been developed and submitted for program development.

- **Reviewing and certifying system access for all users;**

SSA Comment

SSA agrees with the recommendation and will continue to make improvements in this area. SSA currently has in place a process to review and certify systems access for all users, but recognizes that improvements are possible. SSA established a workgroup led by the Office of Systems to develop and implement a standardized security profile structure for all users. Subsequent to the auditor's recommendation, we have also reviewed systems access for users in selected categories, i.e., users with security administration authority, programmers and users who have separated or transferred.

- **Enhancing procedures for removing system access when employees are transferred or leave SSA;**

SSA Comment

SSA agrees with this recommendation and will continue to improve our procedures for removing system access when employees are transferred or leave SSA. SSA had a mechanism in place since the early 1990's to interface its TOP SECRET access file with its Human Resources Management Information System. However, based on the auditor's recommendation we have taken steps to improve the procedures in this area. A requirement which will improve our interface in the areas noted has been submitted to the Office of Systems. The enhancement is in the requirements and development stage.

- **Continuing to focus on strengthening physical access controls;**

SSA Comment

SSA agrees with this recommendation and will continue to focus on strengthening physical security, particularly in the National Computer Center (NCC). SSA has reemphasized guard procedures for checking building access and property passes and in challenging unauthorized persons in restricted areas. SSA has also made improvements in exterior lighting, perimeter fencing, and trimming of foliage along the fence. In addition, SSA is updating its camera coverage within the NCC.

- **Completing certification and accreditation of SSA systems; and**

SSA Comment

SSA agrees with this recommendation and recertified all of its sensitive systems, including TOP SECRET, in January 1998. SSA management and the Office of the Inspector General will continue to periodically review TOP SECRET to ensure it remains effective. As recommended in last year's audit, SSA designated FACTS, FALCON, Death Alert, Control and Update System and the Audit Trail System (ATS) as sensitive systems, designated systems managers for each system and expects to have sensitive system security plans prepared and approved by June 1999.

- **Developing and implementing an ongoing program for measuring user compliance with SSA security policies and procedures.**

SSA Comment

SSA agrees with this recommendation and has a number of existing and planned programs to measure user compliance with security policies and procedures. We currently monitor compliance through General Accounting Office/OIG audits, financial systems reviews, management control reviews, integrity reviews and other studies/reviews.

SSA is developing the Comprehensive Integrity Review Process (CIRP) which will consolidate integrity review functions into a single automated facility where transactions will be screened against specific criteria, including cross-application criteria. SSA has already implemented a CIRP release pertaining to Alpha-Index, Detailed Earnings Query to determine if requests relate to relatives, co-workers, managers, agency or regional executive staff, local or nationally prominent celebrities and employees' own records. The Agency also implemented the Identification (ID) Query Review which selects those ID queries that cannot be related to a known SSA workload. The next release due in March 1999 will pertain to enumeration actions and later releases will pertain to title II and XVI transactions.

Finding 2, SSA Needs to Accelerate Efforts to Improve and Fully Test Its Plan for Maintaining Continuity of Operations

Recommendations:

- **Complete the Business Impact Analysis update and use the results to validate all critical workloads.**

SSA Comment

SSA agrees with this recommendation and has formed a workgroup to conduct a business impact analysis which includes the review and confirmation of critical workloads and priorities. The workgroup will review and consider the current Agency Contingency (Disaster Recovery) Plan, the Agency Strategic Plan, the Agency Business Plan, the Information Systems Plan and the Governmentwide Study on Infrastructure.

The workgroup plans to produce a report in January 1999 which will describe: current recovery measures; the results of the analysis, including recommended changes to the critical workloads and priorities; and, the Agency's review process which will include a major comprehensive review every 6 years and an interim 3-year review of a lesser nature.

- **Finalize and test as appropriately the draft "cold site" implementation plan.**

SSA Comment

SSA agrees with this recommendation and plans to populate the cold site, if needed, during the 6-week period at the hot site. We are expanding the Disaster Recovery Plan for NCC Operations to reflect the strategy and procedures for equipping the cold site, but do not intend to test that portion of the plan, i.e., acquiring and installing replacement equipment and setting up a functioning computer center in the cold site. Rather, the goal is to have the necessary plan and steps in place to accomplish this. SSA has a high degree of confidence that the cold site can be fully equipped either by SSA or by a contractor in a very short period of time.

The Agency Contingency Plan (Disaster Recovery Plan) and pertinent test plans and capacity issues will be resolved and documented by June 30, 1999.

- **Expedite the current schedule for achieving successful testing of all critical workloads.**

SSA Comment

SSA agrees with this recommendation and has developed an applications test plan in August 1998 that ensures that each critical workload will be tested at least once within a 3-year cycle. We will develop capacity requirements to enable testing of all critical workloads together in a subsequent test. SSA plans for a 5-day test in 1999 and two 4-day tests both in 2000 and 2001.

- **Continue to periodically test all contingency planning procedures and update the associated documentation accordingly.**

SSA Comment

SSA agrees with this recommendation and has completed an update of the Emergency Response Procedure (ERP), including revising team procedures, staff names and call lists in September 1998. We also completed a review of the ERP to the COMDISCO contract in July 1998. SSA plans to review, test and reissue procedures quarterly in the future.

Finding 3, SSA Can Improve Controls Over Separation of Duties

Recommendations:

- **Strengthen the use of the 2-Personal Identification Number (PIN) control process. Second-PIN providers should receive additional training on how to exercise the appropriate oversight to reduce the risk of error, fraud, waste, and abuse. In addition, for the most sensitive transactions and functions, the provision of a second PIN should be provided by higher-level SSA personnel or personnel from a separate organizational unit, which may be in a remote location.**

SSA Comment

SSA partially agrees with this recommendation and will strengthen the use of the 2-PIN control process and will remind field office employees of the responsibilities and duties associated with a second PIN action.

We request that the auditor reconsider the recommendation that for the most sensitive transactions and functions, the provision of a second PIN be provided by higher-level SSA personnel or personnel from a separate organizational unit, which may be in a remote location. We believe that the current streamlined measures followed in the field offices provide excellent service to the public in a timely manner and also includes adequate management controls. Currently, we give our field office managers the flexibility to designate persons to help with the different approval processes with the stipulation that the designee cannot have performed an action on the case he/she is approving.

- **Maximize the benefits offered by detective tools such as ATS and CIRP, by using them proactively. To do so, SSA should first develop tolerance level standards and metrics for high-risk transactions and risky transaction combinations. Next, SSA should actively detect and measure the occurrence of high-risk transactions, such as, by job function and field office size and assess their significance using an analytical model. Finally, SSA should create formal mechanisms to provide feedback on these results and incorporate that feedback into the process for making internal control decisions. The results of these measurement and analysis activities may indicate that SSA needs to improve the current methodology for creating, modifying, and administering access control software profiles. If so, process-wide oversight should be made a part of the methodology, enabling more proactive profile management and formal acknowledgement of risk acceptance.**

SSA Comment

We agree with this recommendation and will work with the auditor to develop the process. We request that the auditor provide us specific examples to follow to implement the recommendation.

Concerning the comment on access control software profiles, SSA recently added this to its Security Integrity 5-Year Plan but it has not yet been scheduled.

Report on Compliance with Laws and Regulations

Recommendations:

- **SSA is not in full compliance of Section 221(i) of the Social Security Act which requires periodic Continuing Disability Reviews (CDRs) for Title II beneficiaries. SSA's management estimated the total backlog of Title II cases yet to be reviewed for continuing eligibility at XXXXX million cases. If CDRs are not performed timely, beneficiaries who are no longer eligible for disability may inappropriately continue to receive benefits, including Medicare benefits.**

SSA Comment

SSA agrees with this recommendation and is currently determining the current backlog of CDRs and will provide that information to you as soon as it is available. We did over 146,889 more CDRs than originally planned in FY 1998 and, as a result, are updating our 7-year plan.

While we agree that SSA has not been in full compliance with Section 221(I) of the Social Security Act, we believe that SSA's efforts to become compliant should be recognized. We recommend that the following language be added to the end of the first bullet:

"Recognizing its responsibility to meet the requirements of the law, SSA has a plan to eliminate the backlog of title II CDRs. SSA now has completed its third year of the plan and is on target to eliminate the backlog by FY 2000."

- **Under the Federal Financial Management Improvement Act (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. We found**

  weaknesses in information protection, business continuity planning and separation of duties, 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 Comment

SSA partially agrees with this finding, specifically that part concerning the three findings mentioned earlier in the report pertaining to protection of information, continuity of operations and separation of duties. The Agency is continuing to make improvements in those areas as shown in this letter.

We do not agree, however, that these are instances of substantial noncompliance. As the auditor's report indicated, SSA has made noteworthy progress in correcting the conditions reported in those three areas. We believe we have progressed sufficiently to be in substantial compliance in all three areas. Further, we believe that SSA is overall in substantial compliance with FFMIA. Nonetheless, SSA will continue to make improvements as stated herein.