AUDITORS' REPORT

November 9, 2016

The Honorable Carolyn W. Colvin
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) 2016 consolidated financial statements. This letter transmits the KPMG *Independent Auditors' Report* on the audit of SSA's FY 2016 consolidated financial statements. KPMG's report includes the following:

- Report on the Financial Statements, including the Opinions on the Consolidated Financial Statements and Sustainability Financial Statements;
- Report on Internal Control over Financial Reporting, including the Opinion on Management's Assertion About the Effectiveness of Internal Control; and
- Other Reporting Requirements Required by *Government Auditing Standards*.

OBJECTIVE OF A FINANCIAL STATEMENT AUDIT

KPMG conducted its audit of the consolidated financial statements and sustainability financial statements in accordance with auditing standards generally accepted in the United States; *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*. The objective of a financial statement audit is to obtain reasonable assurance that the financial statements are free of material misstatement. An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

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 predictions, and are not intended to imply that current policy or law is sustainable. 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.

In addition, KPMG examined management's assertion that SSA maintained effective internal control over financial reporting as of September 30, 2016, based on criteria established in the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States. KPMG conducted their examination in accordance with attestation standards established by the American Institute of Certified Public Accountants; the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and the internal control audit requirements included in OMB Bulletin No. 15-02. Those standards and OMB Bulletin No. 15-02 require that KPMG plan and perform the examination to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Their examination included assessing the risk that a material weakness exists, and testing and evaluating the design and operating effectiveness of internal control 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

Grant Thornton, LLP audited SSA's FY 2015 consolidated financial statements and the statements of social insurance as of January 1, 2011 through January 1, 2015, and issued an unmodified opinion on those statements. Grant Thornton, LLP also reported that SSA was maintaining effective internal control over financial reporting as of September 30, 2015 based on criteria under OMB Circular A-123, *Management's Responsibility for Internal Controls*, and the *Federal Manager's Financial Integrity Act of 1982*. However, Grant Thornton, LLP identified three significant deficiencies in internal controls: (1) Information Systems Controls, (2) Calculation, Recording, and Prevention of Overpayments, and (3) Redeterminations.

KPMG issued unmodified opinions on SSA's FY 2016 consolidated financial statements, and the sustainability financial statements as of January 1, 2016, and the changes in its social insurance amounts for the period January 1, 2015 to January 1, 2016. In addition, KPMG issued an unqualified opinion on management's assertion that SSA maintained effective internal control over financial reporting as of September 30, 2016 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 two significant deficiencies in internal controls: (1) Information Technology Systems Controls, and (2) Accounts Receivable/Overpayments. KPMG did not identify a significant deficiency in redeterminations.

SIGNIFICANT DEFICIENCY – INFORMATION TECHNOLOGY SYSTEMS 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. Specifically, KPMG's testing disclosed the following deficiencies.

1. **Threat and Vulnerability Management:** Weaknesses with cyber/network security controls during testing of threat and vulnerability management processes.
2. **IT Oversight and Governance:** Lack of an organizational information security risk assessment and strategy that considers risk framing, assumptions, tolerance, and constraints, as well as, agency priorities and tradeoffs. Further, it noted areas where sites had not implemented effective IT internal controls locally that adhered to SSA requirements, policies, and procedures. During site visits to one program service center, and five disability determination services, KPMG also noted a lack of oversight for decentralized information systems and locations, inconsistent implementation of SSA IT control requirements associated

with access controls, segregation of duties, change management, and a lack of risk management activities, including security assessment and authorization processes.

3. **Change and Configuration Management:** In the areas of change and configuration management, the program service center did not consistently implement SSA's change management directives, policies, and procedures. In addition, security baselines for the platforms supporting Old-Age, Survivors, and Disability Insurance (OASDI), Supplemental Security Income (SSI), financial reporting, and limitation on administrative expenses transactions did not follow applicable federal guidance and were not tailored to SSA's risk profile. KPMG also noted instances where security settings did not comply with SSA's risk models and security policies.

4. **Access Controls:** Control failures related to appropriate completion of logical access authorization forms, review and recertification of privileged and non-privileged access, and timely removal of logical access for applications processing OASDI, SSI, financial reporting, and limitation on administrative expenses transactions, as well as the case processing systems at the disability determination services. Additionally, KPMG noted deficiencies related to physical access to the computer rooms that housed the program service center and disability determination services servers and hardware.

SIGNIFICANT DEFICIENCY – ACCOUNTS RECEIVABLE/OVERPAYMENTS

In addition to the IT Systems Control significant deficiency, KPMG identified four deficiencies in internal control that, when aggregated, are considered to be a significant deficiency related to weaknesses in internal controls related to accounts receivable/overpayments. Specifically, KPMG's testing disclosed the following deficiencies.

1. **Financial Accounting Process and IT Systems Related to Overpayments:** 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 addition, KPMG identified control deficiencies related to the periodic testing of IT system programs to ensure accounts receivable information is accurate and complete.

2. **Documentation Supporting Accounts Receivable/Overpayment Claims and Calculations:** In approximately 30 percent of samples tested, KPMG identified errors that affected the accuracy of the overpayment. In addition, in approximately 25 percent of samples tested, KPMG identified some or none of the documentation to support the existence of a claim could be located.

3. **Compliance with SSA Policies and Procedures Affecting Effectiveness of Internal Controls:** Instances where SSA and Disability Determination Services employees did not fully comply with SSA policies, including retaining sufficient evidence to support a claim for overpayment.

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

KPMG identified no reportable instances of noncompliance 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 2016 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. 15-02;
- 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, 2016, 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, management's assertions about the 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
Acting Inspector General

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

INDEPENDENT AUDITORS' REPORT

The Honorable Carolyn W. Colvin
Acting Commissioner
Social Security Administration:

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

- The consolidated balance sheet as of September 30, 2016, and the related consolidated statements of net cost and changes in net position, and 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 (U.S. generally accepted accounting principles);
- The sustainability financial statements which comprise the statement of social insurance as of January 1, 2016, and the statement of changes in social insurance amounts for the period January 1, 2015 to January 1, 2016, are presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles;
- Management's assertion that SSA maintained effective internal control over financial reporting as of September 30, 2016 is fairly stated, in all material respects, 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. 15-02, *Audit Requirements for Federal Financial Statements*.

The following sections discuss these conclusions in more detail.

REPORT ON THE FINANCIAL STATEMENTS

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

Management's Responsibility for the Financial Statements

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

Auditors' Responsibility

Our responsibility is to express opinions on these financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and OMB Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 15-02 require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the 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 also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

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

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 SSA as of September 30, 2016, and its net cost, changes in net position, and budgetary resources for the year 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, SSA's social insurance information as of January 1, 2016, and the changes in its social insurance amounts for the period January 1, 2015 to January 1, 2016, in accordance with U.S. generally accepted accounting principles.

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 of the social insurance program. 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, and 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 this sustainability information do not consider changes in policy or all potential future events that could affect future income, future expenditures, and sustainability. 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 consolidated financial statements of SSA as of September 30, 2015 and for the year then ended, and the statements of social insurance as of January 1, 2015, January 1, 2014, January 1, 2013, and January 1, 2012, and the statement of changes in social insurance amounts for the period January 1, 2014 to January 1, 2015, 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.

Interactive Data

Management has elected to reference information on websites or other forms of interactive data outside the *Agency Financial Report* (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 44 of the AFR, and Required Supplementary Information on pages 94 through 106 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 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 audit was 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, 45 through 48, 88 through 93, and 123 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 audit of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING

We have examined management's assertion, included on page 40 of the AFR that SSA maintained effective internal control over financial reporting as of September 30, 2016, based on criteria established in the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States. SSA's management is

responsible for maintaining effective internal control over financial reporting, and for its assertion about the effectiveness of internal control over financial reporting, included on page 40 of the AFR. Our responsibility is to express an opinion on management's assertion based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants; the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and the internal control audit requirements included in OMB Bulletin No. 15-02. Those standards and OMB Bulletin No. 15-02 require that we plan and perform the examination to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our examination included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, and testing and evaluating the design and operating effectiveness of internal control based on the assessed risk. Our examination also included performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

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 evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, management's assertion that SSA maintained effective internal control over financial reporting as of September 30, 2016 is fairly stated, in all material respects, based on the criteria established in the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States.

In accordance with *Government Auditing Standards*, we are required to report findings of significant deficiencies. 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 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 described in the accompanying Exhibit I, Findings A – Information Technology Systems Controls, and B – Accounts Receivable/Overpayments to be significant deficiencies.

SSA's response to the findings identified in our examination is presented on page 122 of the AFR. We did not examine SSA's response and, accordingly, we express no opinion on the response.

We do not express an opinion, or any form of assurance, on management's assertion, included on page 40 of the AFR, referring to operations or compliance with laws and regulations.

This Report on Internal Control over Financial Reporting is intended solely for the information and use of SSA management, the SSA Office of the Inspector General, the OMB, the U.S. Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

KPMG

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. 15-02.

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 DC
November 9, 2016

Independent Auditors' Report
Exhibit I – Significant Deficiencies

A. Information Technology Systems Controls

Background

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 applications. As part of our testing, we performed IT security testing, penetration testing, and vulnerability assessments over the platforms that support relevant applications that process OASDI and SSI, financial reporting, and Limitation on Administrative Expenses transactions. 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 application-level 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 and the organization as a whole. Information Technology Application Controls (ITAC) include controls over input, processing of data, and output of data, as well as interface, master file, and other user controls. These controls provide assurance over the data completeness, accuracy, and validity. We performed our audit at SSA Headquarters, as well as one program service center (PSC) and five disability determination services (DDS).

Criteria

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. Additionally, Federal Information Processing Standards 200, *Minimum Security Requirements for Federal Information and Information Systems*, and National Institute of Standards and Technology Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, in combination, provide a framework to help ensure Federal agencies apply appropriate security requirements and controls to all IT systems. This framework includes agencies' organizational assessment of risk that validates the initial security control selection and determines whether any 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. 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.

Conditions

During our Fiscal Year (FY) 2016 testing of the significant SSA financial IT systems, we noted control deficiencies that, in aggregate, are a significant deficiency in the areas of threat and vulnerability management, IT oversight and governance, change and configuration management, and access controls.

Threat and Vulnerability Management:

Configuration, vulnerability, and patch management processes are critical components of an effective cyber security strategy because they prevent or detect weaknesses, such as misconfigurations, weak credentials, and vulnerabilities, are essential in combating internal and external cyber threats, exploitations, and unauthorized access. Our penetration testing, IT security testing, and vulnerability assessments identified control deficiencies with cyber/network security controls. Detailed information about these deficiencies or results of IT security testing have been reported in a separate, limited-distribution management letter.

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 Agency's information systems and locations. Through the Agency'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. SSA did not complete an organizational information security risk assessment and strategy that considers risk framing, assumptions, tolerance, and constraints as well as, Agency priorities and tradeoffs. An information security risk management assessment and strategy is critical in making risk-based decisions because without it SSA may not develop an effective risk management program. During our testing, we noted that five DDSs and one PSC had not implemented effective IT internal controls locally that adhered to SSA's Program Operations Manual System (POMS) and enterprise-wide policies and procedures. Specifically, we identified issues associated with security management, logical and physical access controls, segregation of duties, change and configuration management, and platform security. Furthermore, we noted that SSA's requirements and guidance were not sufficiently documented, which resulted in inconsistent implementation and noncompliance with SSA policy. We also noted a lack of oversight for decentralized information systems and locations; inconsistent implementation of SSA IT control requirements associated with access controls, segregation of duties, change management; and a lack of risk management activities, including security assessment and authorization processes at five DDSs and one PSC.

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. SSA's change management directives, and policies and procedures, were not consistently implemented at the PSC where we performed test procedures. SSA's security baselines for the platforms supporting relevant OASDI and SSI, financial reporting, and Limitation on Administration Expenses transactions did not follow applicable Federal guidance, and were not tailored to SSA's risk profile when specifying security option settings. In addition, we identified instances where security settings in financially relevant applications and DDS case processing system platforms did not comply with SSA's risk models and security policies.

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. We noted that SSA had identified mechanisms and processes to strengthen the controls to address deficiencies identified in prior years. However, our testing identified control failures related to appropriate completion of logical access authorization forms, review and

recertification of privileged and non-privileged access, and timely removal of logical access for applications processing OASDI and SSI, financial reporting, and Limitation on Administration Expenses transactions, as well as the case processing systems at the DDS locations. Additionally, we noted deficiencies related to physical access to the computer rooms that housed the PSC and DDS servers and hardware.

Cause

While SSA continued executing its risk-based approach to strengthen controls over its IT systems and databases, and addressing deficiencies identified in prior years, our FY 2016 testing identified control issues in both design and operation of key GITCs and ITACs. We believe that, in many cases, these deficiencies continued to exist because of one, or a combination, of the following.

- Risk mitigation strategies, and related control enhancements, require additional time for full implementation across SSA's network of key IT systems and databases.
- SSA focused its resources on higher risk weaknesses, and therefore, could not implement corrective actions for all aspects of the prior year deficiencies.
- The design and implementation of enhanced controls did not completely address risks and recommendations provided over past audits.
- Oversight and governance were not sufficient to address deficiencies.

Effect

The aforementioned IT control deficiencies pose a risk to the completeness, accuracy, and integrity of SSA's financial information. This could affect the reliability of key application controls and SSA's ability to produce accurate and timely financial statements.

Recommendations

We recommend that SSA management:

1. Address specific deficiencies noted in the IT security testing, penetration testing, and vulnerability assessments. As part of the Agency's threat and vulnerability management process, management should prioritize and implement risk mitigation strategies and plans of actions and milestones.
2. Design and implement effective IT internal controls that adhere to SSA's POMS and enterprise policies and procedures. Reassess and improve the existing technology oversight and governance processes to ensure guidance is completely documented, and SSA IT risk management control requirements are implemented effectively and consistently across the Agency, including DDSs and PSC locations, and compliance with policy is monitored.
3. Reassess and improve security configuration baselines and hardening guides against National Institute of Standards and Technology and applicable industry guidance, tailor them to SSA's risk profile, and specify how security options are to be set. Management should periodically develop and implement controls and processes to assess SSA's compliance with the improved security configuration baselines and hardening guides for production platforms across the Agency, including platforms processing OASDI, SSI, financial reporting, and Limitation on Administration Expenses transactions, as well as the platforms that support PSC and DDS applications.
4. Analyze account management controls, including logical and physical access authorization and review recertification and removal processes, to determine whether current controls mitigate the risk of unauthorized access to and modification of financial, personally identifiable information, and production data and computing resources. As part of these processes, management should improve controls over privileged accounts.
5. Complete user profile content reviews and profile improvement initiatives.

KPMG

B. 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, calculate, record, and monitor the overpayments as an account receivable, and to facilitate timely collection. This process can be complex for some overpayments, 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.

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

Financial Accounting Process and IT Systems Related to Overpayments:

We noted the following control deficiencies related to the financial accounting process and IT systems used to account for overpayments.

- 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.
- SSA relies on IT system programs to produce the summary level information 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 adjustment made to the financial statements. In addition, the quarterly financial statement adjustments to account for overpayments are based on summary-level information that is not reconciled to a 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 documentation maintained to support overpayments, affecting the accuracy of accounts receivable reported in the financial statements:

- In approximately 30 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 25 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 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 receivable type and not at the individual account level.

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

SSA had extensive policies and procedures as documented in the POMS, designed and implemented to account for overpayments, including the timely detection, pursuit, and collection of overpayments. POMS provides 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 the POMS, including maintaining sufficient evidence to support a claim for overpayment. 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 Accounts Receivable:

Overpayment balances can be large and 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 an IT system limitation where receivable installments extending past 2049 are not tracked, resulting in an understatement of accounts receivable in the financial statements for all receivables extending beyond 2049. SSA management has determined that the IT systems limitation, and resulting understatement of accounts receivable are not material to the financial statements or accounts receivable. However, the IT 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 the past 10 years, 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 impact of these control deficiencies, lack of supporting documentation, and IT system limitations, are not considered material to the financial statements by management, these deficiencies could lead to misstatements in the financial statements, and affects 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 and the general ledger timely.
2. Periodically test IT system programs that produce the summary level information used to support the quarterly adjustment to receivables, to ensure that resulting reports are accurate and complete for its intended purpose.
3. Consider developing updated training for field and regional office personnel, related to obtaining and maintaining documentation necessary to support claims for overpayment, to improve compliance with existing policies and procedures.
4. 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.
5. 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 2017.

SOCIAL SECURITY
The Commissioner

November 9, 2016

KPMG LLP
1801 K Street, NW
Washington, DC 20006

Ladies and Gentlemen:

We have reviewed the Independent Auditors' Report concerning your audit of our fiscal year (FY) 2016 financial statements. We are extremely pleased that we received our 23rd consecutive unmodified opinion on our financial statements, an unqualified opinion on management's assertion that our internal controls over financial reporting were operating effectively, and that we had no reportable instances of noncompliance with laws, regulations, or other matters tested.

Your report identified two significant deficiencies in your Report on Internal Control. We concur with the findings.

While we made significant progress to strengthen controls over our systems and to address the previously identified weaknesses, you identified control deficiencies that, in the aggregate, resulted in a significant deficiency in information technology (IT) systems controls. We remain committed to the continuous enhancement of our internal controls over IT systems. We will continue to pursue a risk-based corrective action plan to address the areas of threat and vulnerability management, IT oversight and governance, change and configuration management, and access controls.

Your report also identified certain deficiencies related to accounts receivable and overpayments that, when aggregated, you considered a significant deficiency. We will implement appropriate risk-based corrective actions to address your control deficiencies.

If members of your staff have any questions, they may contact Carla Krabbe at (410) 965-0759.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001