AUDITOR'S REPORTS

SOCIAL SECURITY

November 8, 2010

The Honorable Michael J. Astrue
Commissioner

The *Chief Financial Officers (CFO) Act of 1990* (P.L. 101-576), as amended, requires that the Social Security Administration's (SSA) Inspector General (IG) or an independent external auditor, as determined by the IG, audit SSA's financial statements in accordance with applicable standards. Under a contract monitored by the Office of the Inspector General (OIG), Grant Thornton, LLP, an independent certified public accounting firm, audited SSA's Fiscal Year (FY) 2010 financial statements. This letter transmits Grant Thornton's *Independent Auditor's Report* on the audit of SSA's FY 2010 financial statements. Grant Thornton's Report includes the following:

- Opinion on Financial Statements;
- Opinion on Management's Assertion about the Effectiveness of Internal Control; and
- Report on Compliance and Other Matters.

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.

Grant Thornton's audit was conducted in accordance with auditing standards generally accepted in the United States; Government Auditing Standards issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 07-04, Audit Requirements for Federal Financial Statements. The audit included obtaining an understanding of the internal control, testing and evaluating the design and operating effectiveness of the internal control, and performing such other procedures as considered necessary under the circumstances. Because of inherent limitations in any internal control, misstatements because of error or fraud may occur and not be detected. The risk of fraud is inherent to many of SSA's programs and operations, especially within the Supplemental Security Income program. In our opinion, people outside the organization perpetrate most of the fraud against SSA.

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

OIG audited SSA's FY 2009 financial statements and issued an unqualified opinion on the statements. In its audit of the FY 2010 financial statements, Grant Thornton issued an unqualified opinion. Grant Thornton also reported that SSA had effective internal control over financial reporting based on criteria under OMB Circular A-123, *Management's Responsibility for Internal Control* and SSA's financial management systems substantially complied with the requirements of the *Federal Financial Management Improvement Act of 1996*.

However, Grant Thornton did identify three deficiencies in internal control that, when aggregated, are considered to be a significant deficiency related to a weakness in controls over information security. Specifically, Grant Thornton testing:

1. Disclosed that policies and procedures to reassess periodically the content of security access profiles had not been complied with consistently throughout the Agency.
2. Disclosed evidence that security permissions provided to some employees and contractors were in excess of access required to complete their job responsibilities.
3. Identified configurations that increased the risk of unauthorized access to key financial data and programs during our testing of the mainframe operating system

Grant Thornton identified no reportable instances of noncompliance with the laws, regulations, or other matters tested.

OIG Evaluation of GT Audit Performance

To fulfill our responsibilities under the CFO Act and related legislation for ensuring the quality of the audit work performed, we monitored Grant Thornton's audit of SSA's FY 2010 financial statements by

- reviewing Grant Thornton'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, assessing SSA's internal control, and substantive testing;
- reviewing Grant Thornton's audit report to ensure compliance with Government Auditing Standards and OMB Bulletin No. 07-04;
- coordinating the issuance of the audit report; and
- performing other procedures we deemed necessary.

Grant Thornton is responsible for the auditor's report, dated November 8, 2010, and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding Grant Thornton's performance under the terms of the contract. Our review, as differentiated from an audit in accordance with applicable auditing standards, was not intended to enable us to express, and accordingly we do not express, an opinion on SSA's financial statements, management's assertions about the effectiveness of its internal control over financial reporting, or SSA's compliance with certain laws and regulations. However, our monitoring review, as qualified above, disclosed no instances where Grant Thornton did not comply with applicable auditing standards.

Patrick P. O'Carroll, Jr.
Inspector General

Audit • Tax • Advisory
Grant Thornton LLP
333 John Carlyle Street, Suite 500
Alexandria, VA 22314-5745
T 703.837.4400
F 703.837.4455
www.grantthornton.com

To the Honorable Michael J. Astrue
Commissioner
Social Security Administration

Independent Auditor's Report

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

- The consolidated balance sheet of SSA as of September 30, 2010, and the related consolidated statement of net cost and changes in net position, and the combined statement of budgetary resources for the year then ended and the statement of social insurance as of January 1, 2010 are presented fairly, in all material respects, in conformity with accounting principles generally accepted in the United States of America;
- Management fairly stated that SSA's internal control over financial reporting was operating effectively as of September 30, 2010;
- No reportable instances of noncompliance with laws, regulations or other matters tested.

OPINION ON FINANCIAL STATEMENTS

We have audited the accompanying consolidated balance sheet of the SSA as of September 30, 2010, and the related consolidated statement of net cost and changes in net position, and the combined statement of budgetary resources for the year then ended, and the statement of social insurance as of January 1, 2010. These financial statements are the responsibility of SSA's management. Our responsibility is to express an opinion on these financial statements based on our audit.

The consolidated balance sheet of SSA as of September 30, 2009, and the related consolidated statement of net cost and changes in net position, and the combined statement of budgetary resources for the year then ended were audited by other auditors whose report dated November 9, 2009 expressed an unqualified opinion on those statements. The statements of social insurance as of January 1, 2009, 2008, 2007, and 2006 were also audited by other auditors whose reports dated November 9, 2009 and November 7, 2008 expressed an unqualified opinion on those statements.

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 Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements.* 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 audit provides a reasonable basis for our opinion.

In our opinion, the financial statements referred to above and presented on pages 100 through 130 of this *Performance and Accountability Report* (PAR), present fairly, in all material respects, the financial position of SSA as of September 30, 2010, and its net cost of operations, changes in net position, and budgetary resources for the year then ended, and the financial condition of its social insurance program as of January 1, 2010, in conformity with accounting principles generally accepted in the United States of America.

Our audit was conducted for the purpose of forming an opinion on the consolidated and combined financial statements taken as a whole. The Additional Information presented on the statement of social insurance as of January 1, 2010 is presented for purposes of additional analysis and is not a required part of the consolidated and combined financial statements. Such information has been subjected to the auditing procedures applied in the audit of the consolidated and combined financial statements and, in our opinion, is fairly stated in all material respects in relation to the consolidated and combined financial statements taken as a whole.

As discussed in Note 17 to the financial statements, the statement of social insurance presents the actuarial present value of the SSA's estimated future income to be received from or on behalf of the participants and estimated future expenditures to be paid to or on behalf of participants during a projection period sufficient to illustrate long-term sustainability of the social insurance program. In preparing the statement of social insurance, management considers and selects assumptions and data that it believes provide a reasonable basis for the assertions in the statements. However, because of the large number of factors that affect the statement of social insurance and the fact that future events and circumstances cannot be known with certainty, there will be differences between the estimates in the statement of social insurance and the actual results, and those differences may be material.

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

We have also audited management's assertion, included in the accompanying *Federal Managers' Financial Integrity Act* (FMFIA) Assurance Statement on page 43 of this PAR that SSA's internal control over financial reporting was operating effectively as of September 30, 2010 based on criteria established under OMB Circular No. A-123, *Management's Responsibility for Internal Control.* We did not test all internal controls, relevant to the operating objectives broadly, defined by the *Federal Managers' Financial Integrity Act of 1982.* SSA's management is responsible for maintaining effective internal control over financial reporting and for its assertion of the operating effectiveness of internal control over financial reporting. Our responsibility is to express an opinion on management's assertion based on our audit.

We conducted our audit 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. 07-04. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

An agency's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with generally accepted accounting principles. An agency's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the agency;

(2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the agency are being made only in accordance with authorizations of management and those charged with governance; and (3) provide reasonable assurance regarding prevention, or timely detection and correction of unauthorized acquisition, use, or disposition of the agency's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls 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 internal control over financial reporting was operating effectively as of September 30, 2010, is fairly stated, in all material respects based on criteria established under OMB Circular No. A-123.

Other Internal Control Matters

Our work identified the need to improve certain internal controls, as described below and in a separate, limited-distribution management letter. A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the agency's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. Our audit was not designed to identify all deficiencies in internal control over financial reporting that might be significant deficiencies. We identified the following deficiencies that we consider, in combination, to be a significant deficiency in SSA's internal control over financial reporting.

Significant Deficiency

Weakness in Controls Over Information Security

Our testing disclosed that policies and procedures to periodically reassess the content of security access profiles had not been complied with consistently throughout the Agency. Our testing also disclosed evidence that security permissions provided to some employees and contractors were in excess of access required to complete their job responsibilities. Additionally, we identified configurations that increased the risk of unauthorized access to key financial data and programs during our testing of the mainframe operating system.

Specific disclosure of detailed information about these exposures might further compromise controls and are therefore not provided within this report. Rather, the specific details of weaknesses noted are presented in a separate, limited-distribution management letter.

Recommendations

We recommend that SSA management implement policies and procedures that require a periodic review of the content of all security profiles. These policies and procedures should enforce a consistent approach for profile review and should require auditable artifacts to evidence the completion of these reviews. If designed appropriately and implemented effectively, management should be able to decrease the risk of personnel and contractors maintaining excessive access to transactions and data.

We also recommend that management implement controls to test and monitor configurations on the mainframe to identify and address inherent security risks. This should include a comprehensive procedure to test new software and updates to existing software on the mainframe prior to implementation. Management must also implement procedures that require on-going monitoring of implemented mainframe configurations to identify and address security risks.

More specific recommendations focused on the individual exposures we identified are included in a separate limited-distribution management letter, which also includes management's response and their planned corrective actions.

REPORT ON COMPLIANCE AND OTHER MATTERS

The management of SSA is responsible for compliance with laws and regulations. As part of obtaining reasonable assurance about whether the financial statements are free of material misstatement, we performed tests of the compliance with laws and regulations, including laws governing the use of budgetary authority, government-wide policies and laws identified in Appendix E of OMB Bulletin No. 07-04, and other laws and regulations, noncompliance with which could have a direct and material effect on the financial statements. Under the *Federal Financial Management Improvement Act of 1996* (FFMIA), we are required to report whether the SSA's financial management systems substantially comply with the Federal financial management systems requirements, applicable Federal accounting standards, and the United States Government Standard General Ledger at the transaction level. To meet this requirement, we performed tests of compliance with FFMIA section 803(a) requirements.

We did not test compliance with all laws and regulations applicable to SSA. We limited our tests of compliance to the provisions of laws and regulations cited in the preceding paragraph of this report. Providing an opinion on compliance with those provisions was not an objective of our audit, 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 or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 07-04 and no instances of substantial noncompliance that are required to be reported under FFMIA.

OTHER INFORMATION

The Management's Discussion and Analysis (MD&A) included on pages 5 through 46 and the Required Supplementary Information (RSI) included on pages 136 through 151 of this PAR are not a required part of the consolidated and combined financial statements but are supplementary information required by the Federal Accounting Standards Advisory Board and OMB Circular No. A-136, *Financial Reporting Requirements.* We have applied certain limited procedures, which consisted principally of inquiries of management regarding the methods of measurement and presentation of the MD&A and RSI. However, we did not audit the information and express no opinion on it.

Our audit was conducted for the purpose of forming an opinion on the consolidated and combined financial statements taken as a whole. The Schedule of Budgetary Resources included on page 135 of this PAR is not a required part of the consolidated and combined financial statements but is supplementary information required by OMB Circular No. A-136. This schedule and the consolidating and combining information included on pages 131 to 134 of this PAR are not a required part of the consolidated and combined financial statements. Such information has been subjected to the auditing procedures applied in the audit of the consolidated and combined financial statements and, in our opinion, is fairly stated in all material respects in relation to the consolidated and combined financial statements taken as a whole.

The Commissioner's Message on page 1 and the other accompanying information included on pages 2 through 4, 47 through 96 and 163 to the end of this PAR is presented for purposes of additional analysis and is also not a required part of the financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the consolidated and combined financial statements, and accordingly, we express no opinion on it.

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

Grant Thornton LLP

Alexandria, Virginia
November 8, 2010

SOCIAL SECURITY
The Commissioner

November 1, 2010

Grant Thornton LLP
333 John Carlyle
Alexandria, VA 22314

Ladies and Gentlemen:

We have reviewed the draft Independent Auditor's Report concerning your audit of our fiscal year 2010 financial statements. We are extremely pleased that we received our 17th consecutive unqualified opinion on our financial statements, an unqualified opinion on management's assertion that our internal controls were operating effectively, and that there were no reportable instances of noncompliance with laws or regulations.

Your report did identify a significant deficiency regarding the need to improve certain internal controls. We concur with this finding and will implement the necessary corrective actions to strengthen our internal controls. We have enclosed a more detailed explanation of our plans.

If you have questions, please do not hesitate to contact me or have your staff contact Carla Krabbe at (410) 965-0759.

Sincerely,

Michael J. Astrue

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Enclosure - Page 1 - Grant Thornton LLP

Comments of the Social Security Administration (SSA) on Grant Thornton LLP's Draft Independent Auditor's Report

General Comments

Thank you for the opportunity to comment on the draft Independent Auditor's Report concerning our fiscal year (FY) 2010 financial statements.

We are pleased that your report indicates our internal control over financial reporting is operating effectively. However, the report did note the need for additional improvements over certain internal controls and contained related recommendations.

The agency continues to strengthen our already robust security program. We utilize a layered approach to securing our information and systems. Access controls, including mainframe security profiles, limit access based upon the security principles of "least privileged access" and "need to know." We also capture audit and integrity review information to detect inappropriate or suspicious activity, and train our security officers to monitor security violation reports. Additionally, we provide security awareness training and warnings to employees reminding them of their obligation not to access unauthorized information.

We will continue to work to improve the overall effectiveness of our security controls. We agree with your recommendations and offer the following comments.

Recommendation 1

We recommend that SSA management implement policies and procedures that require a periodic review of the content of all security profiles. These policies and procedures should enforce a consistent approach for profile review and should require auditable artifacts to evidence the completion of these reviews. If designed appropriately and implemented effectively, management should be able to decrease the risk of personnel and contractors maintaining excessive access to transactions and data.

Comment

We agree with the recommendation. In January 2010, an agency workgroup convened to develop new policies and procedures for conducting periodic reviews of the content of our security profiles. We plan to implement these new policies and procedures in FY 2011. We also initiated a project to develop and implement a commercial off-the-shelf (COTS) based software solution to automate the process of reviewing security profile content. The Office of the Chief Information Officer is working with the Office of Systems to define the functional and technical requirements for this automated solution. This solution will provide improved tools to assist security officers with reviewing security profile content and provide auditable evidence of the completion of these reviews. This solution helps ensure that both agency-wide and locally managed

security profiles are reviewed consistently throughout the agency and will provide management information for monitoring the progress of profile reviews. We will base the automated COTS solution on the procedures drafted by the agency workgroup. Additionally, the COTS solution will improve our Triennial Certification program by providing meaningful information to managers needed for conducting reviews of access granted to employees and contractors.

Recommendation 2

We also recommend that management implement controls to test and monitor configurations on the mainframe to identify and address inherent security risks. This should include a comprehensive procedure to test new software and updates to existing software on the mainframe prior to implementation. Management must also implement procedures that require ongoing monitoring of implemented mainframe configurations to identify and address security risks.

Comment

We agree with the recommendation. While the mainframe configuration increased the risk of unauthorized access, the likelihood of this happening was extremely low. As soon as we became aware of the weakness, we took remedial action that addressed the weakness. We implemented specific controls to identify and address security risks of this nature, and we are expanding current procedures to identify and address mainframe security risks.