OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

November 12, 2019

The Honorable Andrew Saul
Commissioner

The Office of the Inspector General (OIG) contracted with the independent certified public accounting firm Grant Thornton LLP (Grant Thornton). Under the contract, Grant Thornton audited (1) SSA's consolidated financial statements as of September 30, 2019 and 2018; (2) the sustainability financial statements, including the statements of social insurance as of January 1, 2019, 2018, and 2015; (3) the statements of changes in social insurance amounts for the periods January 1, 2018 to January 1, 2019 and January 1, 2017 to January 1, 2018; (4) and the related notes to the sustainability financial statements. We also contracted with Grant Thornton to provide a report on internal control over financial reporting and noncompliance with laws, regulations, contracts, grant agreements, and other matters, including the requirements of the *Federal Financial Management Improvement Act of 1996*. The contract requires that the audit be performed in accordance with auditing standards generally accepted in the United States; *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements*. Those Standards and Bulletin require that Grant Thornton plan and perform the audits to obtain reasonable assurance about whether the financial statements are free from material misstatement and whether effective internal control over financial reporting was maintained in all material respects.

This letter transmits Grant Thornton's *Report of Independent Certified Public Accountants*. Grant Thornton found the following.

- The consolidated and sustainability financial statements are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America.
- SSA management maintained, in all material respects, effective internal control over financial reporting as of September 30, 2019. However, Grant Thornton identified three significant deficiencies in internal control: (1) Certain Financial Information Systems Controls, (2) Information Systems Risk Management, and (3) Accounts Receivable with the Public (Benefit Overpayments).
- No instances of noncompliance with laws, regulations, contracts, grant agreements and other matters.

OIG Evaluation of Grant Thornton Audit Performance

To fulfill our responsibilities under the *Chief Financial Officers Act of 1990* and related legislation for ensuring the quality of the audit work performed, we monitored Grant Thornton's audit of SSA's consolidated and sustainability financial statements by

- evaluating the independence, objectivity, and qualifications of the auditors and specialists;
- reviewing Grant Thornton's audit approach and planning;
- monitoring the audit's progress at key points;

- examining Grant Thornton's documentation related to planning the audit, assessing SSA's internal control, and substantive testing;
- reviewing Grant Thornton's audit report to ensure compliance with Government Auditing Standards and OMB Bulletin No. 19-03;
- coordinating the issuance of the audit report; and
- performing other procedures we deemed necessary.

Grant Thornton is responsible for the attached auditors' report, dated November 12, 2019, and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding Grant Thornton's performance under the contract terms. Our review, as differentiated from an audit in accordance with applicable auditing standards, was not intended to enable us to express, and, accordingly, we do not express, an opinion on SSA's consolidated financial statements; sustainability financial statements; internal control over financial reporting; or SSA's compliance with certain laws, regulations, contracts and grant agreements. However, our monitoring review, as qualified above, disclosed no instances where Grant Thornton did not comply, in all material respects, with applicable auditing standards.

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

Gail S. Ennis

Gail S. Ennis
Inspector General

GRANT THORNTON LLP
111 S. CALVERT ST., SUITE 2320
BALTIMORE, MD 21202
D 410 685 4000
F 410 837 0587
S linkd.in/grantthorntonus
twitter.com/grantthorntonus

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

Andrew Saul, Commissioner
Social Security Administration

Gail S. Ennis, Inspector General
Social Security Administration

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

- The consolidated balance sheets of SSA as of September 30, 2019 and 2018, the related consolidated statements of net cost and changes in net position, and the 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;

- The sustainability financial statements which comprise the statements of social insurance as of January 1, 2019, 2018 and 2015 and the statements of changes in social insurance amounts for the period January 1, 2018 to January 1, 2019 and January 1, 2017 to January 1, 2018 are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America;

- Although internal controls could be improved, SSA management maintained, in all material respects, effective internal control over financial reporting as of September 30, 2019; and

- No reportable instances of noncompliance for fiscal year 2019, with provisions of applicable laws, regulations, contracts, and grant agreements we tested.

The following sections discuss in more detail (1) our report on the financial statements and internal control over financial reporting which includes a matter of emphasis paragraph related to the sustainability financial statements, required supplementary information (RSI) and other information included with the financial statements, (2) our report on compliance with laws, regulations, contracts, and grant agreements, and (3) the Agency's response to findings.

Report on the financial statements and internal control over financial reporting

We have audited the accompanying financial statements of the Social Security Administration (the "Agency"), which comprise the consolidated financial statements and the sustainability financial statements. The consolidated financial statements comprise the consolidated balance sheets as of September 30, 2019 and 2018, and the related consolidated statements of net cost, changes in net position, and the combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements.

The sustainability financial statements comprise the statements of social insurance as of January 1, 2019, 2018, and 2015, the statements of changes in social insurance amounts for the periods January 1, 2018 to January 1, 2019 and January 1, 2017 to January 1, 2018, and the related notes to the sustainability financial statements.

We also have audited the internal control over financial reporting of the Social Security Administration as of September 30, 2019, based on criteria established under 31 U.S.C. § 3512 (c),(d) (commonly known as the *Federal Managers' Financial Integrity Act* or "FMFIA") and in *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

Management's responsibility for the financial statements and internal control over financial reporting

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of effective internal control over financial reporting relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error. Management is also responsible for evaluating the effectiveness of internal control over financial reporting based on the criteria established under FMFIA and its assessment about the effectiveness of internal control over financial reporting as of September 30, 2019, included in the accompanying Commissioner's Assurance Statement.

Auditor's responsibility

Our responsibility is to express opinions on these financial statements and an opinion on the entity's internal control over financial reporting based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget ("OMB") Bulletin 19-03, *Audit Requirements for Federal Financial*

Statements. Those standards and OMB Bulletin 19-03 require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement and whether effective internal control over financial reporting was maintained in all material respects.

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

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

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

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

Definition and inherent limitations of internal control over financial reporting

An entity's internal control over financial reporting is a process affected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America. An entity's internal control over financial reporting provides reasonable assurance that (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with accounting principles generally accepted in the United States of America, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition, and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority, regulations, contracts and grant agreements, noncompliance with which could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct, misstatements due to fraud or error. Also, projections of any assessment of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Agency's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Opinions on the financial statements

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the Social Security Administration as of September 30, 2019 and 2018, and its net cost, changes in net position, and budgetary resources for the years then ended, in accordance with accounting principles generally accepted in the United States of America.

Also, in our opinion, the sustainability financial statements referred to above present fairly, in all material respects the Social Security Administration's social insurance information as of January 1, 2019, 2018, and 2015 and its

changes in social insurance amounts for the periods January 1, 2018 to January 1, 2019 and January 1, 2017 to January 1, 2018, in accordance with accounting principles generally accepted in the United States of America.

Emphasis of matter

As discussed in Note 17 to the financial statements, the sustainability financial statements are based on management's assumptions. These sustainability financial statements present the actuarial present value of the Agency's estimated future income to be received and future expenditures to be paid using a projection period sufficient to illustrate long-term sustainability. The sustainability financial statements are intended to aid users in assessing whether future resources will likely be sufficient to sustain public services and to meet obligations as they come due. The statements of social insurance and changes in social insurance amounts are based on income and benefit formulas in current law and assume that scheduled benefits will continue after any related trust funds are exhausted. The sustainability financial statements are not forecasts or predictions. The sustainability financial statements are not intended to imply that current policy or law is sustainable. In preparing the sustainability financial statements, management considers and selects assumptions and data that it believes provide a reasonable basis to illustrate whether current policy or law is sustainable. Assumptions underlying such sustainability information do not consider changes in policy or all potential future events that could affect future income, future expenditures, and sustainability, for example, implementation of policy changes to avoid trust fund exhaustion. Because of the large number of factors that affect the sustainability financial statements and the fact that future events and circumstances cannot be estimated with certainty, even if current policy is continued, there will be differences between the estimates in the sustainability financial statements and the actual results, and those differences may be material. Our opinion is not modified with respect to this matter.

Opinion on internal control over financial reporting

In our opinion, although certain internal controls could be improved, the Social Security Administration maintained, in all material respects, effective internal control over financial reporting as of September 30, 2019, based on criteria established under 31 U.S.C § 3512 (c),(d) (commonly known as FMFIA) and in *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

As discussed in more detail, our Fiscal Year 2019 audit identified deficiencies in the Agency's controls over Certain Financial Information Systems Controls, Information Systems Risk Management and Accounts Receivable with the Public (Benefit Overpayments) described in the accompanying Appendix *Significant Deficiencies in Internal Control Over Financial Reporting*, that represent significant deficiencies in the Agency's internal control over

financial reporting. We considered these significant deficiencies in determining the nature, timing, and extent of our audit procedures on the Agency's Fiscal Year 2019 financial statements. Although the significant deficiencies in internal control did not affect our opinion on the Agency's Fiscal Year 2019 financial statements, misstatements may occur in unaudited financial information reported internally and externally by the Agency because of these significant deficiencies.

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

Other matters

The sustainability financial statements of the Agency as of and for the years ended January 1, 2017 and 2016 were audited by other auditors. Those auditors' report, dated November 9, 2017, expressed an unmodified opinion on those financial statements and included an emphasis of matter paragraph that describe the assumptions upon which the sustainability financial statements are based discussed in Note 17 to the financial statements.

Required supplementary information
Accounting principles generally accepted in the United States of America require that the information in Management's Discussion and Analysis from pages 5 to 37 and the combining schedule of budgetary resources and the required supplementary social insurance information from pages 91 to 103 be presented to supplement the basic financial statements. Such information, although not a required part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board and OMB Circular A-136, *Financial Reporting Requirements*, which consider it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. Management is responsible for preparing, measuring, and presenting the required supplementary information in accordance with accounting principles generally accepted in the United States of America. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America. These limited procedures consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of

the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other information
Our audits were conducted for the purpose of forming an opinion on the basic financial statements as a whole. The Commissioner's Message on page 1 and the other information on pages 2 through 4, 39 through 43, 87 through 90 and 123 through 230 are presented for purposes of additional analysis and are not a required part of the basic financial statements. Management is responsible for preparing and presenting other information included in documents containing the audited financial statements and auditor's report, and for ensuring the consistency of that information with the basic financial statements and the required supplementary information. We read the other information in order to identify material inconsistencies, if any, with the basic financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Report on compliance with laws, regulations, contracts, grant agreements and other matters

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

Management's responsibility
Management is responsible for complying with laws, regulations, contracts, and grant agreements applicable to the Agency.

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

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

on compliance with laws, regulations, contracts, and grant agreements applicable to the Agency. Accordingly, we do not express such an opinion.

Under the Federal Financial Management Improvement Act ("FFMIA"), we are required to report whether the Agency's financial management systems substantially comply with FFMIA Section 803(a) requirements. To meet this requirement, we performed tests of compliance with the federal financial management systems requirements, applicable federal accounting standards, and the *United States Standard General Ledger* ("USSGL") at the transaction level. However, providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly we do not express such an opinion. The results of our tests of FFMIA Section 803(a) requirements disclosed no instances of substantial noncompliance that are required to be reported under FFMIA.

Agency's response to findings
The Agency's response to our findings, which is included on page 121 of this Agency Financial Report, was not subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on the Agency's response.

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

Grant Thornton LLP

Baltimore, Maryland
November 12, 2019

APPENDIX – SIGNIFICANT DEFICIENCIES IN INTERNAL CONTROL OVER FINANCIAL REPORTING

Significant Deficiency in Internal Control over Certain Financial Information Systems Controls

Overview

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

Our internal control testing covered both IT general and application controls. IT general controls testing encompassed the security management program, access controls (physical and logical), configuration and change management, segregation of duties, and service continuity/contingency planning. IT general controls provide the foundation for the integrity of systems including applications and the system software that comprise the general support systems for the major applications. General and application-level controls are critical to ensuring the accurate and complete processing of transactions and integrity of stored data. Application controls include application-specific general controls, input, processing of data, and output of data as well as interface, master file, and other user controls. These controls provide assurance over the completeness, accuracy, and validity of data. Our audit included testing of the Agency's mainframe, networks, databases, applications, and other supporting systems and was conducted at Headquarters as well as off-site locations.

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

Deficiencies in Control Design and/or Operational Effectiveness

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

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

Access Controls

Access controls provide assurance that critical information systems' assets are physically safeguarded and logical access to sensitive applications, system utilities, and data are provided only when authorized and appropriate. Weaknesses in such controls can compromise the integrity of data and increase the risk that such data may be inappropriately accessed and/or disclosed as well as modified by unauthorized persons, which may affect the accuracy of the financial statements. Our testing identified control failures related to account management controls including access authorizations, recertification of access, and the timely removal of logical access after termination. We noted issues with segregation of duties, privileged access, the review of disability determination services user profile content, and the review of security violation reports and additional audit logs. Further, we noted exceptions related to controls to prevent programmer access to the production environment. More specifically, SSA implemented a secondary user ID process to allow programmers access to production data through a highly monitored, time-limited process. During testing, we determined this control was not operating effectively, as approvals and reviews of the access were not performed timely. Finally, we identified physical security control weaknesses that potentially allowed unauthorized individuals access to non-sensitive areas.

Network Security Controls

Configuration, vulnerability, and patch management processes are examples of critical components to effective network security. Related processes and controls must be designed to prevent or detect such weaknesses as misconfigurations, weak credentials, and vulnerabilities and are essential in

combating internal and external cyber-threats, exploitations, and unauthorized access. We identified certain inventory, patch management, and network security deficiencies, many of which persisted from prior audits. We present information about these deficiencies in a separate management letter.

Configuration Management

Configuration management involves the identification and management of security features for hardware, software, and firmware components of an information system at a given point while controlling changes to that configuration as part of the systems' life cycle. A disciplined process is required so configurations align with security standards and to ensure no unauthorized changes are implemented to configuration settings. We noted instances where configurations were not monitored or aligned with best practices or SSA's standards. In addition, we noted SSA needed to improve its controls over (1) establishing comprehensive security configuration baselines; (2) reviewing security configurations periodically; (3) hardening security guides; (4) adhering to these baselines and guides through periodic monitoring; and (5) assessing, remediating, and/or approving deviations (if applicable).

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

Recommendations

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

1. Analyze the audit findings to identify root causes and trends, assess risk of control failures, and re-evaluate priorities for remediation. SSA should develop and/or review its risk-based approach and develop a roadmap of corrective actions. SSA should set attainable milestones for corrective actions and remediate these deficiencies timely.
2. Strengthen SSA's internal control system for access controls, network security, and configuration management to improve its effectiveness in identifying, documenting, and linking these controls to business processing controls that support financial reporting; assessing the design and effectiveness of these controls; and remediating any identified IT control gaps.

Significant Deficiency in Information Systems Risk Management

Overview

A dynamic, flexible, and robust information system/IT risk management program is essential to manage security and privacy risk in SSA's diverse IT environment. As threats evolve and become more sophisticated, complex, and numerous, appropriate risk management is required to build security into new systems, mitigate existing and emerging threats, and ensure that essential mission support services are available. Further, it is needed to protect the confidentiality, integrity, and availability of SSA's financial and program information.

SSA must implement a risk management program that provides reasonable assurance that risks are identified and assessed, that controls are appropriately designed, and operating effectively across the Agency's information systems and locations. Through the Agency's security management program, SSA's risk management framework must include a continuous cycle of activity for developing and assessing the discipline and structure of its control environment, assessing risk, developing and implementing effective security procedures, communicating, and monitoring the effectiveness of those procedures.

IT risk management also must be integrated, deployed, and communicated throughout the entity, divisions, operating units and functions. SSA executive oversight, management and personnel are all responsible for information security and privacy. OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* provides implementation guidance to Federal agencies for meeting risk management reporting requirements. The memorandum states: "An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include…cyber…and a broad range of operational risks such as information security…Effective management of cybersecurity risk requires that agencies align information security management processes with strategic, operational, and budgetary planning processes…."

Deficiencies in Control Design and/or Operational Effectiveness

In Fiscal Year 2018, we noted deficiencies in IT oversight and governance, which had first been cited in Fiscal Year 2014 as part of the aggregated information system controls significant deficiency. We noted as part of our field work that issues persisted from past audits because of limited remediation of root causes. In addition, because of additional factors identified in the current year as part of our fieldwork at disability determination services and regional offices including an increase in the pervasiveness of prior year issues, failures noted with certain site's

demonstration of integrity, oversight, and responsibility for their control environment, and to highlight this issue is not isolated to IT departments, we decided to extract the IT oversight and governance component of the aggregated significant deficiency into a stand-alone significant deficiency.

In Fiscal Year 2019 we noted recurring issues, in regards to processes, people and technology in place to support SSA's IT risk management function. More specifically:

- Process – We noted SSA's processes lacked the following.
    - Repeatable and standardized risk management practices that were consistently applied and implemented across the organization at the entity, divisions, operating units and functions. For example, we noted several instances where SSA divisions, regional offices and disability determination services personnel did not document internal control design, retain evidence of control execution, and/or evidence of monitoring controls. We cited control deficiencies related to the completeness and accuracy of information system inventories and boundaries, common control inheritance considerations, and a lack of completed requirements within security assessment and authorization packages.
    - A clear and concise security architecture function. Specifically, SSA did not consistently implement an information security architecture across the enterprise, business processes, and system levels necessary for maintaining a disciplined and structured methodology for managing risk.
    - A proactive process to identify, block and/or remove unauthorized software and executable code, as well as, appropriate execution of the risk management function in the Agency's system development life cycle.
- People – Per the *Standards for Internal Control in the Federal Government* OV1.06, "People are what make internal control work. Management is responsible for an effective internal control system. As part of this responsibility, management sets the entity's objectives, implements controls, and evaluates the internal control system. However, personnel throughout an entity play important roles in implementing and operating an effective internal control system." We noted as part of our field work that SSA lacked information security resources at various levels within the organization to effectively implement IT risk management functions. In addition, we noted instances where SSA and disability determination services personnel were not aware of *Standards for Internal Control in the Federal Government* requirements and requirements to document control design and activities as well as retain evidence of their execution. Finally, we

noted SSA had not adequately identified individuals with significant information security responsibilities to provide role based security training.

- Technology – We noted that SSA did not consistently and/or effectively deploy technology to manage its IT risk management function. SSA has made progress in this area but was still implementing and/or tuning software in many instances. For example, we noted issues with information system hardware and software inventory management, a lack of network access control, automation and tools for managing security configurations, and comprehensive tools to evaluate and communicate risks.

These findings did not have a material impact on the financial statements; however, they could have such negative effects as inaccurate security categorization of systems and applications; ineffective identification, implementation and documentation of required controls; inappropriate testing and monitoring of those controls; and approving authorization to operate packages for the system without an appropriate understanding of risks.

Recommendations

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

1. Revise existing information system risk management framework(s) and strategy, using NIST 800-37 Rev. 2 “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy” to consistently apply risk management practices throughout the Agency. In addition, develop and implement a consistent approach to risk management within its security architecture and system development life cycle processes.
2. Review and revise existing organizational structures to deploy information security resources at various levels within the organization to implement and monitor SSA’s revised risk management practices and provide the appropriate level of recurring training to individuals with internal control and information security responsibilities.
3. Review its current governance, risk, and compliance tools and software and consider additional tools and automation within its risk management practices and security controls.

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

Overview

When SSA beneficiaries receive payments beyond their entitled amount, a benefit overpayment exists. When SSA detects an overpayment, SSA records an accounts receivable with the public to reflect the amount due SSA from the beneficiary. Because of the nature of the benefit-payment programs, SSA has extensive operations geographically dispersed throughout the United States. Overpayment detection, calculation, and documentation can take place in various places, including approximately 1,200 field offices, 8 Processing Centers, or various function areas within the SSA central office. Therefore, SSA has specific policies, procedures, and internal controls in place to consistently detect, calculate, and document overpayments and the related accounts receivable balances. Since this process can be complex for some cases and relies on manual input, SSA's adherence to its internal controls is critical to accurately recording, documenting, and tracking overpayment balances. Management also relies on its IT infrastructure, interfaces, and controls to record and prevent erroneous payments.

Reconciliation of Accounts Receivable Ledgers

Office of Management and Budget (OMB) Circular A-123, Appendix D, *Compliance with Federal Financial Management Improvement Act*, requires application of the U.S. Government Standard General Ledger at the transaction level. For both its OASDI and SSI programs, SSA tracks individual debtor overpayment transactions and accounts receivable balances in subsidiary ledger systems and adjusts the general ledger according to the balances reported from the subsidiary ledgers. SSA implemented a new OASDI accounts receivable reconciliation process in Fiscal Year 2019 that has operated effectively in reconciling its OASDI accounts receivable subsidiary ledger activity to the general ledger. However, consistent with prior years, our testing revealed that the detail level beneficiary information in the SSI accounts receivable subsidiary ledger did not agree with the summary-level reports from the SSI subsidiary ledger.

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

System limitations prevent SSA from reconciling the SSI differences between the detail and summary-level information within the subsidiary ledger.

However, the unreconciled differences are immaterial to the financial statements and the accounts receivable with the public line items.

Deficiencies in Overpayment Documentation and Calculations

We noted that prior audits identified significant deficiencies in internal controls related to SSA adhering to Program Operations Manual System criteria regarding maintaining sufficient evidence to support overpayments balances or sufficient evidence to support approval of waived overpayments. Program Operations Manual System provides important policies, procedures, and internal controls over processing and documenting overpayments. Based on evidence obtained during our business process walkthroughs, we determined in Fiscal Year 2018 that SSA had developed updated training for field and regional office personnel on obtaining and maintaining documentation necessary to support claims for overpayments and approval of waived overpayments.

However, based on inquiry with management, the timing of training deployment and time needed for the training to effectuate through the internal control environment, prevented improvements to be yielded in Fiscal Year 2019. Additionally, our internal control testing of overpayments waived in the current fiscal year continued to demonstrate insufficient documentation of waiver approvals as well as insufficient documentation of initial overpayment records. Therefore, we did not test a separate sample of new overpayments identified in Fiscal Year 2019 for internal control effectiveness. Insufficiently following established policy and lack of documentation to support overpayments can lead to difficulties in calculating and substantiating outstanding accounts receivable balances and potential misstatements to accounts receivable with the public balance presented on the financial statements.

In addition, we selected a statistical sample of outstanding OASDI and SSI overpayment balances and noted overpayment calculation errors in 5 (16 percent) of 31 sampled OASDI items. Although the statistically projected impact of these calculation errors was not material to the financial statements, these errors further evidence control weaknesses in the accounts receivable with the public processes, including inappropriate overpayment tracking that could lead to misstatements in the financial statements.

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

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

According to Statement of Federal Financial Accounting Standards (SFFAS) 1, *Accounting for Selected Assets and Liabilities*, a receivable should be recognized when a federal entity establishes a claim to cash or other assets against other entities, either based on legal provisions, such as a payment due date, (e.g., taxes not received by the date they are due), or goods or services provided. If the amount is unknown, a reasonable estimate should be made. Further SFFAS 7, *Accounting for Revenue and Other Financing Sources and Concepts for Reconciling Budgetary and Financial Accounting* states that accounts receivable should be recognized when a collecting entity establishes a specifically identifiable, legally enforceable claim to cash or other assets through its established assessment processes to the extent the amount is measurable.

We noted that SSA identified a system design process limitation concerning long-term withholding agreements that extend past December 2049 where the system cannot capture and track debt scheduled for collection beyond December 2049. Therefore, the accounts receivable balances related to these overpayments are understated in the amount of the installment payments expected to be collected beyond December 2049. The projected understatements are immaterial to the financial statements and the accounts receivable with the public balance. While the Agency is enhancing system capabilities to properly account for these receivables and updating policies to avoid longer-term repayment programs, failure to resolve the system design process limitation will continue to understate accounts receivable balances. In addition, the impact of this issue will continue to grow as December 2049 approaches if other factors remain constant.

Recommendations

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

Reconciliation of Accounts Receivable Ledgers

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

Deficiencies in Overpayment Documentation and Calculations

1. Continue exploring opportunities to improve overpayment accuracy and document retention through engaging field office and payment center employees in trainings related to common weaknesses and more complex overpayment cases.

2. Enhance management review of overpayment processing considering risk based factors such as current overpayment balances, manual intervention required, and age.
3. Consider implementation of new overpayment documentation tools to ensure overpayments are documented completely, accurately, and timely by field offices or Processing Centers within the appropriate systems of record.

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

1. Continue working toward updated debt management systems without the technical limitations over the length of time repayment installments can be recorded.
2. Continue pursuing changes in repayment policy to minimize future extended repayment plans.
3. Continue analyzing and tracking the impact of the December 2049 system design process limitation on the financial statements.