OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

November 9, 2017

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), KPMG LLP (KPMG), an independent certified public accounting firm, audited SSA's Fiscal Year (FY) 2017 consolidated financial statements. This letter transmits the KPMG *Independent Auditors' Report* on the audit of SSA's FY 2017 consolidated financial statements. KPMG's report includes the following:

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

Objectives of a Financial Statement and Effectiveness of Internal Controls over Financial Reporting Audits

KPMG conducted its audit of the consolidated financial statements 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. 17-03, *Audit Requirements for Federal Financial Statements.* Those standards and OMB Bulletin No. 17-03 require that KPMG 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 significant accounting estimates made by management 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 to meet obligations as they come due. The sustainability financial statements are not forecasts or prediction, 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, KPMG audited SSA's internal control over financial reporting as of September 30, 2017 based on criteria established 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 issued unmodified opinions on SSA's FY 2017 and 2016 consolidated financial statements, the sustainability financial statements as of January 1, 2017 and January 1, 2016, and the changes in its social insurance amounts for the periods January 1, 2016 to January 1, 2017 and January 1, 2015 to January 1, 2016. Refer to SSA's FY 2017 *Agency Financial Report* webpage (https://www.ssa.gov/finance) to access the financial statements. In addition, KPMG issued an unmodified opinion that SSA maintained effective internal control over financial reporting as of September 30, 2017 based on criteria established in the *Standards for Internal Control in the Federal Government* issued by the Comptroller of the United States. However, KPMG did identify 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.

Significant Deficiency – Certain Financial Information System Controls

KPMG identified four systems control deficiencies that, when aggregated, are considered to be a significant deficiency in the area of Information Technology (IT) Systems Controls. This significant deficiency is a repeat from the prior year. Specifically, KPMG's testing disclosed the following deficiencies.

1. **IT Oversight and Governance:** SSA's organizational information security risk assessment and strategy did not fully consider risk framing, assumptions, tolerance, and constraints as well as Agency priorities and tradeoffs. In addition, SSA's Program Operations Manual System (POMS) lacked certain control requirements and guidance over access controls and segregation of duties leading to instances of inconsistent implementation and noncompliance with SSA policy. Personnel at disability determination services (DDS) and program service centers (PSC) were not always aware of control requirements.

2. **Access Controls:** Instances where documentation supporting the operation of controls related to the completion, review, and recertification of logical access authorization forms was not always available and instances where users had inappropriate logical access to both the development and production change management environments for financially relevant applications, a production application dataset, and an application transaction. In addition, KPMG identified deficiencies related to physical access to certain computer rooms that housed the DDS and PSC servers and hardware. Finally, SSA had not always implemented optimal security settings in its production operating systems and databases supporting financially relevant applications to conform to industry and National Institute of Standards and Technology (NIST) guidance and SSA's defined risk profiles.

3. **Network Security Controls:** KPMG identified configuration, patch management, and access control deficiencies with network security controls, many of which continued to exist from the prior year's audit.

4. **Change and Configuration Management:** KPMG identified instances where management did not fully comply with certain change management directives, policies, and procedures for the financially relevant system management by SSA Headquarters. In addition, KPMG identified instances where security settings in financially relevant application platforms and DDS case processing system platforms did not always comply with SSA's risk models and security policies.

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

KPMG found that management did not design and implement effective controls to ensure certain information produced by the entity (IPE), used in performing manual process-level controls in benefits due and payable as well as accounts receivable, was complete and accurate. SSA's risk assessment process did not identify completeness and accuracy of IPE resulting from the IT controls deficiencies, identified above, as a risk that required additional compensating controls.

Significant Deficiency – Accounts Receivable/Overpayments

KPMG 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/overpayments. This significant deficiency is a repeat from the prior year. Specifically, KPMG's testing disclosed the following deficiencies.

1. **Financial Accounting Process Related to Overpayments:** Subsidiary ledgers used to account for Old-Age, Survivors and Disability Insurance (OASDI) and Supplemental Security Income overpayments did not agree with the general ledger, and SSA lacked an internal control requiring routine reconciliation of subsidiary ledgers to the general ledger.

2. **Documentation Supporting Accounts Receivable/Overpayment Claims and Calculations:** In approximately 48 percent of samples tested, KPMG identified errors that affected the accuracy of the overpayment. In addition, in approximately 22 percent of samples tested, SSA could not locate some or all of the documentation to support the existence of a claim.

3. **Compliance with SSA Policies and Procedures Impacting Effectiveness of Internal Controls:** KPMG identified instances where SSA and DDS employees did not fully comply with SSA policies, including retaining sufficient evidence to support a claim for overpayment or approval of waived overpayments.

4. **IT System Limitations Affecting Accuracy and Presentation of OASDI Accounts Receivable:** SSA identified an IT system limitation where OASDI receivable installment payments extending past the year 2049 were not tracked.

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

OIG Evaluation of KPMG 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 KPMG's audit of SSA's FY 2017 consolidated financial statements by

- reviewing KPMG's audit approach and planning;
- evaluating its auditors' qualifications and independence;
- monitoring the audit's progress at key points;
- examining KPMG's documentation related to planning the audit, assessing SSA's internal control, and substantive testing;
- reviewing KPMG's audit report to ensure compliance with Government Auditing Standards and OMB Bulletin No. 17-03;
- coordinating the issuance of the audit report; and

- performing other procedures we deemed necessary.

KPMG is responsible for the attached auditors' report, dated November 9, 2017, and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding KPMG'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 KPMG 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

Enlosure

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

INDEPENDENT AUDITORS' REPORT

Nancy A. Berryhill
Acting Commissioner
Social Security Administration:

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

- The consolidated balance sheets as of September 30, 2017 and 2016, and the related consolidated statements of net cost, changes in net position, and combined statements of budgetary resources for the years then ended, are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America (U.S. generally accepted accounting principles);
- The sustainability financial statements which comprise the statements of social insurance as of January 1, 2017 and 2016, and the statements of changes in social insurance amounts for the periods January 1, 2016 to January 1, 2017 and January 1, 2015 to January 1, 2016, are presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles;
- SSA maintained, in all material respects, effective internal control over financial reporting as of September 30, 2017, based on the criteria established in the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States;
- No instances of substantial noncompliance with the requirements of Section 803(a) of the *Federal Financial Management Improvement Act of 1996* (FFMIA); and
- No instances of noncompliance with certain provisions of laws, regulations, contracts, grant agreements, or other matters identified in our testing that are required to be reported under *Government Auditing Standards* issued by the Comptroller General of the United States or Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*.

The following sections discuss these conclusions in more detail.

REPORT ON THE FINANCIAL STATEMENTS AND INTERNAL CONTROL

We have audited the accompanying financial statements of the SSA, which comprise the consolidated financial statements and the sustainability financial statements (herein referred to as financial statements). The consolidated financial statements comprise the consolidated balance sheets as of September 30, 2017 and 2016, and the related consolidated statements of net cost, changes in net position, and combined statements of budgetary resources for the years then ended, and the related notes to the financial statements. The sustainability financial statements comprise the statements of social insurance as of January 1, 2017 and 2016, and the statements of changes in social insurance amounts for the periods January 1, 2016 to January 1, 2017 and January 1, 2015 to January 1, 2016, and the related notes to the sustainability financial statements.

We also have audited SSA's internal control over financial reporting as of September 30, 2017, based on the criteria established in the *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

KPMG

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

Management is responsible for the preparation and fair presentation of these financial statements in accordance with U.S. generally accepted accounting principles; 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 its assessment about the effectiveness of internal control over financial reporting, included in the Management Assurances Statements on page 34 of the Agency Financial Report (AFR).

Auditors' 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; in accordance with the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and in accordance with Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 17-03 require that we 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. 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 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 auditors' judgment, including the assessment of the risks 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.

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 U.S. generally accepted accounting principles. An entity'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 entity; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with U.S. generally accepted accounting principles, and that receipts and expenditures of the entity 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 entity'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 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.

Opinions

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, 2017 and 2016, and its net costs, changes in net position, and budgetary resources for the years then ended in accordance with U.S. generally accepted accounting principles.

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, 2017 and 2016, and the changes in its social insurance amounts for the periods January 1, 2016 to January 1, 2017 and January 1, 2015 to January 1, 2016, in accordance with U.S. generally accepted accounting principles.

Also, in our opinion, the Social Security Administration maintained, in all material respects, effective internal control over financial reporting as of September 30, 2017, based on the criteria established in the *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

Emphasis of Matter

As discussed in Note 18 to the financial statements, the sustainability financial statements are based on management's assumptions. These sustainability financial statements present the actuarial present value of SSA'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 or unsustainable debt levels. 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.

Other Matters

Accompanying Prior Period Financial Statements

The accompanying statements of social insurance as of January 1, 2015, January 1, 2014, and January 1, 2013, and the related notes to the financial statements, were audited by other auditors whose report, dated November 9, 2015, on those financial statements was unmodified and included an emphasis of matter paragraph that described that 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, as discussed in Note 18 to the 2015 financial statements.

Management Assurance Statements

We do not express an opinion or any form of assurance on management's statement referring to compliance with laws and regulations in the Management Assurances Statement on page 34 of the AFR.

Internal Control Over Financial Reporting

In accordance with *Government Auditing Standards*, we are required to report findings of significant deficiencies. 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. We consider the deficiencies in SSA's internal control described in the accompanying Exhibit I, Findings A – Certain Financial Information System Controls, B – Controls over the Reliability of Information Used in Certain Control Activities, and C – Accounts Receivable / Overpayments to be significant deficiencies.

SSA's response to the findings identified in our audit is presented on page 113 of the AFR. SSA's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Interactive Data

Management has elected to reference information on websites or other forms of interactive data outside the AFR to provide additional information for the users of its financial statements. Such information is not a required part of the basic financial statements or supplementary information required by the Federal Accounting Standards Advisory Board (FASAB). The information on these websites or the other interactive data has not been subjected to any of our auditing procedures, and accordingly we do not express an opinion or provide any assurance on it.

Required Supplementary Information

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis on pages 5 through 38 of the AFR, and Required Supplementary Information on pages 84 through 96 of the AFR be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the FASAB who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which 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 audits 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 of the financial statements 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 included on pages 2 through 4, 39-41, 80-83, and 115 through the end of the 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 audits of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

OTHER REPORTING REQUIRED BY *GOVERNMENT AUDITING STANDARDS*

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the SSA financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 17-03.

We also performed tests of its compliance with certain provisions referred to in Section 803(a) of the *Federal Financial Management Improvement Act of 1996* (FFMIA). 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 disclosed no instances in which SSA's financial management systems did not substantially comply with the (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Government Standard General Ledger at the transaction level.

Purpose of the Other Reporting Required by *Government Auditing Standards*

The purpose of the communication described in the Other Reporting Required by *Government Auditing Standards* section is solely to describe the scope of our testing of compliance and the result of that testing, and not to provide an opinion on compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

Washington, D.C.
November 9, 2017

A. Certain Financial Information System Controls

Social Security Administration (SSA) management relies on an automated information technology (IT) systems environment for administering and processing the Old-Age and Survivors Insurance (OASI), and Disability Insurance (DI) (collectively known as OASDI) programs, as well as the Supplemental Security Income (SSI) program and for financial statement reporting. Our internal control testing covered the General Information Technology Controls (GITC) of SSA's financially relevant applications and associated operating systems, databases, and infrastructure. GITCs provide the foundation for the integrity of systems including applications and the system software that comprise the general support systems for the major applications. GITCs, combined with IT application-level and manual controls, are critical to ensure accurate and complete processing of transactions and integrity of stored data. We also performed application control testing on IT systems and processes that were significant to the financial statements. Application controls include controls over data input, processing of data, and output of data, as well as interface, master file, and other user controls. These controls provide assurance over the data completeness, accuracy, and validity. The Government Accountability Office's *Federal Information System Controls Audit Manual* defines the objectives used to evaluate GITCs in five key control areas: the security management program, physical and logical access controls, configuration and change management, segregation of duties, and service continuity/contingency planning.

Criteria

Federal Information Processing Standards 200, *Minimum Security Requirements for Federal Information and Information Systems*, and National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, in combination, provide a framework for Federal agencies to apply to help ensure appropriate security requirements and controls to relevant IT systems. This framework includes agencies' organizational assessment of risk that validates the initial security control selection and determines whether additional controls are needed to protect organizational operations. The resulting set of security controls establishes a level of security due diligence for the organization.

The *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States, Principle No. 7, *Identify, Analyze, and Respond to Risk*s, provides requirements for the risk assessment process. Principle No. 7 states, in part, that management identifies risks throughout the entity to provide a basis for analyzing risks. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.

The *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States, Principle No. 11, *Design Activities for the Information System*, provides internal control requirements for IT systems the Government uses. Principle No. 11 states, in part, that management designs control activities over the IT infrastructure to support the completeness, accuracy, and validity of information processing by information technology. Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Security management includes access rights across various levels of data, operating system (system software), network, application, and physical layers. Management also designs control activities over access to protect an entity from inappropriate access and unauthorized use of the system.

The *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States, Principle No. 13, *Use Quality Information*, states, in part, that management designs a process that uses the entity's objectives and related risks to identify the information requirements needed to achieve the objectives and address the risks. Management processes relevant data from reliable sources into quality information within the entity's information system.

The *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States, Principle No. 17, *Evaluate Issues and Remediate Deficiencies*, states, in part, that management should remediate identified internal control deficiencies on a timely basis.

Conditions

We noted certain control deficiencies in the areas of IT oversight and governance, access controls, network security controls, and change and configuration management controls that, in aggregate, contribute to a repeat significant deficiency. The existence of these IT control deficiencies require SSA to place added dependency on manual controls to mitigate the risks of material misstatements to the financial statements. As SSA continues to automate processes to improve customer service and support its mission, their ability to continue to fully compensate for IT control deficiencies with manual controls, will become less feasible, and over time, may impact the reliability of financial and operational reports used by management.

IT Oversight and Governance:

Appropriate IT governance and oversight ensures risks are identified and assessed and controls are appropriately designed, implemented, and are operating effectively across the SSA's information systems and locations. Through the SSA's security management program, SSA's risk management framework should include continuous risk assessments, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures. We noted as part of our field testing that control deficiencies identified in prior audits continued to exist due to limited current fiscal year resources assigned to remediation efforts. SSA's organizational information security risk assessment and strategy did not fully consider risk framing, assumptions, tolerance, and constraints as well as Agency priorities and tradeoffs. We also noted that SSA's Program Operations Manual System (POMS) lacked certain control requirements and guidance over access controls and segregation of duties, and, therefore, we identified instances of inconsistent implementation and noncompliance with SSA policy. Therefore, personnel at the disability determination services (DDS) locations and the program service center (PSC) tested this year were not always aware of these control requirements.

Access Controls:

Access controls provide assurance that critical IT systems are physically safeguarded and logical access to sensitive applications, system utilities, and data is provided only when authorized. Weaknesses in such controls can compromise the integrity of data and increase the risk that data may be inappropriately accessed, or modified by unauthorized persons, affecting the accuracy of the financial statements. Our testing identified certain instances where documentation supporting the operation of controls related to the completion, review, and recertification of logical access authorization forms was not always available and certain other instances where users had inappropriate logical access to both the development and production change management environments for financially relevant applications, a production application dataset, and an application transaction. We also noted deficiencies related to physical access to certain computer rooms that housed the PSC and DDS servers and hardware. SSA had not always implemented optimal security settings in its production operating systems and databases supporting financial relevant applications to conform to industry and NIST guidance and SSA's defined risk profiles.

Network Security Controls:

Configuration and patch management processes are examples of critical components of an effective network security system because they prevent or detect weaknesses, such as misconfigurations, weak credentials, and unauthorized access. We identified certain configuration, patch management, and access control deficiencies with network security controls, many of which continued to exist from the prior year's audit. Information about these deficiencies are 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 to prevent the introduction of functional or security risks. Configuration management involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. A disciplined process for testing, approving, and migrating changes between environments, including into production, is essential to ensure systems operate as intended and there are no unauthorized changes to source code, data, and configuration settings. We noted instances where management did not fully comply with certain SSA's change management directives, policies, and procedures for the financial relevant systems managed by SSA Headquarters. In addition, we identified instances where security settings in financially relevant application platforms and DDS case processing system platforms did not always comply with SSA's risk models and security policies.

Cause

Although SSA remediated some prior-year findings and continued to develop corrective actions to remediate IT findings, our FY 2017 testing identified similar IT control deficiencies, mainly related to the lack of controls that would enforce compliance with existing directives, policies, and procedures. Many of the deficiencies continued to exist because management had not placed strategic emphasis on (1) identifying the root causes of the repeat IT control deficiencies, setting attainable milestones for corrective actions, and implementing controls that strengthen its existing internal control system to effectively identify, document, and link IT and business process controls to support financial reporting; (2) adequately assessing the design and operating effectiveness of essential IT controls; and (3) remediating IT control deficiencies, including those deficiencies related to lack of documentation, in a timely manner.

Effect

In addition to the effects summarized above within each sub-section, the aforementioned control deficiencies increase the risk to the completeness, accuracy, and integrity of certain SSA system-generated reports and may also affect the reliability of key application controls.

Recommendations

We recommend that SSA management:

1. Place strategic emphasis on identifying the root causes of the repeat access control, IT governance, and change and configuration management deficiencies; set attainable milestones for corrective actions; and remediate these deficiencies timely.
2. Design and implement controls to ensure SSA's employees comply with existing directives, policies, and procedures pertaining to access controls, IT governance, and change and configuration management.
3. Strengthen SSA's internal control system over access controls, IT governance, 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 IT controls; and remediating any identified IT control gaps.

B. Controls over the Reliability of Information Used in Certain Control Activities

Background

The IT control deficiencies discussed above elevate the risk that data produced by the SSA IT systems, also known as information produced by the entity (IPE), may not be complete or accurate. When management uses IPE in the performance of its manual process level controls, they must have reasonable confidence that the IPE is reliable for its intended purpose, and if necessary, add controls that compensate for information systems control deficiencies.

Criteria

The *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States, Principle No. 7, *Identify, Analyze, and Respond to Risk*s, provides requirements for the risk assessment process. Principle No. 7 states, in part, that management identifies risks throughout the entity to provide a basis for analyzing risks. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.

The *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States, Principle No. 13, *Use Quality Information*, states, in part, that management designs a process that uses the entity's objectives and related risks to identify the information requirements needed to achieve the objectives and address the risks. Management processes relevant data from reliable sources into quality information within the entity's information system.

Condition

We found that management did not design and implement effective controls to ensure that certain IPE used in the performance of manual process level controls in the areas of benefits due and payable and accounts receivable was complete and accurate. For example, SSA relies on IT system programs to produce the summary level information for accounts receivable where program parameters are not periodically tested to ensure resulting reports are accurate and complete for their intended purpose of supporting the quarterly accounts receivable and allowance for doubtful accounts receivable adjustments made to the financial statements.

Cause

SSA's risk assessment process did not identify completeness and accuracy of IPE resulting from the IT control deficiencies, identified above, as a risk that required additional compensating controls.

Effect

This condition could diminish the effectiveness of controls that are dependent on information produced by certain SSA IT systems and therefore, could lead to misstatements in benefits due and payable and accounts receivable financial statement amounts.

Recommendation

We recommend that SSA management strengthen SSA's risk assessment process by considering IT control deficiencies identified in prior years' self-assessment and audits to determine the sufficiency of internal controls over the completeness and accuracy of information in SSA's system generated reports. Such considerations should be documented. In addition, design and implement additional controls over the completeness and accuracy of information in SSA's system generated reports used in the performance of other controls, based on the results of SSA's risk assessment process.

C. Accounts Receivable / Overpayments

Background

Accounts receivable with the public consists primarily of overpayments made to beneficiaries beyond their entitled benefit. Public law and SSA policies require that beneficiaries notify SSA when there is a change in status that may affect their entitlement. However, proper, lawful, and timely notification to SSA does not always occur, resulting in the majority of overpayments. SSA depends on its processes and controls to detect overpayments, and calculate, record, and monitor the overpayments as an account receivable, and to facilitate timely collection. Beneficiaries who are found to be without fault in causing the overpayment, and are unable to repay the debt may be granted a waiver, permanently removing the debt from the accounts receivable balance. This process can be complex for some overpayments and waivers, and relies heavily on manual input and follow-up as well as adherence to SSA policies and procedures by a large number of people in SSA field offices and processing centers.

Criteria

The *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States, Principle No.10, *Design Control Activities*, provides the requirements for the design of internal controls over transactions and balances. Principle No. 10 states, in part, that management should document internal control, all transactions, and other significant events, in a manner that allows the documentation to be readily available for examination. Further, Principle No. 13, *Use Quality Information,* states management should use quality information to achieve the entity's objectives. Quality information is defined as being appropriate, current, complete, accurate, accessible, and timely.

Office of Management and Budget (OMB) Circular A-123, *Managements Responsibility for Enterprise Risk Management and Internal Control*, Appendix D, which incorporates by reference Circular A-127, *Financial Management Systems*, as revised, states that, financial events shall be recorded applying the requirements of the *U.S. Government Standard General Ledger* (USSGL). Application of the USSGL at the transaction level requires that approved transactions be recorded using appropriate general ledger accounts as defined in the USSGL guidance. Circular A-123, Appendix D also states that the agency financial management system shall be able to provide financial information in a timely and useful fashion to allow compliance with Federal accounting standards, and support fiscal management of program delivery and program decision making, including, as necessary, the requirements for financial statements prepared in accordance with the form and content prescribed by OMB.

Statement of Federal Financial Accounting Standard No 7, *Accounting for Revenue and Other Financing Sources*, as revised, states that nonexchange revenues 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 can be reasonably estimated.

Conditions

We noted certain control deficiencies in the area of accounts receivable/ overpayments that, in aggregate, contribute to a repeat significant deficiency.

Financial Accounting Process Related to Overpayments:

We noted that the subsidiary ledgers used to account for OASDI and SSI overpayments did not agree with the general ledger, and SSA lacked an internal control requiring routine reconciliation of subsidiary ledgers to the general ledger. In some cases, the data in multiple systems used to maintain information on overpayments did not agree and could not be reconciled. For example, the quarterly financial statement adjustments to account for overpayments are based on summary-level information that did not reconcile to the detailed list of individual debtor receivables at the transaction level.

Documentation Supporting Accounts Receivable / Overpayment Claims and Calculations:

We noted the following control deficiencies related to the maintenance of documentation to support overpayments, affecting the accuracy of accounts receivable reported in the financial statements:

- In approximately 48 percent of samples tested, we identified errors that affected the accuracy of the overpayment, including instances where we were unable to recalculate the overpayment based on the documentation maintained. A statistical projection of actual errors to the entire population of overpayment receivables was not material to the financial statements.
- In approximately 22 percent of samples tested, some or all of the documentation to support the existence of a claim could not be located. In a subset of exceptions identified, SSA agreed that the overpayment was uncollectible and should not have been reported as a receivable in the financial statements. We were unable to determine whether the uncollectible balances were included in SSA's allowance for doubtful accounts receivable, because SSA's method for assessing collectability is based on program receivables as a whole, and not at the individual account level. A statistical projection of actual errors to the entire population of overpayment receivables was not material to the financial statements.

Compliance with SSA Policies and Procedures Impacting Effectiveness of Internal Controls:

SSA has extensive policies and procedures as documented in the POMS, designed and implemented to account for overpayments, including the timely detection, pursuit, collection and waiver of overpayments. POMS provide effective guidance for use throughout SSA, including field offices, PSCs, DDSs, and elsewhere in SSA where accounting, quality review, and monitoring of overpayments is performed. We noted several instances where SSA and DDS employees did not fully comply with the POMS, including maintaining sufficient evidence to support a claim for overpayment or approval of waived overpayments. Collectively, these instances of non-compliance with SSA policies limit the effectiveness of internal controls over accounts receivable with the public, and SSA's ability to collect outstanding debts.

IT System Limitations Affecting Accuracy and Presentation of OASDI Accounts Receivable:

Overpayment balances due from beneficiaries are often repaid to SSA in monthly installments as deductions from monthly benefits. Payments of these installments can go beyond the year 2049. SSA has identified a Title II IT system limitation where receivable installment payments extending past December 31, 2049 are not tracked or reported, resulting in a potential understatement of accounts receivable, net of allowance for doubtful accounts receivable, in the financial statements for all receivables extending beyond 2049. SSA management has determined that the Title II systems limitation, and resulting understatement of accounts receivable are not material to the financial statements or accounts receivable. However, the Title II systems limitation does affect SSA's ability to accurately account for long-term accounts receivable and develop a true aging of amounts due for use in its allowance for doubtful accounts analysis.

Cause

SSA has experienced a steady growth in accounts receivable, in part due to a policy to maintain a record of overpayments for long periods. SSA intends to pursue collection of overpayments years or even decades later when beneficiaries apply for OASDI or additional SSI payments. The accounts receivable subsidiary ledger databases were designed to support operations and the management of the OASDI and SSI programs, but not necessarily for financial reporting. In addition, the IT systems used to track overpayment activity, such as new debt and collections, do not support full compliance with USSGL at the transaction level. Because of the IT systems limitations, and the structure of the databases, financial management has not been able to implement certain controls over accounts receivable.

Effect

Although the potential impact of these deficiencies, including the lack of supporting documentation, are not considered significant to the internal control system by management, these deficiencies could lead to misstatements in the financial statements, and affect management's ability to properly record, track, and collect outstanding overpayments.

Recommendations

We recommend that SSA perform the following to address the control deficiencies described above:

1. Implement a periodic control to reconcile the accounts receivable subsidiary ledgers to the general ledger, and ensure the financial statement balances are supported by a detailed listing of accounts receivable. Establish procedures to ensure the summary level information used to record accounts receivable is reconciled to a detailed list of individual debtor receivables at the transaction level. Investigate and resolve differences between the subsidiary ledgers, the summary level information and the general ledger timely.
2. Consider developing updated training for field and regional office personnel, related to obtaining and maintaining documentation necessary to support claims for overpayment and approval of waived overpayments, to improve compliance with existing policies and procedures.
3. Continue efforts to address the IT system limitations and improve functionality so that overpayment receivables, including those extending beyond year 2049, are accounted for and accurately presented in the financial statements, and better information related to overpayments is available for financial analysis.

4. Consider including a review of the overpayment process, IT systems used, and further evaluation of design and effectiveness of controls (addressing the deficiencies cited above), in the OMB Circular A-123 assessment plan for FY 2018.