

AUDITOR'S REPORTS



December 9, 2013

The Honorable Carolyn W. Colvin
Acting Commissioner

The *Chief Financial Officers Act of 1990 (CFO)* (Pub. L. No. 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) 2013 financial statements. Grant Thornton, LLP, also audited the FY 2012 financial statements presented in SSA's FY 2013 Agency Financial Report for comparative purposes. This letter transmits the Grant Thornton, LLP, *Independent Auditor's Report* on the audit of SSA's FY 2013 financial statements. Grant Thornton, LLP's, Report includes the following.

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

Objective of a Financial Statement Audit

The objective of a financial statement audit is to obtain reasonable assurance that 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 an assessment of the accounting principles used, and significant estimates made, by management as well as an evaluation of the overall financial statement presentation.

Grant Thornton, LLP, conducted its audit 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. 14-02, *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 due to 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

Grant Thornton, LLP, issued an unmodified opinion¹ on SSA's FY 2013 and 2012 financial statements. Grant Thornton, LLP, also reported that SSA was maintaining effective internal control over financial reporting as of September 30, 2013 based on criteria under OMB Circular A-123, *Management's Responsibility for Internal Control*, and the *Federal Manager's Financial Integrity Act of 1982* (FMFIA).

However, Grant Thornton, LLP, did identify two significant deficiencies in internal controls.

Significant Deficiency - Information Systems Control

It is Grant Thornton, LLP's, opinion that SSA made significant progress in strengthening controls over its information systems to address the material weakness reported in FY 2012. While SSA made these significant efforts to strengthen controls over its systems and address weaknesses, Grant's Thornton, LLP's, FY 2013 testing continues to identify control issues in both design and operation of key controls. In its audit, Grant Thornton, LLP, identified four deficiencies that, when aggregated, are considered to be a significant deficiency in the areas of Information Systems Control. Specifically, Grant Thornton, LLP's, testing disclosed

1. lack of a comprehensive Agency-wide policies and procedures related to vulnerability management, including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure/validation;
2. lack of comprehensive Agency-wide policies and procedures related to management of application and system software changes, including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk and requirements for the review and approval of testing results;
3. lack of controls related to the identification and monitoring of high-risk programs operating on the mainframe; and
4. weaknesses in logical access controls, such as access authorization, access removal, profile content, and analysis review program and supporting profile controls.

Significant Deficiency - Calculation, Recording, and Prevention of Overpayments

In addition to the Information Systems Control significant deficiency, Grant Thornton, LLP, identified three deficiencies in internal control that, when aggregated, are considered to be a significant deficiency related to weaknesses in internal controls related to Calculation, Recording, and Prevention of Overpayments. Specifically, Grant Thornton, LLP's, testing disclosed

1. overpayment calculation errors with 38 percent of items selected in its statistical sample;
2. system limitations where overpayment receivable installments extending past year 2049 are not systematically tracked and reported; and
3. a control failure where SSA was not reconciling key data fields between SSA internal databases, resulting in overpayment errors.

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

¹ Grant Thornton, LLP, issued an unqualified opinion on SSA's FY 2012 financial statements. The American Institute of Certified Public Accountants (AICPA) generally accepted auditing standard AU-C section 700.19 requires the auditor to express an "unmodified opinion" when the auditor concludes that the financial statements are presented fairly, in all material respects, in accordance with the applicable financial reporting framework for audits of financial statements ending on or after December 15, 2012. For consistency, we will refer to an unqualified opinion as an "unmodified opinion" for all fiscal years.

OIG Evaluation of Grant Thornton, LLP, 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, LLP's, audit of SSA's FY 2013 financial statements by

- reviewing Grant Thornton, LLP's, audit approach and planning;
- evaluating its auditors qualifications and independence;
- monitoring the audit's progress at key points;
- examining Grant Thornton, LLP's, documentation related to planning the audit, assessing SSA's internal control, and substantive testing;
- reviewing Grant Thornton, LLP's, audit report to ensure compliance with Government Auditing Standards and OMB Bulletin No. 14-02;
- coordinating the issuance of the audit report; and
- performing other procedures we deemed necessary.

Grant Thornton, LLP, is responsible for the attached auditor's report, dated December 9, 2013, and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding Grant Thornton, LLP'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, LLP, did not comply with applicable auditing standards.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of this report to appropriate congressional committees with oversight and appropriation responsibilities over SSA. In addition, we will post a copy of the report on our public Website.



Patrick P. O'Carroll, Jr.
Inspector General



Audit • Tax • Advisory
Grant Thornton LLP
333 John Carlyle Street, Suite 400
Alexandria, VA 22314-5745
T 703.837.4400
F 703.837.4455
www.GrantThornton.com

The Honorable Carolyn W. Colvin
Acting Commissioner
Social Security Administration

INDEPENDENT AUDITOR'S REPORT

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

- The consolidated balance sheets of SSA as of September 30, 2013 and 2012, the related consolidated statements of net cost and changes in net position, the combined statements of budgetary resources for the years then ended, the statements of social insurance as of January 1, 2013 and January 1, 2012 and statement of changes in social insurance amounts for the periods January 1, 2012 to January 1, 2013 and January 1, 2011 to January 1, 2012 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, 2013; and
- No reportable instances of noncompliance with laws, regulations, or other matters tested.

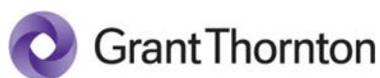
The following sections outline each of these conclusions in more detail.

OPINION ON FINANCIAL STATEMENTS

We have audited the accompanying consolidated balance sheets of SSA as of September 30, 2013 and 2012, the related consolidated statements of net cost and changes in net position, the combined statements of budgetary resources for the years then ended, the statements of social insurance as of January 1, 2013, January 1, 2012, January 1, 2011, and January 1, 2010 and the statements of changes in social insurance amounts for the periods January 1, 2012 to January 1, 2013 and January 1, 2011 to January 1, 2012. The statement of social insurance as of January 1, 2009 was audited by other auditors whose reports dated November 9, 2009 expressed an unmodified opinion on those statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.



Auditor's Responsibility

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 Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 14-02 requires that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Opinion

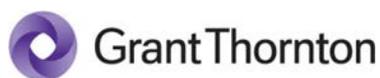
In our opinion, the financial statements referred to above and presented on pages 40 through 74 of this Agency Financial Report (AFR), present fairly, in all material respects, the financial position of SSA as of September 30, 2013 and 2012, its net cost of operations, changes in net position, and budgetary resources for the years then ended, the financial condition of its social insurance program as of January 1, 2013, January 1, 2012, January 1, 2011, and January 1, 2010 and changes in social insurance amounts for the period January 1, 2012 to January 1, 2013 and January 1, 2011 to January 1, 2012, in conformity with accounting principles generally accepted in the United States of America.

As discussed in Note 17 to the financial statements, the statements of social insurance present the actuarial present value of 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 MANagements ASSERTION ABOUT THE EFFECTIVENESS OF INTERNAL CONTROL

We have examined managements assertion as of September 30, 2013, based on criteria established under 31 U.S.C. 3512(c), (d), the *Federal Managers' Financial Integrity Act of 1982* (FMFIA), and the 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 FMFIA. SSA's management is responsible for maintaining effective internal control over financial reporting and for its assertion of the effectiveness of internal control over financial reporting included in the accompanying FMFIA Assurance Statement on page 31 of this AFR. Our responsibility is to express an opinion on managements assertion based on our examination.

We conducted our examination in accordance with attestation standards established by the AICPA; and internal control audit requirements included in OMB Bulletin No. 14-02. Attestation standards require that we plan and perform the examination to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our examination 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 examination provides a reasonable basis for our opinion.

An Agency's internal control over financial reporting is a process affected 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.

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 a 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. No deficiencies in internal control were identified that were considered material weaknesses. However, material weakness may exist that have not been identified.

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. We identified certain deficiencies that, in the aggregate, are considered a significant deficiency in the areas of Information Systems Controls and Controls over Calculation, Recording and Prevention of Overpayments.

SIGNIFICANT DEFICIENCY - INFORMATION SYSTEMS CONTROLS

SSA's business processes which generate the information included in financial statements are dependent upon the Agency's information systems. A comprehensive and effective internal control program over these systems is paramount to the reliability, integrity, and confidentiality of data while mitigating the risk of errors, fraud, and other illegal acts.

Overview

Management relies extensively on information systems operations for the administration and processing of the Title II and Title XVI programs, to both process and account for their expenditures, as well as for financial reporting. Internal controls over these environments are essential for the reliability, integrity, and confidentiality of the program's data and mitigate the risks of error, fraud and other illegal acts.

Our internal control testing covered both general and application controls. General Controls encompass the entity-wide security program (EWSP), access controls (physical and logical), configuration and change management, segregation of duties, and service continuity/contingency planning. General controls provide the foundation for the integrity of systems including applications and the system software which make up the general



support systems of the major applications. General controls, combined with application level controls, are critical to ensure accurate and complete processing of transactions and integrity of stored data. Application controls include controls over input, processing of data, and output of data as well as interface, master file, and other user controls. These controls provide assurance over the completeness, accuracy, and validity of data. Our examination included testing of the Agency's mainframe, networks, databases, applications, and other supporting systems and was conducted at headquarters, as well as, off-site locations such as Disability Determination Services (DDS) Centers and field offices (FOs).

Deficiencies Noted in Information Systems

SSA made significant progress in strengthening controls over its information systems to address the material weakness reported in FY 2012. In response to the material weakness SSA developed functional remediation teams to investigate issues, identify root causes, and implement corrective actions. Each functional remediation team, with oversight from SSA leadership, took risk-based approaches to remediation—addressing higher risk areas immediately, and planning for future security enhancements. Management's risk based approach included correction of vulnerabilities identified through our specific tests, as well as, development and implementation of institutionalized and repeatable processes to prevent future weaknesses.

While SSA made these significant efforts to strengthen controls over its systems and address weaknesses, our FY 2013 testing continues to identify control issues in both design and operation of key controls. We believe that in many cases these deficiencies continue to exist because of one or a combination of the following:

- Control enhancements and newly designed controls require additional time to effectuate throughout the environment;
- By focusing resources on higher risk weaknesses, SSA was unable to implement corrective action for all aspects of the prior year issues; and/or
- The design and/or operational effectiveness of enhanced or newly designed controls did not completely address risks.

We noted deficiencies in the following areas that contribute to the significant deficiency:

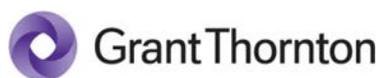
- Threat Identification and Vulnerability Management
- Change Management
- Mainframe Security
- Access Controls/Segregation of Duties

Threat Identification and Vulnerability Management

Software should be scanned and updated frequently to guard against security threats. Effective vulnerability and patch management as well as virus protection programs ensure that security threats are identified, risks are assessed, and actions are taken to prevent inappropriate access or software errors within an organization's Information Technology environment. Our testing identified the following issue:

- *Lack of a comprehensive Agency-wide policy and procedures related to vulnerability management, including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure/validation.*

During our internal penetration testing we were able to take advantage of software vulnerabilities, misconfigurations, and restricted information and ultimately assume control over two servers, the Windows domain, as well as, gaining access to the mainframe without detection. This is the third successive year we have gained control of the SSA Windows system without detection. During subsequent assessments of the



Agency's overall vulnerability management process, we noted that a key scanning tool was not being fully used to identify vulnerabilities across SSA's network, and that Agency-wide comprehensive policies and procedures on vulnerability management were not established.

The Agency corrected the specific software vulnerabilities identified during our penetration testing, developed configuration standards for the software, and began using more capabilities of the scanning tool. However, without a comprehensive process in place, security threats may not be appropriately prioritized and remediated.

Change Management

Change management processes provide assurance that software, data, and other changes associated with information systems are approved and tested so they do not introduce functional or security risks. A disciplined process for testing, approving, and migrating changes between environments, including into production, is essential to ensure that systems operate as intended and that no unauthorized changes are implemented. Our testing identified the following issue:

- *Lack of comprehensive Agency-wide policy and procedures related to management of application and system software changes, including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk and requirements for the review and approval of testing results.*

While our testing demonstrated that change management activities were occurring for both application and system software changes, the Agency had not fully documented a comprehensive policy and procedures covering the entirety of change management processes conducted by the Agency. Our testing noted the following:

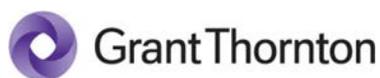
- System Software - An impact/risk assessment to determine the security implications for mainframe changes did not occur. Further, for the majority of changes tested, we noted that developers were responsible for testing their own changes and implementing these changes into production. While Management performed a review to validate that updates made were associated with an approved change, there were no requirements nor guidance related to the types of testing to be performed (including security reviews), nor for retention or independent review of testing documentation, nor validation that the change made was limited to the requirements in the approved change ticket.
- Application Changes - We noted instances where evidence to support testing and other requirements could not be provided.

These issues increase the risk that changes to applications and supporting system software, that may impact benefit claim processing, payments, or financial data, do not function as intended or introduce security risks.

Mainframe Security

Mainframe system software includes programs that are essential to the effective functioning of the operating system. Some of these programs act as an extension of the operating system and therefore are required to access restricted functions and can override security. Maintaining an authorized listing of high risk programs and implementing appropriate change and monitoring controls is essential to mainframe security. Our testing identified the following issue:

- *Lack of controls related to the identification and monitoring of high-risk programs operating on the mainframe.*



The Agency had not finalized and fully implemented controls associated with ensuring that privileged programs have been approved, can only be modified appropriately, and pose no security risks. Management continues to make control enhancements, including but not limited to, identifying privileged programs, the review of privileged programs from a security perspective, access restrictions to all privileged programs, and change/monitoring control enhancements.

Without appropriate controls, there is an increased risk that the security posture and controls may be bypassed or compromised.

Access Controls/Segregation of Duties

Access controls provide assurance that critical systems assets are physically safeguarded and that logical access to sensitive applications, system utilities, and data is provided only when authorized and appropriate. These controls mitigate the inherent risk that unauthorized users and computer processes cannot access sensitive data, as well as, that users are not given access to system functions that could create a segregation of duties conflict. Weaknesses in such controls can compromise the integrity of sensitive data and increase the risk that such data may be inappropriately accessed and/or disclosed. Our testing identified the following issues with logical access controls:

- *Access Authorization*

Our testing identified control failures related to the appropriate completion of authorization forms. Included in these control failures were instances of new hires, transferred employees, and contractors.

- *Access Removal*

Our testing identified control failures related to the timely removal of logical access for terminated employees' logical access to the mainframe, network, and other supporting systems. Included in these control failures were instances of SSA employees and state DDS employees who retained access after they were terminated. Additionally, SSA did not have an authoritative source to identify and manage all contractors and therefore was unable to supply actual departure dates for contractors to substantiate timely removal of access.

- *Profile Content and Analysis Review Program and Supporting Profile Controls*

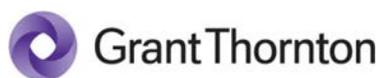
SSA Management continues to make progress in assessing profile content to validate that profiles only provide access to the minimal resources required for users to complete job functions. However, SSA had not completed the review of all profiles that are relevant to critical applications and supporting systems nor had SSA completed other profile quality initiatives including, but not limited to, some control enhancements.

As a result of these deficiencies, we noted numerous issues of unauthorized and inappropriate access including application developers (programmers) with unmonitored access to production data and application transactions, access to key transactions and data, key change management libraries, and other sensitive system software resources.

Recommendations

In order to mitigate the risks of the issues noted in the significant deficiency, management should consider:

- Formally documenting comprehensive policies and procedures related to (1) threat identification and vulnerability management and (2) application and system software change management that addresses issues noted.



- Developing a comprehensive program to identify and monitor high risk programs operating on the mainframe.
- Analyzing current access authorization and removal processes to determine if current controls mitigate the risk of unauthorized access and modify controls considering automation and monitoring.
- Continuing, as part of the SSA profile quality program, additional profile content reviews and other key profile improvement initiatives.

SIGNIFICANT DEFICIENCY - CALCULATION, RECORDING AND PREVENTION OF OVERPAYMENTS

Overview

Benefit overpayments occur when beneficiaries receive payments beyond their entitled amount. Upon detection of an overpayment, the agency records an accounts receivable with the public to reflect the amount due to SSA from the beneficiary. Due to the nature of the benefit payment programs, SSA has extensive operations geographically dispersed throughout the United States. Overpayment detection, calculation, and documentation can take place in various places, including approximately 1,300 Field Offices (FOs) or eight Program Service Centers (PSCs). Therefore, SSA has specific policies and procedures in place to ensure consistent treatment and documentation of overpayments and the related accounts receivable balances. Since this process can be complex for some cases and relies heavily on manual input, SSA's adherence to its policies and procedures is critical to correct and timely decisions, and accurately tracking balances. Management also relies heavily on its Information Technology infrastructure, interfaces and controls to record and prevent erroneous payments.

Deficiencies in Overpayment Calculations and Records

Similar to prior years, Grant Thornton noted deficiencies in the documentation maintained around overpayments. During the current year, we selected a statistical sample of overpayments and noted overpayment calculation errors with 38 percent of the items selected. Although the impact of these errors is not deemed material, these errors evidence further control weaknesses in the overpayment process, including inappropriate overpayment tracking.

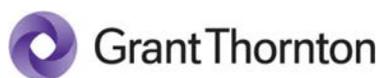
Deficiencies in Overpayment Records and Tracking

Large overpayment balances are often paid back to SSA in monthly installments. Payments of these installments can go beyond the year 2049. SSA has identified a systems limitation where receivable installments extending past 2049 are not tracked and reported systematically. Therefore, the accounts receivable balances related to these overpayments is understated. The projected understatements are immaterial. This issue has been previously discussed in Government Accountability Office (GAO) reports and continues to be studied by the agency.

During our testing of overpayments, we encountered samples where the 2049 situation contributed to manual errors. While the agency is working on enhancing the capabilities to properly account for these receivables and updating policies to avoid longer term repayment programs, failure to resolve the 2049 issue will continue to increase the likelihood of manual errors as well as continue to understate accounts receivable balances.

Deficiencies in Overpayment Prevention

During our Computer Assisted Auditing Techniques (CAATs), we identified certain key data fields, such as Date of Death, which did not agree between SSA internal databases. As a result, our testing detected overpayments issued to a limited number of deceased individuals. While these cases were clearly immaterial to SSA financial statements, they were indicative of a control failure where SSA was not reconciling data between systems to detect discrepancies which could lead to payment errors. While overpayments occur for many reasons, SSA should take all possible actions under their control to prevent and detect overpayments. Failure to detect overpayments results in continued erroneous benefit payments and unrecorded corresponding accounts receivable. The longer an



overpayment goes undetected, the greater the overpayment balance becomes and the lower the chance of accounts receivable collections.

Recommendations

In order to mitigate the risks of the issues noted in the significant deficiency, management should consider:

Deficiencies in Overpayment Calculations and Records

- Performing a risk based analysis on current overpayment balances to detect and correct errors in existing overpayment balances, considering manual intervention, balance, and age.
- Enhancing documentation requirements and improve overpayment documentation tools to ensure overpayments are completely, accurately, and timely documented by FOs or PSCs within the appropriate systems of record.
- Increasing management review over manual transactions impacting overpayment balances.

Deficiencies in Overpayment Records and Tracking

- Evaluating technical enhancements that will address payment plans that extend beyond the year 2049.
- Evaluating changes in repayment plans to minimize future long term repayment plans.

Deficiencies in Overpayment Prevention

- Enhancing periodic reconciliations between SSA data which can impact payment amounts.

In our opinion, management's assertion that SSA maintained effective internal control over financial reporting as of September 30, 2013 is fairly stated, in all material respects, based on criteria established under FMFIA and OMB Circular No. A-123.

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 basic financial statements are free of material misstatement, we performed tests of 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. 14-02, 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 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 test 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. 14-02, and no instances of substantial noncompliance that are required to be reported under FFMIA.



Other Matters

The Management's Discussion and Analysis (MD&A) included on pages 5 through 36, and the Required Supplementary Information (RSI) included on pages 75 and 81 through 92 of this AFR are not a required part of the basic financial statements but are supplementary information required by the Federal Accounting Standards Advisory Board and OMB Circular A-136, *Financial Reporting Requirements*. This required supplementary information is the responsibility of management. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America established by the AICPA. These limited procedures consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

The other information included on pages 1 through 4, 37 through 39, 76 through 80, 93 through 95 and 105 to the end of this AFR, is presented for purposes of additional analysis and is not a required part of the basic financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the basic 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.

A handwritten signature in black ink that reads "Grant Thornton LLP".

Alexandria, Virginia
December 9, 2013



SOCIAL SECURITY

The Commissioner

December 9, 2013

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 (FY) 2013 financial statements. We are extremely pleased that we received our 20th consecutive unmodified opinion on our financial statements, an unmodified opinion on management's assertion that our internal controls were operating effectively, and a finding that there were no reportable instances of noncompliance with laws or regulations.

Your report acknowledged our significant progress in strengthening controls over our information systems to address the material weakness reported in FY 2012. While we made significant progress strengthening controls over our systems and addressing the previously identified weaknesses, you identified control issues in both the design and operation of key controls, resulting in a significant deficiency in information systems controls. We concur with your recommendations and remain committed to the continuous enhancement of our internal controls over information systems. We will continue to pursue a risk-based corrective action plan to address threat identification and vulnerability management, change management, mainframe security, and access controls/segregation of duties.

Your report also identified certain deficiencies related to the calculation, recording, and prevention of overpayments that, when aggregated, you considered a significant deficiency. We acknowledge the need to strengthen our controls in the overpayment process and will implement the necessary corrective actions.

We have enclosed a more detailed explanation of our plans.

If members of your staff have any questions, they may contact Carla Krabbe, our Associate Commissioner for Financial Policy and Operations, at (410) 965-0759.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

Enclosure

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) 2013 financial statements.

We are pleased that your report makes note of our significant progress in strengthening controls over our information systems to address the prior year material weakness. As we did in FY 2013, we will continue to strengthen our security program by remediating and institutionalizing the new processes that we put in place, making risk-based decisions, continuing to leverage current agency processes, and adding layers of defense to our current security program.

Your report also identified certain deficiencies related to the calculation, recording, and prevention of overpayments. We acknowledge the need to strengthen our controls in the overpayment process and will implement the necessary corrective actions to calculate, record, track, and prevent overpayments.

We offer the following comments.

Significant Deficiency - Information Systems Controls

Recommendation 1

Formally document comprehensive policies and procedures related to (1) threat identification and vulnerability management and (2) application and system software change management that address issues noted during the audit.

Comment

We agree with this recommendation. In FY 2013, we instituted a new daily penetration testing program related to threat identification and vulnerability management. Our goal in FY 2014 is to continue to mature this program. We have begun integrating the processes that have worked effectively and are analyzing the requirements in prioritizing vulnerabilities for a comprehensive end-to-end process. Remediation of any additional vulnerability found will be effectuated through the current and continually improving process. We have already increased the types of vulnerabilities we identify. In addition, analysis is underway to prioritize vulnerabilities. Not only have we made significant improvements in this area in a relatively short time, we believe the gaps have decreased and the real need now is to highlight individually where components of the end-to-end process can gain efficiency.

We also agree with this recommendation to formally document our change management process. As with FY 2013, we continue to investigate improving risk categorization along with required testing for system software changes that could cause a significant outage or security risk. We are working to define the different levels of controls required based on the change. We agree that we need to add consistency as our process matures. We also plan to further assess risk and document as necessary.

Enclosure – Page 2 – Grant Thornton LLP

Recommendation 2

Develop a comprehensive program to identify and monitor high risk programs operating on the mainframe.

Comment

We agree with this recommendation. We will continue to improve management of privileged programs in FY 2014. We are also considering the possibility of a manual review of privileged programs, in addition to an automated scanning and review of privileged programs. As we continue to improve in this area, we are taking a risk-based approach to address the highest-level risk first.

Recommendation 3

Analyze current access authorization and removal processes to determine if current controls mitigate the risk of unauthorized access and modify controls considering automation and monitoring.

Comment

We agree with this recommendation. In FY 2014, we will implement an electronic process to grant access. We are also working on a fully automated process to grant access, which will help mitigate the control failures in access authorization.

Our goal is to automate access control changes wherever possible. In FY 2014, we will analyze new tools for managers to facilitate easy, continuous monitoring of staff's access. In addition, we are reviewing separation procedures and training for opportunities to improve performance in this area.

Recommendation 4

Continue, as part of the SSA profile quality program, additional profile content reviews and other key profile improvement initiatives.

Comment

We agree with this recommendation. We took a risk-based approach to perform the profile content review in FY 2013. To date, we have completed 4 campaigns, with the remaining campaigns scheduled for completion in early 2015. The remaining campaigns will include profiles with access related to Critical Infrastructure Protection Plan and Financially Significant Systems, focusing on higher-risk profiles first.

In addition, we are concurrently performing the Profile Quality Program, which includes several projects with the common goal of maintaining access profiles that allow only approved access to the minimum resources required. The Profile Quality Program includes the following:

- Elimination of obsolete/unused profiles;
- Enforcement of profile naming standards;
- Profile lifecycle and Change Management process enhancements; and
- Resource classification and enhanced controls.

Enclosure – Page 3 – Grant Thornton LLP

Significant Deficiency - Calculation, Recording, and Prevention of Overpayments

Deficiencies in Overpayment Calculations and Records

General Comment

To improve quality in overpayment workloads, we are implementing a regional Continuous Quality Initiative at field offices (FO) and payment service centers (PSC). We expect to implement this initiative nationwide by February 2014.

Recommendation 1

Performing a risk based analysis on current overpayment balances to detect and correct errors in existing overpayment balances, considering manual intervention, balance, and age.

Comment

We agree with this recommendation. We will explore options for instituting a risk-based approach to detect and correct overpayment errors.

Recommendation 2

Enhancing documentation requirements and improve overpayment documentation tools to ensure overpayments are completely, accurately, and timely documented by FOs or PSCs within the appropriate systems of record.

Comment

We agree with this recommendation. Through our Continuous Quality Initiative, we will address overpayment documentation issues and improve overpayment documentation tools, where feasible, to ensure FOs and PSCs completely, accurately, and timely document overpayments.

Recommendation 3

Increasing management review over manual transactions impacting overpayment balances.

Comment

We agree with this recommendation. Through our Continuous Quality Initiative, we will perform additional reviews of overpayments both in FOs and in the PSCs.

Deficiencies in Overpayment Records and Tracking

General Comment

In July 2011, a Government Accountability Office audit identified a Title II system limitation concerning long-term withholding agreements that extend past the year 2049. The system limitation prevents us from tracking the post- 2049 debt. This limitation requires operational, financial, information technology (IT), and policy solutions throughout our agency.

As a short-term solution, we issued updated guidance in August 2012 to address the 2049 situation. This guidance provides a uniform process for FOs to address newly established overpayments that would trigger a 2049 situation.

Enclosure – Page 4 – Grant Thornton LLP

We continue to explore a strategic approach for multiple long-term solutions, which may include changes to our systems, policies, and procedures.

Recommendation 1

Evaluating technical enhancements that will address payment plans that extend beyond the year 2049.

Comment

We agree with the recommendation. In FY 2013, we evaluated the cost and timeframe for changing our systems to address the 2049 limitation. The cost in IT resources exceeded what we had available; therefore, the proposal did not move forward in light of competing priorities. We continue to explore for a long-term solution.

Recommendation 2

Evaluating changes in repayment plans to minimize future long term repayment plans.

Comment

We agree with this recommendation. In an effort to minimize future long-term repayment plans, we are increasing our recovery efforts to include a minimum of 10 percent of the monthly benefit amount, rather than a \$10 minimum, through a notice of proposed rulemaking. We are pursuing additional options to mitigate this issue.

Deficiencies in Overpayment Prevention

Recommendation 1

Enhancing periodic reconciliations between SSA data which can impact payment amounts.

Comment

We agree with this recommendation. We recently implemented a new monthly death match process and are working on a Death Process Redesign project to streamline the reconciliation processes.

This page was intentionally left blank.