AUDITOR'S REPORTS

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

November 9, 2015

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 (Grant Thornton) an independent certified public accounting firm, audited SSA's Fiscal Year (FY) 2015 financial statements. Grant Thornton also audited the FY 2014 financial statements presented in SSA's FY 2015 Agency Financial Report for comparative purposes. This letter transmits the Grant Thornton *Independent Auditor's Report* on the audit of SSA's FY 2015 financial statements. Grant Thornton'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 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. 15-02, *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 in 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 issued an unmodified opinion on SSA's FY 2015 and 2014 financial statements. Grant Thornton also reported that SSA was maintaining effective internal control over financial reporting as of September 30, 2015 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 did identify three significant deficiencies in internal controls.

Significant Deficiency – Information Systems Control

It is Grant Thornton's opinion that SSA made progress in strengthening controls over its information systems to address the significant deficiency reported in FY 2014. While SSA continued executing its risk-based approach to strengthen controls over its systems and address weaknesses, Grant Thornton's FY 2015 testing identified similar control issues in both design and operation of key controls. Grant Thornton identified information systems control deficiencies that, when aggregated, are considered to be a significant deficiency in the area of Information Systems Controls. Specifically, Grant Thornton's testing disclosed the following.

1. Weaknesses with cyber/network security controls during testing of threat and vulnerability management processes.
2. Recurring issues during site visits associated with security management, physical and logical access controls, and platform security. Further, it noted areas where SSA's requirements and guidance were ambiguous and not sufficiently documented, resulting in noncompliance or inconsistent implementation with SSA policy. Finally, it noted a lack of oversight for decentralized information systems and locations, inconsistent implementation of SSA information technology control requirements associated with system development and a lack of risk management activities, including but not limited to, security assessment and authorization processes in the regions and disability determination services.
3. While SSA made progress in addressing the FY 2014 significant deficiency, a lack of comprehensive Agency-wide policy and procedures related to management of application and system software changes, many procedures related to management of application and system software changes were still in development and had not been effectuated through SSA's central office and regions. Grant Thornton continued to note that SSA's systems software change processes did not require security categorization and risk analysis for changes, testing requirements based on risk, and requirements for the review and approval of testing results.
4. Weaknesses in logical access controls, such as access authorization, access removal, profile content, and analysis review program and supporting profile controls, as well as, numerous issues of unauthorized and inappropriate access.

Significant Deficiency – Calculation, Recording, and Prevention of Overpayments

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

1. control weaknesses over overpayment documentation and overpayment calculation errors with 24 percent of items selected in its statistical sample, which lead to difficulties in substantiating accounts receivable balances;

2. system limitations where overpayment receivable installment payments extending beyond year 2049 were not systematically tracked and reported; and
3. control failures where SSA was not reconciling key data fields between SSA internal databases, resulting in overpayment errors.

Significant Deficiency – Redeterminations

Finally, Grant Thornton identified deficiencies in internal control that, when aggregated, are considered to be a significant deficiency related to weaknesses in internal controls related to redeterminations. Specifically, Grant Thornton's testing disclosed instances where redetermination interviewers did not comply with established control policies, and results were not appropriately recorded.

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

OIG Evaluation of Grant Thornton 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 2015 financial statements by

- reviewing Grant Thornton's audit approach and planning;
- evaluating its auditors' qualifications and independence;
- monitoring the audit's progress at key points;
- examining Grant Thornton's documentation 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. 15-02;
- coordinating the issuance of the audit report; and
- performing other procedures we deemed necessary.

Grant Thornton is responsible for the attached auditor's report, dated November 9, 2015 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.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of this report to 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

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, 2015 and 2014, 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, 2015, January 1, 2014, January 1, 2013, January 1, 2012, and January 1, 2011 and the statements of changes in social insurance amounts for the periods January 1, 2014 to January 1, 2015 and January 1, 2013 to January 1, 2014 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, 2015;
- No instances of substantial noncompliance with the requirements of the Federal Financial Management Improvement Act of 1996 (FFMIA); and
- No reportable instances of noncompliance with laws, regulations, contracts, grant agreements 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 financial statements of SSA, which comprise the consolidated balance sheets as of September 30, 2015 and 2014 and 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, 2015, January 1, 2014, January 1, 2013, January 1, 2012, and January 1, 2011 and the statements of changes in social insurance amounts for the periods January 1, 2014 to January 1, 2015 and January 1, 2013 to January 1, 2014 and the related notes to the financial 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. 15-02, *Audit Requirements for Federal Financial Statements.* Those standards and OMB Bulletin No. 15-02 require 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 50 through 87 of this Agency Financial Report (AFR) present fairly, in all material respects, the financial position of SSA as of September 30, 2015 and 2014, 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, 2015, January 1, 2014, January 1, 2013, January 1, 2012, and January 1, 2011 and changes in social insurance amounts for the periods January 1, 2014 to January 1, 2015 and January 1, 2013 to January 1, 2014, in accordance with accounting principles generally accepted in the United States of America.

Emphasis of Matter

As discussed in Note 18 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 MANAGEMENT'S ASSERTION ABOUT THE EFFECTIVENESS OF INTERNAL CONTROL

We have examined management's assertion included on page 40 of this AFR, that SSA maintained effective internal control over financial reporting as of September 30, 2015, 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 40 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 American Institute of Certified Public Accountants (AICPA); *Government Auditing Standards*, issued by the Comptroller General of the United States; and internal control audit requirements included in OMB Bulletin No. 15-02. 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 or significant deficiency 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 weaknesses 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 significant deficiencies in the areas of Information Systems Controls and Calculation, Recording and Prevention of Overpayments and Redeterminations.

SIGNIFICANT DEFICIENCY - INFORMATION SYSTEMS CONTROLS

Overview

Management relies extensively on information systems 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 and integrity of the program's data and mitigate the risks of misstatements whether due to fraud or error.

Our internal control testing covered both general and application controls. General controls encompass the security management program, 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 for 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 audit 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.

Deficiencies Noted in Information Systems

SSA continues to make progress in strengthening controls over its information systems to address the significant deficiency reported in Fiscal Year (FY) 2014. In response to continued control weaknesses, SSA's functional remediation teams continue to implement risk based corrective actions, which, in many cases, is a continuation of ongoing remedial efforts from past years. Management's planned risk based approach included correction of weaknesses identified through our specific tests, as well as, development and implementation of institutionalized and repeatable processes to prevent future weaknesses.

While SSA continued executing its risk-based approach to strengthen controls over its systems and address weaknesses, our FY 2015 testing identified similar 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:

- Risk mitigation strategies and related control enhancements require additional time to be fully implemented or to effectuate throughout the environment.
- SSA focused its resources on higher risk weaknesses and therefore was unable to implement corrective action for all aspects of the prior year deficiencies.
- The design of enhanced or newly designed controls did not completely address risks and recommendations provided over past audits.
- Oversight and governance were not sufficient to address deficiencies.

We noted deficiencies that contribute to the significant deficiency in the areas of threat and vulnerability management, information technology (IT) oversight and governance, change management, and access controls.

Threat and Vulnerability Management

Configuration, vulnerability, and patch management processes are critical components of an effective cyber security strategy. These processes and related controls that prevent or detect weaknesses such as misconfigurations, weak credentials, and vulnerabilities are essential in combating internal and external cyber threats, exploitations, and unauthorized access. Our information security and penetration testing, vulnerability management, and configuration management assessments identified control weaknesses with cyber/network security controls, many of which continue to exist from past audits. Specific disclosure of detailed information about these weaknesses might further compromise controls and are therefore not provided within this report. Rather, the specific details are presented in a separate, limited-distribution management letter.

IT Oversight and Governance

Appropriate IT governance and oversight provides assurance that risks are identified and assessed, controls are appropriately designed, and are operating effectively across the Agency's information systems and locations. Through the Agency's security management program, SSA's risk management framework must include a continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures. We noted as part of our field testing that issues continued to persist from past audits due to limited remediation in the current FY associated with past weaknesses. Specifically,

recurring issues continue to be cited associated with security management, physical and logical access controls, and platform security. Further, there are areas where SSA's requirements and guidance was ambiguous and/or not sufficiently documented, which resulted in inconsistent implementation or noncompliance with SSA policy. Finally, we noted a lack of oversight for decentralized information systems and locations, inconsistent implementation of SSA IT control requirements associated with system development, and a lack of risk management activities, including but not limited to, security assessment and authorization (SA&A) processes in the regions and disability determination services (DDS).

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. SSA implemented a change management directive in FY 2015 which documented control objectives and requirements for centralized and decentralized applications developed by SSA. However, many procedures designed to support the directive were still in development and the directive had not effectuated through SSA's central office and regions. In addition, we continue to note that SSA's system software change processes did not require security categorization and risk analysis for all changes, testing requirements based on risk, and requirements for the review and approval of testing results.

Access Controls

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. 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 control failures related to appropriate completion of logical access authorization forms and timely removal of location access. Further, we continue to note that 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. Finally, we noted that SSA management continued 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, control enhancements. As a result of these deficiencies, we noted numerous issues of unauthorized and inappropriate access including application developers (programmers) who had unmonitored access to production data and application transactions, 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 the following:

- Address specific weaknesses noted in information security and penetration testing, as well as, vulnerability/configuration management assessments. In addition, SSA should continue, as part of the SSA threat and vulnerability management processes, prioritization and implementation of risk mitigation strategies and plans of action and milestones.
- Enhance current information technology oversight and governance processes to ensure SSA information technology risk management requirements, as they apply to SSA systems, cloud systems, and contractor systems, are effectively and consistently implemented across the organization.

- Develop comprehensive policies and procedures related to application and system-software change management that address issues noted during the audit.
- Analyze account management controls including access authorization, recertification, and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and oversight of processes.
- Continue, as part of the Cyber Sprint initiative, to improve controls over privileged accounts.
- Continue, as part of the SSA profile quality program, additional profile content reviews and 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 SSA records an accounts receivable with the public to reflect the amount due to SSA from the beneficiary. Because of 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 1,200 Field Offices (FOs) or eight Processing Centers (PCs). 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 IT infrastructure, interfaces and controls to record and prevent erroneous payments.

Deficiencies in Overpayment Calculations and Records

During FY 2015, the Agency implemented a new Continuous Quality Review (CQR) control in all of its regions to remediate findings noted in the prior year over the calculation and recording of overpayments. However, despite the addition of the CQR control, Grant Thornton continued to note control deficiencies in the documentation maintained around overpayments, due to manual errors and failure to properly retain documents. Insufficient documentation to support overpayments can lead to difficulties in calculating and substantiating outstanding accounts receivable balances. In addition, we selected a statistical sample of overpayments and noted overpayment calculation errors with 24 percent of the items selected. Although the impact of these calculation errors is not deemed material to the financial statements, these errors evidence control weaknesses in the accounts receivable process, including inappropriate overpayment tracking that could lead to misstatements in the financial statements.

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 the Year 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 SSA.

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 Year 2049 issue will continue to increase the likelihood of errors due to the manual process of tracking this debt, as well as continue to understate accounts receivable balances.

Deficiencies in Overpayment Prevention

While conducting Computer Assisted Auditing Techniques (CAATs), we continued to identify certain key data fields, such as Date of Death, which did not agree between SSA internal databases (master files). As a result, our testing detected overpayments issued to a limited number of individuals who were not entitled to benefits. While these cases were clearly immaterial to SSA financial statements, they were indicative of a control failure where SSA's data reconciliations were not operating effectively and/or potential discrepancies were not acted upon in a timely fashion in order to detect and prevent overpayment errors. While overpayments occur for many reasons, SSA should take all possible actions under their control to prevent and detect such payments. 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 while the probability of accounts receivable collection decreases. This finding continues to recur and we note CAATs routines performed in prior years continue find the same exceptions in the current year, indicating the agency is not timely detecting overpayments.

Recommendations

To mitigate the risks of the issues noted in the significant deficiency, management should consider the following:

Deficiencies in Overpayment Calculations and Records

- Continue evaluating current overpayment balances, based on a risk based approach, to detect and correct errors in existing overpayment balances, considering manual intervention, balance, and age. Consider analyzing debt outstanding for individuals with a Date of Death on any SSA system.
- Enhancing documentation requirements and improve overpayment documentation tools to ensure overpayments are completely, accurately, and timely documented by FOs or Processing Centers (PCs) within the appropriate systems of record.
- Continue to increase management review over manual transactions impacting overpayment balances, including CQ Reviews and PC Inline Reviews.

Deficiencies in Overpayment Records and Tracking

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

Deficiencies in Overpayment Prevention

- Continue enhancing periodic reconciliations between SSA data which can impact payment amounts in order to detect and act on overpayments more timely.

SIGNIFICANT DEFICIENCY – REDETERMINATIONS

As the Supplemental Security Income (SSI) Program is a needs based program, beneficiaries' payments amounts can change based on numerous factors such as income, assets and living situations. SSA requires its SSI beneficiaries to undergo periodic reviews of their benefit payment amount considering these factors. Claims representatives in the field office perform this process during a redetermination interview. In order to ensure consistent processing of redeterminations across the approximately 1,200 field offices, SSA has detailed policies and procedures as well as an internal control system related to the completion of redeterminations, which rely heavily on human input by the claims representatives.

We observed redetermination interviews in process and noted several instances where the interview did not comply with established control policies due to claims representative manual errors. In the interviews where we noted exceptions, the unanswered questions or responses recorded incorrectly could lead to changes in benefit payment amounts.

In addition, we selected a sample of completed redeterminations and noted deficiencies in the documentation of the redetermination. Failure to perform and document redeterminations in accordance with established policies could result in benefit overpayments, including payment to ineligible individuals and the potential inability to support benefit payment amounts.

Recommendations

To mitigate the risks of the issues noted in the significant deficiency, management should consider the following:

- Enhance training and reminders to claims representatives completing redeterminations in the field offices to ensure that all applicable questions in the redetermination application are answered.
- Increase the frequency and scope of management review over redetermination interviews.
- Establish and enforce procedures to ensure that claims representatives encourage beneficiaries to do a thorough review of the redetermination input data.

In our opinion, management's assertion that SSA maintained effective internal control over financial reporting as of September 30, 2015 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, regulations, contracts, and grant agreements, if applicable. As part of obtaining reasonable assurance about whether the basic financial statements are free of material misstatement, we performed tests of compliance with laws, regulations, contracts, and grant agreements, including laws governing the use of budgetary authority, government-wide policies and other laws and regulations, noncompliance with which could have a direct and material effect on the financial statements. Under 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 regulations and contracts applicable to SSA. We limited our tests of compliance to the provisions of laws, regulations and contracts 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, regulations and contracts, or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 15-02, and no instances of substantial noncompliance that are required to be reported under FFMIA.

Other Matters

The Management's Discussion and Analysis (MD&A) and the Schedule of Budgetary Resources included on pages 6 through 44 and page 94, respectively, and the Required Supplementary Information (RSI) included on pages 95 through 106 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.

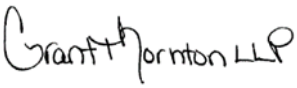
Agency's Responses to Findings

The Agency's responses to the findings identified in our audit and presented on pages 119 through 124 of this AFR were not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the responses.

Other Information

The Acting Commissioner's Message on page 1 and the other information included on pages 2 through 5, 47 through 49, 88 through 93, 125 through 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.



Alexandria, Virginia
November 9, 2015

SOCIAL SECURITY

The Commissioner

November 9, 2015

Grant Thornton LLP
333 John Carlyle St.
Alexandria, VA 22314

Ladies and Gentlemen:

We have reviewed the draft Independent Auditor's Report concerning your audit of our fiscal year (FY) 2015 financial statements. We are extremely pleased that we received our 22nd consecutive unmodified opinion on our financial statements, an unmodified opinion on management's assertion that our internal controls over financial reporting were operating effectively, and that we had no reportable instances of noncompliance with laws, regulations, or other matters tested.

We are pleased that you acknowledged our progress in strengthening controls over our information systems to address the significant deficiency reported in FY 2014. While we made significant progress to strengthen controls over our systems and to address 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 and vulnerability management, information technology oversight and governance, change management, and access controls.

Your report 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 overpayment controls. We will continue to implement the necessary risk-based corrective actions to calculate, record, track, and prevent overpayments. This fiscal year, your report also identified exceptions related to redetermination interviews and documentation that, when aggregated, you considered a significant deficiency. We acknowledge the importance in performing and documenting redeterminations in accordance with established policies and procedures. We will implement the necessary risk-based corrective actions to ensure consistent processing of redeterminations.

We have enclosed a more detailed explanation of our plans. If members of your staff have any questions, they may contact Carla Krabbe at (410) 965-0759.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Enclosure – Page 1 – Grant Thornton LLP

Comments of the Social Security Administration on Grant Thornton LLP's
Fiscal Year 2015 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) 2015 financial statements.

We are pleased that your report notes our progress in strengthening controls over our information systems to address the prior year significant deficiency. As we did in FY 2015, we will continue to strengthen our security program by remediating and institutionalizing the processes 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 identifies 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 risk-based corrective actions to calculate, record, track, and prevent overpayments.

Your report also identifies exceptions related to redetermination interviews and documentation. We acknowledge the importance in performing and documenting redeterminations in accordance with established policies and procedures. We will explore and implement the necessary risk-based corrective actions to ensure consistent processing of redeterminations.

We offer the following comments.

Significant Deficiency - Information Systems Controls

Recommendation 1 (Threat and Vulnerability Management)

Address specific weaknesses noted in information security and penetration testing, as well as, vulnerability/ configuration management assessments. In addition, SSA should continue, as part of the SSA threat and vulnerability management processes, prioritization and implementation of risk mitigation strategies and plans of action and milestones.

Comment

We agree with this recommendation. In FY 2015, we expanded our penetration testing program to include the analysis of external threats, in addition to internal threats. We successfully implemented new policies and programs to mitigate risks in this area. On October 19, 2015, we implemented a zero tolerance policy for weak credentials as we further refine our threat and vulnerability management program. We continue to emphasize prioritization and implementation of risk mitigation strategies, and plans of action and milestones as we remediate vulnerabilities.

Recommendation 2 (IT Oversight and Governance)

Enhance current information technology oversight and governance processes to ensure SSA information technology risk management requirements, as they apply to SSA systems, cloud systems, and contractor systems, are effectively and consistently implemented across the organization.

Comment

We agree with this recommendation. We continue to improve and standardize processes for information technology (IT) applications developed by non-Deputy Commissioner for Systems components and establish criteria for IT applications subject to Security Assessment and Authorization requirements.

For disability determinations services (DDS), we are accelerating the expansion of the suitability clearance process to identify and strengthen our controls surrounding Homeland Security Presidential Directive 12 suitability clearances for the State DDSs. We are in the process of implementing an automated, standardized DDS Security

Enclosure – Page 2 – Grant Thornton LLP

Plan that includes logs to facilitate the annual review and recertification of physical access to DDS facilities, including sensitive areas such as the computer room. The plan requires annual review and recertification of all parts, including the access logs. The DDS Security Plan also includes logs to facilitate the review of AS/400 security relevant events and command line access of users with privileged access and special authorities.

Regarding cloud systems, we are identifying risks and establishing processes and controls to assess and monitor cloud service providers.

In addition, we are working to ensure that our information security program extends to externally-managed contractor systems operating on our behalf. We continue working to improve current IT oversight and governance processes to ensure our systems comply with appropriate risk management requirements.

Recommendation 3 (Change Management)

Develop comprehensive policies and procedures related to application and system-software change management that address issues noted during the audit.

Comment

We agree with this recommendation. In FY 2015, we developed comprehensive policies and procedures related to application and system software change management. In addition, we placed the *SSA Application Software Release and Configuration Management Directive* into effect as part of a multi-stage approach to documenting comprehensive end-to-end policy and procedures. This comprehensive directive covers the entirety of change management processes and controls we conduct. For FY 2016, we will continue to implement tools, policies, and procedures in support of this directive.

Recommendation 4 (Access Controls)

Analyze account management controls including access authorization, recertification, and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and oversight of processes.

Comment

We agree with this recommendation. In FY 2015, we developed and tested a fully automated process to grant logical access. Scheduled for release in early FY 2016, this fully automated process will help continue to mitigate the control failures in access authorization.

Recommendation 5 (Access Controls)

Continue, as part of the Cyber Sprint initiative, to improve controls over privileged accounts.

Comment

We agree with this recommendation. In FY 2016, we will enhance our current policies and procedures associated with privileged accounts and expand privileged account review efforts across our platforms.

Enclosure – Page 3 – Grant Thornton LLP

Recommendation 6 (Access Controls)

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

Comment

We agree with this recommendation. In FY 2015, we made great progress in implementing least privilege access to financially significant resources. We also expanded our profile content review campaign to include batch profiles and performed systematic clean up to remove latent access. For FY 2016, we plan to finalize and document a strategy to periodically review high priority profiles.

Significant Deficiency - Calculation, Recording, and Prevention of Overpayments

Deficiencies in Overpayment Calculations and Records

Recommendation 1

Continue evaluating current overpayment balances, based on a risk based approach, to detect and correct errors in existing overpayment balances, considering manual intervention, balance, and age. Consider analyzing debt outstanding for individuals with a Date of Death on any SSA system.

Comment

We agree with this recommendation. We continue our efforts to identify and implement effective risk-based approaches to detect and correct overpayment errors. Due to the complexity of these manual transactions, we are exploring the use of data analytic techniques and methods to assist us in targeting the areas to ensure effective use of our resources.

Recommendation 2

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

Comment

We agree with this recommendation. Through our continuous quality initiatives, we will continue to address overpayment documentation issues in our field offices and processing centers. These initiatives will also clarify policies and provide additional targeted training to our employees.

Recommendation 3

Continue to increase management review over manual transactions impacting overpayment balances, including CQ Reviews and PC Inline Reviews.

Comment

We agree with this recommendation. Through our continuous quality initiatives, we will continue to expand our reviews of overpayments in our PCs and enhance our field office review processes to address overpayment accuracy and documentation issues.

Enclosure – Page 4 – Grant Thornton LLP

Deficiencies in Overpayment Records and Tracking

Recommendation 1

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

Comment

We agree with this recommendation. In FY 2015, we established an inter-component workgroup to review and address the recommendations made in the *Repayment Plans that Extend beyond the Year 2049 Final Risk and Impact Assessment Report.*

We have dedicated IT resources to explore the development of a new accounts receivable process. We will ensure that any new processes established will prevent this situation from occurring in the future.

Recommendation 2

Continue pursuing changes in repayment policy to minimize future long-term repayment plans.

Comment

We agree with this recommendation. We have prepared a legislative proposal to revise our minimum benefit withholding from $10 to 10 percent of the monthly Title II benefit payment for new repayment plans. We will work with all parties to expedite this legislative change.

Deficiencies in Overpayment Prevention

Recommendation 1

Continue enhancing periodic reconciliations between SSA data which can impact payment amounts in order to detect and act on overpayments more timely.

Comment

We are exploring the use of data analytic techniques and methods to assist us in identifying and reconciling data anomalies that may affect payment amounts.

Significant Deficiency - Redeterminations

Recommendation 1

Enhance training and reminders to claims representatives completing redeterminations in the field offices to ensure that all applicable questions in the redetermination application are answered.

Comment

We agree with this recommendation. In FY 2015, we issued reminders to our field office employees on the proper processing of redeterminations. We also will enhance training and issue appropriate reminders to claims representatives completing redeterminations by the end of the second quarter of FY 2016.

Enclosure – Page 5 – Grant Thornton LLP

Recommendation 2

Increase the frequency and scope of management review over redetermination interviews.

Comment

We agree with this recommendation. We will explore options for additional management oversight over the redetermination process.

Recommendation 3

Establish and enforce procedures to ensure that claims representatives encourage beneficiaries to do a thorough review of the redetermination input data.

Comment

We agree with this recommendation. We will work to ensure claims representatives encourage beneficiaries to perform a thorough review of the redetermination input data.

We currently afford beneficiaries the opportunity to review and ask questions about the information recorded during the redetermination, and provide a copy of the redetermination as a receipt for their records.

We have two controls in place that address this concern:

1. We provide a printed redetermination output to beneficiaries to review at the conclusion of the redetermination interview. The claims representative must print this before closing the redetermination. The output shows the information collected and instructs the recipient to let us know if any of the information needs correction or updating; and

2. If there are changes because of a processed redetermination, the system generates notices describing those changes and any rights for administrative review.

Both of these mechanisms allow beneficiaries to confirm whether the employee accurately recorded information during the interview.