OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

November 9, 2018

Nancy A. Berryhill
Acting Commissioner

The *Chief Financial Officers Act of 1990* (Pub. L. No. 101-576), as amended, requires that the Social Security Administration's (SSA) Inspector General or an independent external auditor, as determined by the Inspector General, audit SSA's consolidated 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) 2018 consolidated financial statements. This letter transmits Grant Thornton's *Report of Independent Certified Public Accountants* on the audit of SSA's FY 2018 consolidated and sustainability financial statements. Grant Thornton's report includes the following.

- Opinions on the Financial Statements, including the Opinions on the Consolidated Financial Statements and Sustainability Financial Statements, and the Effectiveness of SSA's Internal Controls over Financial Reporting.
- Other Reporting Requirements Required by *Government Auditing Standards*.

OBJECTIVES OF A FINANCIAL STATEMENT AND EFFECTIVENESS OF INTERNAL CONTROLS OVER FINANCIAL REPORTING AUDITS

Grant Thornton conducted its audit of the consolidated and sustainability financial statements and SSA's internal control over financial reporting 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. 19-01, *Audit Requirements for Federal Financial Statements.* Those Standards and Bulletin require that Grant Thornton plan and perform the audits to obtain reasonable assurance about whether the financial statements are free from material misstatement and whether effective internal control over financial reporting was maintained in all material respects.

An audit of financial statements involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. An audit of financial statements also includes evaluating the appropriateness of accounting policies used and the reasonableness of management's significant accounting estimates as well as evaluating the overall presentation of the financial statements.

The sustainability financial statements are based on management's assumptions and are intended to aid users in assessing whether future resources will likely be sufficient to sustain public services and meet obligations as they come due. The sustainability financial statements are not forecasts or predictions and are not intended to imply that current policy or law is sustainable. Given the number of factors that affect the sustainability financial statements and the fact that future events and circumstances cannot be estimated with certainty, even if current policy is continued, the estimates in the sustainability financial statements and the actual results will differ.

In addition, Grant Thornton audited SSA's internal control over financial reporting as of September 30, 2018 based on criteria established under 31 U.S.C. § 3512 (c), (d) (commonly known as the Federal Managers' Financial Integrity Act or "FMFIA") and in the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States. An audit of internal controls over financial reporting included performing procedures to obtain audit evidence about whether a material weakness exists, obtaining an understanding of internal

control over financial reporting, and testing and evaluating the design and operating effectiveness of internal control over financial reporting based on the assessed risk. Because of its inherent limitations, internal control over financial reporting may not prevent or detect and correct misstatements.

AUDIT OF FINANCIAL STATEMENTS, EFFECTIVENESS OF INTERNAL CONTROL, AND COMPLIANCE WITH LAWS AND REGULATIONS

KPMG LLP (KPMG) issued unmodified opinions on SSA's FY 2017 consolidated and sustainability financial statements. KPMG also issued an unmodified opinion that SSA maintained effective internal control over financial reporting as of September 30, 2017 based on criteria established under FMFIA and in the *Standards for Internal Control in the Federal Government* issued by the Comptroller of the United States. However, KPMG identified three significant deficiencies in internal controls as of September 30, 2017: (1) Certain Financial Information System Controls, (2) Controls over the Reliability of Information Used in Certain Control Activities, and (3) Accounts Receivable/Overpayments.

Grant Thornton issued unmodified opinions on SSA's FY 2018 consolidated financial statements, the sustainability financial statement as of January 1, 2018, and the changes in its social insurance amounts for the period January 1, 2017 to January 1, 2018. In addition, Grant Thornton issued an unmodified opinion that SSA maintained effective internal control over financial reporting as of September 30, 2018 based on criteria established under FMFIA and in the *Standards for Internal Control in the Federal Government*, issued by the Comptroller of the United States. However, Grant Thornton did identify three significant deficiencies in internal controls as of September 30, 2018: (1) Certain Financial Information Systems Controls, (2) Controls over the Reliability of Information Used in Certain Control Activities, and (3) Accounts Receivable with the Public (Benefit Overpayments). These findings did not have a material impact on the financial statements.

SIGNIFICANT DEFICIENCY – CERTAIN FINANCIAL INFORMATION SYSTEMS CONTROLS

Grant Thornton identified a number of systems control deficiencies, when aggregated, are considered to be a significant deficiency in the area of Information Technology (IT) Systems Controls. The control deficiencies were mapped to four overall components that are described below. This significant deficiency is a repeat from prior years. Specifically, Grant Thornton's testing disclosed the following deficiencies.

1. **IT Oversight and Governance:** Grant Thornton continued to identify recurring issues associated with security management, physical and logical access controls, segregation of duties, information system contingency planning, and configuration management, including, in some cases, implementation and monitoring of appropriate security configurations on platforms. Further, there were areas where SSA's requirements and guidance were inconsistently implemented and / or locations were unaware of certain requirements. Finally, Grant Thornton cited control deficiencies related to the completeness and accuracy of information system inventories and boundaries, control inheritance considerations, and lack of completed requirements within security assessment and authorization packages.

2. **Access Controls:** Grant Thornton's testing identified control failures related to account management controls including access authorizations, re-certification of access, and the timely removal of logical access after termination. Further Grant Thornton noted issues with segregation of duties, privileged access, the review of mainframe profile content, and the review of security violation reports. Finally, Grant Thornton identified physical security control weaknesses that potentially allowed unauthorized individuals access to non-sensitive areas.

3. **Network Security Controls:** Grant Thornton identified inventory, configuration management, patch management, and access control deficiencies with network security controls, many of which continued to persist from prior audits.

4. **Change and Configuration Management:** Grant Thornton noted instances where management did not consistently comply with or implement SSA's change management directives, policies, and procedures for financially relevant system changes. In addition, Grant Thornton noted SSA needed to improve its controls over (1) establishing comprehensive security configuration baselines; (2) reviewing security configurations periodically; (3) hardening security guides; (4) adhering to these baselines and guides by periodically monitoring; and (5) assessing, remediating, and/or approving deviations (if applicable).

SIGNIFICANT DEFICIENCY – CONTROLS OVER THE RELIABILITY OF INFORMATION USED IN CERTAIN CONTROL ACTIVITIES

Grant Thornton found deficiencies in the control design and operating effectiveness related to information produced by entity (IPE). This significant deficiency is a repeat from last year.

Grant Thornton was not able to determine whether SSA's recently issued policy was implemented and effectuated agency-wide because it was not finalized until the last month of FY 2018 and evidence of implementation of the formal policy was not available. Lack of a formal policy being in place for the majority of the FY increased the likelihood that controls were not appropriately executed and inaccurate data may have been relied on.

In addition, Grant Thornton's testing of operating effectiveness identified that 2 of 18 scans were not completed. Because there were no routinely executing controls, there was an increased risk that management was relying on inaccurate data.

Grant Thornton only noted findings related to the completeness and accuracy of financially relevant IPE in the area of Accounts Receivable with the Public (Benefit Overpayments), as discussed below.

SIGNIFICANT DEFICIENCY – ACCOUNTS RECEIVABLE WITH THE PUBLIC (BENEFIT OVERPAYMENTS)

Grant Thornton identified four deficiencies in internal control that, when aggregated, are considered to be a significant deficiency related to weaknesses in internal controls over Accounts Receivable with the Public. This significant deficiency is a repeat from prior years. Specifically, Grant Thornton's testing disclosed the following deficiencies.

1. **Reconciliation of Accounts Receivable Ledgers:** Detailed beneficiary information for Old-Age, Survivors and Disability Insurance (OASDI) and Supplemental Security Income overpayments did not agree with summary level reports from subsidiary ledgers, which are then relied upon to update the general ledger. Current system limitations prevent SSA from reconciling the differences between the detail and summary level information with subsidiary ledgers. SSA continues to design and implement additional controls to reconcile the information; however, these processes were not finalized by year-end.

2. **Overpayment Documentation and Calculations:** In approximately 40 percent of sample cases tested, Grant Thornton identified errors that affected the accuracy of the overpayment. In addition, testing continued to demonstrate insufficient documentation with overpayment records and waiver approvals.

3. **Overpayment Records and Tracking for Long-term Installment Payments:** SSA identified an IT system limitation where receivable installment payments extending past the year 2049 were not tracked.

4. **Overpayment Prevention:** Grant Thornton conducted Computer Assisted Auditing Techniques and identified discrepancies between data fields as well as data indicating ineligibility for benefit payments based on SSA requirements. Grant Thornton categorized these discrepancies into those that resulted in an overpayment or did not impact the beneficiary's benefit payment but could lead to future overpayments.

Grant Thornton identified no reportable instances of non-compliance with the laws, regulations, contracts, grant agreements, or other matters tested.

OIG Evaluation of Grant Thornton Audit Performance

To fulfill our responsibilities under the *Chief Financial Officers Act of 1990* and related legislation for ensuring the quality of the audit work performed, we monitored Grant Thornton's audit of SSA's FY 2018 consolidated and sustainability 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. 19-01;
- coordinating the issuance of the audit report; and
- performing other procedures we deemed necessary.

Grant Thornton is responsible for the attached auditors' report, dated November 9, 2018, and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding Grant Thornton's performance under the contract terms. 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 consolidated financial statements; sustainability financial statements; effectiveness of its internal control over financial reporting; or SSA's compliance with certain laws, regulations, contracts and grant agreements. However, our monitoring review, as qualified above, disclosed no instances where Grant Thornton did not comply with applicable auditing and attestation 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.

Gale Stallworth Stone

Gale Stallworth Stone
Acting Inspector General

Enclosure

Grant Thornton LLP
1000 Wilson Boulevard, Suite 1400
Arlington, VA 22209

T 703.847.7500
F 703.848.9580
www.GrantThornton.com

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

Nancy A. Berryhill
Acting Commissioner
Social Security Administration

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

- The consolidated balance sheet of SSA as of September 30, 2018, the related consolidated statements of net cost and changes in net position, and the combined statement of budgetary resources for the year then ended, are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America;
- The sustainability financial statements which comprise the statement of social insurance as of January 1, 2018 and the statement of changes in social insurance amounts for the period January 1, 2017 to January 1, 2018 are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America;
- Although internal controls could be improved, SSA management maintained, in all material respects, effective internal control over financial reporting as of September 30, 2018; and
- No reportable instances of noncompliance for Fiscal Year 2018, with provisions of applicable laws, regulations, contracts, and grant agreements we tested.

The following sections discuss in more detail our report on the financial statements and on internal control over financial reporting which includes a matter of emphasis paragraph related to the sustainability financial statements, required supplementary information (RSI) and other information included with the financial statements, our report on compliance with laws, regulations, contracts, and grant agreements, and the Agency's response to findings.

Report on the Financial Statements and Internal Control over Financial Reporting

We have audited the accompanying financial statements of the Social Security Administration (the "Agency"), which comprise the consolidated financial statements and the sustainability financial statements. The consolidated financial statements comprise the consolidated balance sheet as of September 30, 2018, the related consolidated statements of net cost, changes in net position, and the combined statement of budgetary resources for the year then ended, and the related notes to the consolidated financial statements.

The sustainability financial statements comprise the statements of social insurance as of January 1, 2018, 2015, and 2014, the statement of changes in social insurance amounts for the period January 1, 2017 to January 1, 2018, and the related notes to the sustainability financial statements.

We also have audited the internal control over financial reporting of the Social Security Administration as of September 30, 2018, based on criteria established under 31 U.S.C. § 3512 (c),(d) (commonly known as the Federal Managers' Financial Integrity Act or "FMFIA") and in *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

Management's Responsibility for the Financial Statements and Internal Control over Financial Reporting

Agency 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 effective internal control over financial reporting relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error. Management is also responsible for evaluating the effectiveness of internal control over financial reporting based on the criteria established under FMFIA and its assessment about the effectiveness of internal control over financial reporting as of September 30, 2018, included in the accompanying FMFIA Assurance Statement.

Auditor's Responsibility

Our responsibility is to express opinions on these financial statements and an opinion on the entity's internal control over financial reporting 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 19-01, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin 19-01 require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement and whether effective internal control over financial reporting was maintained in all material respects.

An audit of financial statements 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 Agency's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances. An audit of financial statements 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.

An audit of internal control over financial reporting involves performing procedures to obtain audit evidence about whether a material weakness exists. The procedures selected depend on the auditor's judgment, including the assessment of the risk that a material weakness exists. An audit of internal control over financial reporting also involves obtaining an understanding of internal control over financial reporting and testing and evaluating the design and operating effectiveness of internal control over financial reporting based on the assessed risk. Our audit of internal control also considered the Agency's process for evaluating and reporting on internal control over financial reporting based on criteria established under FMFIA. Our audits also included performing such other procedures as we considered necessary in the circumstances.

We did not evaluate all internal controls relevant to operating objectives as broadly established under FMFIA, such as those controls relevant to preparing performance information and ensuring efficient operations. We limited our internal control testing to testing controls over financial reporting. Our internal control testing was for the purpose of expressing an opinion on whether effective internal control over financial reporting was maintained, in all material respects. Consequently, our audit may not identify all deficiencies in internal control over financial reporting that are less severe than a material weakness.

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

Definition and Inherent Limitations of Internal Control over Financial Reporting

An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America. An entity's internal control over financial reporting provides reasonable assurance that (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with accounting principles generally accepted in the United States of America, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition, and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority, regulations, contracts and grant agreements, noncompliance with which 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 due to fraud or error. Also, projections of any assessment 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 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, such that there is a reasonable possibility that a material misstatement of the Agency's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Opinions on the Financial Statements

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the Social Security Administration as of September 30, 2018, and its net cost, changes in net position, and budgetary resources for the year then ended, in accordance with accounting principles generally accepted in the United States of America.

Also, in our opinion, the sustainability financial statements referred to above present fairly, in all material respects the Social Security Administration's social insurance information as of January 1, 2018, 2015, and 2014 and its changes in social insurance amounts for the periods January 1, 2017 to January 1, 2018, in accordance with accounting principles generally accepted in the United States of America.

Emphasis of Matter

As discussed in Note 17 to the financial statements, the sustainability financial statements are based on management's assumptions. These sustainability financial statements present the actuarial present value of the Agency's estimated future income to be received and future expenditures to be paid using a projection period sufficient to illustrate long-term sustainability. The sustainability financial statements are intended to aid users in assessing whether future resources will likely be sufficient to sustain public services and to meet obligations as they come due. The statements of social insurance and changes in social insurance amounts are based on income and benefit formulas in current law and assume that scheduled benefits will continue after any related trust funds are exhausted. The sustainability financial statements are not forecasts or predictions. The sustainability financial statements are not intended to imply that current policy or law is sustainable. In preparing the sustainability financial statements, management considers and selects assumptions and data that it believes provide a reasonable basis to illustrate whether current policy or law is sustainable. Assumptions underlying such sustainability information do not consider changes in policy or all potential future events that could affect future income,

future expenditures, and sustainability, for example, implementation of policy changes to avoid trust fund exhaustion. Because of the large number of factors that affect the sustainability financial statements and the fact that future events and circumstances cannot be estimated with certainty, even if current policy is continued, there will be differences between the estimates in the sustainability financial statements and the actual results, and those differences may be material. Our opinion is not modified with respect to this matter.

Opinion on Internal Control over Financial Reporting

In our opinion, although certain internal controls could be improved, the Social Security Administration maintained, in all material respects, effective internal control over financial reporting as of September 30, 2018, based on criteria established under 31 U.S.C § 3512 (c),(d) (commonly known as FMFIA) and in *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

As discussed in more detail, our 2018 audit identified deficiencies in the Agency's controls over Certain Financial Information Systems Controls, Controls over the Reliability of Information Used in Certain Control Activities and Accounts Receivable with the Public (Benefit Overpayments), described in the accompanying Appendix *Significant Deficiencies in Internal Control Over Financial Reporting*, that represent significant deficiencies in the Agency's internal control over financial reporting. We considered these significant deficiencies in determining the nature, timing, and extent of our audit procedures on the Agency's 2018 financial statements. Although the significant deficiencies in internal control did not affect our opinion on the Agency's 2018 financial statements, misstatements may occur in unaudited financial information reported internally and externally by the Agency because of these significant deficiencies.

In addition to the significant deficiencies in internal control over Certain Financial Information Systems Controls, Controls over the Reliability of Information Used in Certain Control Activities and Accounts Receivable with the Public (Benefit Overpayments), during our 2018 audits, we also identified deficiencies in the Agency's internal control over financial reporting that we do not consider to be material weaknesses or significant deficiencies. Nonetheless, these deficiencies warrant Agency management's attention. We have communicated these matters to Agency management and, where appropriate, will report on them separately.

Other Matters

The consolidated financial statements of the Agency as of and for the year ended September 30, 2017 and the sustainability financial statements as of and for the years ended January 1, 2017 and 2016 were audited by other auditors. Those auditors' report, dated November 9, 2017, expressed an unmodified opinion on those financial statements and included an emphasis of matter paragraph that described the assumptions upon which the sustainability financial statements are based discussed in Note 18 to the financial statements.

Required Supplementary Information

Accounting principles generally accepted in the United States of America require that the information in Management's Discussion and Analysis from pages 5 to 36 and the combining schedule of budgetary resources, and the required supplementary social insurance information from pages 83 to 95 be presented to supplement the basic financial statements. Such information, although not a required part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board and OMB Circular A-136, *Financial Reporting Requirements*, which consider it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. Management is responsible for preparing, measuring, and presenting the required supplementary information in accordance with accounting principles generally accepted in the United States of America. We have applied certain limited procedures to the required supplementary information

in accordance with auditing standards generally accepted in the United States of America. 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

Our audits were conducted for the purpose of forming an opinion on the basic financial statements as a whole. The Acting Commissioner's Message on page 1 and the other information on pages 2 through 4, 37 through 39, 79 through 82 and 116 through 226 is presented for purposes of additional analysis and is not a required part of the basic financial statements. Management is responsible for preparing and presenting other information included in documents containing the audited financial statements and auditor's report, and for ensuring the consistency of that information with the basic financial statements and the required supplementary information. We read the other information in order to identify material inconsistencies, if any, with 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 do not express an opinion or provide any assurance on it.

Report on Compliance with Laws, Regulations, Contracts and Grant Agreements and Other Matters

As part of obtaining reasonable assurance about whether the Agency's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements consistent with the auditor's responsibility discussed below, in accordance with *Government Auditing Standards*. Noncompliance may occur that is not detected by these tests.

Management's Responsibility

Agency management is responsible for complying with laws, regulations, contracts, and grant agreements applicable to the Agency.

Auditor's Responsibility

Our responsibility is to test compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts and disclosures, and perform certain other limited procedures. We did not test compliance with all laws, regulations, contracts, and grant agreements.

Results of our Tests of Compliance with Laws, Regulations, Contracts, and Grant Agreements

The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*. However, the objective of our tests was not to provide an opinion on compliance with laws, regulations, contracts, and grant agreements applicable to the Agency. Accordingly, we do not express such an opinion.

Under the Federal Financial Management Improvement Act ("FFMIA"), we are required to report whether the Agency's financial management systems substantially comply with FFMIA Section 803(a) requirements. To meet this requirement, we performed tests of compliance with the federal financial management systems requirements, applicable federal accounting standards, and the *United States Government Standard General Ledger* ("USSGL") at the transaction level. However, providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly we do not express such an

opinion. The results of our tests of FFMIA Section 803(a) requirements disclosed no instances of substantial noncompliance that are required to be reported under FFMIA.

Agency's Response to Findings

The Agency's response to our findings, which is included on page 115 of this Agency Financial Report, was not subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on the Agency's response.

Intended Purpose of Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements

The purpose of this report is solely to describe the scope of our testing of compliance and the results of that testing, and not to provide an opinion on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering compliance. Accordingly, this report is not suitable for any other purpose.

Grant Thornton LLP

Arlington, Virginia
November 9, 2018

APPENDIX – SIGNIFICANT DEFICIENCIES IN INTERNAL CONTROL OVER FINANCIAL REPORTING

Significant Deficiency in Internal Control over Certain Financial Information Systems Controls

Overview

Social Security Administration (SSA) management relies on information systems and information technology (IT) to administer and process the Old-Age and Survivors Insurance (OASI) and Disability Insurance (DI) (collectively known as OASDI or Title II) and Supplemental Security Income (SSI or Title XVI) programs, to process and account for their expenditures, and for financial reporting. A lack of appropriately designed or implemented internal controls for these information systems and related IT increases the risk of unreliable data, the program's integrity, and misstatements whether due to fraud or error.

Our internal control testing covered both IT general control (ITGC) and application controls. ITGC testing encompassed the security management program, access controls (physical and logical), configuration and change management, segregation of duties, and service continuity/contingency planning. ITGCs provide the foundation for the integrity of systems including applications and the system software that comprise the general support systems for the major applications. General and application-level controls are critical to ensuring the accurate and complete processing of transactions and integrity of stored data. Application controls include controls over application-specific general controls, 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.

The Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, and 200, Minimum Security Requirements for Federal Information and Information Systems, are mandatory security standards required by the *Federal Information Security Modernization Act of 2014* (FISMA). These standards, in combination with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, define a framework for Federal agencies to apply to develop, document, and implement an agency-wide information security program. The information security program is required to provide security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems.

Deficiencies in Control Design and/or Operational Effectiveness

We noted control deficiencies in the areas of IT oversight and governance, access controls, network security controls, and change and configuration management that contribute to an aggregated significant deficiency in information system controls. While SSA continued strengthening controls over its information systems and IT, many of the control deficiencies from past audits continued to persist. We noted that SSA developed several plans, strategies, and initiatives to address control deficiencies noted in past audits. However, these deficiencies continued to exist because of one, or a combination, of the following.

- SSA relied on manually intensive processes.
- SSA had not thoroughly assessed the root cause(s) of deficiencies and prioritized corrective actions to address the highest areas of risk.
- The design of enhanced or newly designed controls did not completely address risks and recommendations provided in past audits.
- Agency management's oversight and governance was not sufficient.

IT Oversight and Governance

Appropriate IT governance and oversight provides assurance that risks are identified and assessed and 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 had persisted from past audits because of limited remediation in the current fiscal year. Specifically, recurring issues continue to be cited associated with security management, physical and logical access controls, segregation of duties, information system contingency planning, and configuration management including, in some cases, implementation and monitoring of appropriate security configurations on platforms. Further, there were areas where SSA's requirements and guidance were inconsistently implemented and / or locations were unaware of certain requirements. Finally, we cited control deficiencies related to the completeness and accuracy of information system inventories and boundaries, control inheritance considerations, and a lack of completed requirements within security assessment and authorization (SA&A) packages. These issues could have such negative effects as inaccurate security categorization of systems and applications; inappropriate identification, implementation and documentation of required controls; inappropriate testing and monitoring of those controls; and approving authorization to operate (ATO) packages for the system without an appropriate understanding of risks.

Access Controls

Access controls provide assurance that critical information systems' assets are physically safeguarded and 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 data and increase the risk that such data may be inappropriately accessed and/or disclosed as well as modified by unauthorized persons, which may affect the accuracy of the financial statements. Our testing identified control failures related to account management controls including access authorizations, recertification of access, and the timely removal of logical access after termination. Further, we noted issues with segregation of duties, privileged access, the review of mainframe profile content, and the review of security violation reports. Finally, we identified physical security control weaknesses that potentially allowed unauthorized individuals access to non-sensitive areas.

Network Security Controls

Configuration, vulnerability, and patch management processes are examples of critical components to effective network security. Related processes and controls must be designed to prevent or detect such weaknesses as misconfigurations, weak credentials, and vulnerabilities and are essential in combating internal and external cyber-threats, exploitations, and unauthorized access. We identified certain inventory, configuration management, patch management, access control, and network security deficiencies, many of which continued to persist from prior audits. Information about these deficiencies was presented in a separate, limited-distribution management letter.

Change and Configuration 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. Configuration management involves the identification and management of security features for hardware, software, and firmware components of an information system at a given point while controlling changes to that configuration as part of the systems' life cycle. A disciplined process for testing, approving, and migrating changes between environments, including into production, is essential to ensure that systems operate as intended, configurations align with security standards, and that no unauthorized changes are implemented to the source code, data, and/or configuration settings. We noted instances where

management did not consistently comply or implement SSA's change management directives, policies and procedures for financially relevant system changes. In addition, we noted SSA needed to improve its controls over (1) establishing comprehensive security configuration baselines; (2) reviewing security configurations periodically; (3) hardening security guides; (4) adhering to these baselines and guides by periodically monitoring; and (5) assessing, remediating, and/or approving deviations (if applicable).

These findings did not have a material impact on the financial statements.

Recommendations

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

1. Analyze the resulting audit findings to identify root causes and trends, assess risk of control failures, and re-evaluate priorities for remediation. SSA should develop and/or review its risk-based approach and develop a roadmap of corrective actions. SSA should set attainable milestones for corrective actions and remediate these deficiencies timely.
2. Enhance its IT oversight, governance, and risk management processes—as they apply to SSA, DDS, contractor, and external systems—to ensure the Agency's IT risk management framework requirements are effectively and consistently implemented across the organization.
3. Strengthen SSA's internal control system for access controls, network security, and change and configuration management to improve its effectiveness in identifying, documenting, and linking these controls to business processing controls that support financial reporting; assessing the design and effectiveness of these controls; and remediating any identified IT control gaps.

Significant Deficiency in Internal Control over the Reliability of Information Used in Certain Control Activities

Overview

Given the nature of SSA operations, reliable system-generated information, also known as information produced by the entity (IPE), is essential to producing the Agency's financial statements as well as providing information for sound management decisions. SSA also relies on IPE when it performs manual internal controls. To rely on IPE, management must have internal controls in place to gain comfort over the completeness and accuracy of the reports and information. Considering the significant deficiency noted over Information Systems Controls, SSA should place additional diligence over their control processes related to the completeness and accuracy of IPE.

The *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States (Green Book) Principle No. 13, *Use Quality Information*, states "Management processes the obtained data into quality information that supports the internal control system. This involves processing data into information and then evaluating the processed information so that it is quality information. Quality information meets the identified information requirements when relevant data from reliable sources are used."

Deficiencies in Control Design

Grant Thornton noted that SSA had executed a written policy over Financial Dataset and Job Completeness Scans, including requirements for maintaining a population of financially significant system-generated reports and requirements for periodically testing (scanning) to determine whether changes to the supporting report code were subject to appropriate change controls. However, because the procedures were refined through the fiscal year, the policy was not finalized until the last month of Fiscal Year 2018, and evidence the formal policy had been implemented was not available. As a result, we could not determine whether the policy was implemented and effectuated Agency-wide. Lack of a

formal policy for the majority of the fiscal year increased the likelihood that controls were not appropriately executed and inaccurate data may have been relied on.

Deficiencies in Control Operating Effectiveness

As part of our initial testing of management's efforts over testing the completeness and accuracy of IPE we selected a preliminary sample of eighteen scans which should have been completed based on SSA's existing procedures. We noted two of eighteen scans had not been completed. These exceptions occurred because of staff turnover and there was no formal documentation of requirements for new staff. Because controls were not executed routinely, there was an increased risk management was relying on inaccurate data, as noted in our testing of operating effectiveness.

Throughout our testing of the completeness and accuracy of financially relevant IPE used in our audit procedures, we only noted findings in accounts receivable, as discussed in our Significant Deficiency in Internal Control over Accounts Receivable with the Public (Benefit Overpayments).

These findings did not have a material impact on the financial statements.

Recommendations

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

1. Full implementation of the written policy for Financial Dataset and Job Completeness Scanning.
2. Periodic review and updating of the population of IPE applicable to the Financial Dataset and Job Completeness Scanning policy.
3. Regular management review and monitoring over completed scans of IPE jobs and datasets.

Significant Deficiency in Internal Control over Accounts Receivable with the Public (Benefit Overpayments)

Overview

When SSA beneficiaries receive payments beyond their entitled amount, a benefit overpayment exists. When SSA detects an overpayment, 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 (FO), 8 Processing Centers (PC), or various function areas within the SSA central office. Therefore, SSA has specific policies, procedures, and internal controls in place to consistently detect, calculate, and document overpayments and the related accounts receivable balances. Since this process can be complex for some cases and relies on manual input, SSA's adherence to its internal controls is critical to accurately recording, documenting, and tracking overpayment balances. Management also relies on its IT infrastructure, interfaces, and controls to record and prevent erroneous payments.

Reconciliation of Accounts Receivable Ledgers

Office of Management and Budget (OMB) Circular A-123, Appendix D, *Compliance with Federal Financial Management Improvement Act*, requires application of the U.S. Government Standard General Ledger (USSGL) at the transaction level. SSA tracks individual debtor overpayment transactions and accounts receivable balances in subsidiary ledger systems and adjusts the general ledger according to the balances reported from the subsidiary ledgers. Our testing revealed the detail level beneficiary

information in the two primary accounts receivable subsidiary ledgers did not agree with the summary-level reports from the subsidiary ledgers.

SSA relies on these summary level reports to update the general ledger; therefore, the balances reported in the general ledger and subsequently the financial statements, differ from the supporting detail level beneficiary data in the subsidiary ledger systems, which could lead to misstatements of the accounts receivable with the public line item.

System limitations prevent SSA from reconciling the differences between the detail and summary-level information with subsidiary ledgers. However, the unreconciled differences are immaterial to the financial statements and the accounts receivable with the public line items.

In Fiscal Year 2018, SSA continued designing and implementing additional controls to reconcile the detail and summary level information; however, these processes had not been finalized by fiscal year-end.

Deficiencies in Overpayment Documentation and Calculations

We noted that prior audits identified significant deficiencies in internal controls related to SSA adhering to Program Operations Manual System (POMS) criteria regarding maintaining sufficient evidence to support overpayments balances or sufficient evidence to support approval of waived overpayments. POMS provides important policies, procedures, and internal controls over processing and documenting overpayments. Based on evidence obtained during our business process walkthroughs, we determined SSA had developed updated training for field and regional office personnel on obtaining and maintaining documentation necessary to support claims for overpayments and approval of waived overpayments.

However, based on inquiry with management, the timing of training deployment and time needed for the training to effectuate through the internal control environment, prevents improvements to be yielded in Fiscal Year 2018. Therefore, we did not test a separate sample of new overpayments identified in Fiscal Year 2018 for internal control effectiveness. Our internal control testing of overpayments waived in the fiscal year continued demonstrating insufficient documentation of waiver approvals as well as insufficient documentation of initial overpayment records. Insufficiently following established policy and lack of documentation to support overpayments can lead to difficulties in calculating and substantiating outstanding accounts receivable balances and potential misstatements to accounts receivable with the public balance presented on the financial statements.

In addition, we selected a statistical sample of outstanding overpayments balances and noted overpayment calculation errors in 27 out of 68 items sampled (or 40 percent). Although the statistically projected impact of these calculation errors was not material to the financial statements, these errors further evidence control weaknesses in the accounts receivable with the public processes, including inappropriate overpayment tracking that could lead to misstatements in the financial statements.

Deficiencies in Overpayment Records and Tracking for Long-term Installment Payments

Upon beneficiary request, overpayment balances are often repaid to SSA in monthly installments as withholdings from monthly benefit payments. Depending on the amount of the overpayment balance and the amount of each installment, repayment periods can extend beyond the Year 2049.

According to Statement of Federal Financial Accounting Standards (SFFAS) 7 *Accounting for Revenue and Other Financial Sources*, revenue should be recognized when a specifically identifiable, legally enforceable claim to resources arises, to the extent that collection is probable (more likely than not) and the amount is reasonably estimable.

We noted that SSA 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 are understated in the amount of the installment payments expected to be

collected beyond Year 2049. The projected understatements are immaterial to the financial statements and the accounts receivable with the public balance. While the Agency is working on enhancing system 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 understate accounts receivable balances. In addition, the impact of this issue will continue to grow as the Year 2049 approaches if other factors remain constant.

Deficiencies in Overpayment Prevention

While conducting Computer Assisted Auditing Techniques (CAATs) over SSA's records, we identified instances of discrepancies between data fields as well as data indicating ineligibility for benefit payments based on SSA requirements. These discrepancies were categorized into two types: those that (1) resulted in an overpayment or (2) did not impact a beneficiary's benefit payment but could lead to future overpayments. The discrepancies specific to type (1) included beneficiaries not being transferred to the correct program timely and beneficiaries' secondary records not being considered when calculating the payment amount. The discrepancies specific to type (2) included beneficiaries for which certain data fields, such as Quarters of Coverage requirements and marital information, were inaccurate.

While these cases were clearly immaterial to SSA's financial statements, they were indicative of a control failure where SSA internal processes did not detect and correct potential overpayments or data discrepancies in a timely manner. While overpayments occur for many reasons, SSA should take 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. Further, the longer an overpayment goes undetected, the greater the overpayment balance becomes while the probability of accounts receivable collection decreases.

These findings did not have a material impact on the financial statements.

Recommendations

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

Reconciliation of Accounts Receivable Ledgers

1. Continue implementing and executing reconciliation internal controls between subsidiary ledgers at the detail level and the general ledger, through summary reports. Investigate and document reconciling differences on a periodic and timely manner.
2. Investigate potential system reporting enhancements to reduce unreconciled differences between summary and detail level data produced by subsidiary ledgers.

Deficiencies in Overpayment Documentation and Calculations

1. Continue to explore opportunities to improve overpayment accuracy and document retention through engaging field office and payment center employees in trainings related to common weaknesses and more complex over payment cases.
2. Enhance management review of overpayment processing considering risk based factors such as current overpayment balances, manual intervention required and age.
3. Consider implementation of new overpayment documentation tools to ensure overpayments are documented completely, accurately, and timely by FOs or PCs within the appropriate systems of record.

Deficiencies in Overpayment Records and Tracking for Long-term Installment Payments

1. Continue to work towards updated debt management systems without the technical limitations over the length of time repayment installments can be recorded.
2. Continue pursuing changes in repayment policy to minimize future extended repayment plans.
3. Continue to analyze and track the impact of the current Year 2049 issue on the financial statements.

Deficiencies in Overpayment Prevention

1. Continue evaluating beneficiary data on a recurring basis to identify instances where beneficiaries do not meet eligibility requirements.
2. Enhance periodic reconciliations between various SSA systems.