REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

November 10, 2022

The Honorable Kilolo Kijakazi
Acting Commissioner of Social Security

The Office of the Inspector General (OIG) contracted with the independent certified public accounting firm Grant Thornton LLP (Grant Thornton) to audit: (1) the Social Security Administration's (SSA) consolidated financial statements as of September 30, 2022 and 2021 and the related notes to the consolidated financial statements; (2) the sustainability financial statements, including the statements of social insurance as of January 1, 2022, 2021, 2020, 2019 and 2018, and the related notes to the sustainability financial statements; and (3) the statements of changes in social insurance amounts for the periods January 1, 2021 to January 1, 2022 and January 1, 2020 to January 1, 2021. The OIG also contracted with Grant Thornton to provide an opinion on internal control over financial reporting and report on compliance with laws, regulations, contracts, grant agreements, and other matters and to report on whether SSA's financial management systems did not comply substantially with the requirements of the *Federal Financial Management Improvement Act of 1996 (FFMIA)*. The contract requires that the audit be conducted 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 Bulletin No. 22-01, *Audit Requirements for Federal Financial Statements*. Those Standards and Bulletin require that Grant Thornton plan and perform the audits to obtain reasonable assurance about whether the financial statements are free from material misstatement and whether effective internal control over financial reporting was maintained in all material respects.

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.
- SSA management maintained, in all material respects, effective internal controls over financial reporting as of September 30, 2022, based on criteria established under the *Federal Managers' Financial Integrity Act and in Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States. However, Grant Thornton identified three significant deficiencies in internal controls: (1) Certain Financial Information Systems Controls, (2) Information Systems Risk Management, and (3) Accounts Receivable with the Public (Benefit Overpayments).
- No instances in which SSA's financial management system did not comply substantially with the requirements of FFMIA.

- No reportable instances of noncompliance with provisions of applicable laws, regulations, contracts, grant agreements, and other matters tested.

OFFICE OF THE INSPECTOR GENERAL 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 auditors' and specialists' independence, objectivity, and qualifications;
- 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 Office of Management and Budget Bulletin No. 22-01;
- coordinating the issuance of the audit report; and
- performing other procedures we deemed necessary.

Grant Thornton is responsible for the attached auditors' report, dated November 10, 2022, 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 conclusions on whether SSA's financial management systems complied substantially with FFMIA; or compliance with provisions of 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
Inspector General

GRANT THORNTON LLP
111 South Calvert Street, Suite 2320
Baltimore, MD 21202

D 410 685 4000
F 410 837 0587

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

Kilolo Kijakazi, Acting 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, 2022 and 2021, 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, 2022, 2021, 2020, 2019 and 2018 and the statements of changes in social insurance amounts for the period January 1, 2021 to January 1, 2022 and January 1, 2020 to January 1, 2021 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, 2022; and
- No reportable instances of noncompliance for fiscal year 2022, 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 an emphasis of matter paragraph related to the sustainability financial statements, and 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

Opinions on the financial statements

We have audited the consolidated 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, 2022 and 2021, 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 financial statements.

The sustainability financial statements comprise the statements of social insurance as of January 1, 2022, 2021, 2020, 2019 and 2018, the statements of changes in social insurance amounts for the periods January 1, 2022 to January 1, 2021 and January 1, 2020 to January 1, 2021, and the related notes to the sustainability financial statements.

In our opinion, the accompanying consolidated financial statements present fairly, in all material respects, the financial position of the Agency as of September 30, 2022 and 2021, 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 accompanying sustainability financial statements present fairly, in all material respects the Agency's social insurance information as of January 1, 2022, 2021, 2020, 2019, and 2018 and its changes in social insurance amounts for the periods January 1, 2022 to January 1, 2021 and January 1, 2020 to January 1, 2021, in accordance with accounting principles generally accepted in the United States of America.

Opinion on internal control over financial reporting

We also have audited the internal control over financial reporting of the Agency as of September 30, 2022, 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.

In our opinion, although certain internal controls could be improved, the Agency maintained, in all material respects, effective internal control over financial reporting as of September 30, 2022, based on criteria established under 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 2022 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 collectively represent the 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 2022 financial statements. Although the significant deficiencies in internal control did not affect our opinions on the Agency's 2022 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.

Basis for opinions

We conducted our audits in accordance with auditing standards generally accepted in the United States of America (US GAAS); the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States (*Government Auditing Standards)*; and Office of Management and Budget ("OMB") Bulletin 22-01, *Audit Requirements for Federal Financial Statements*. Our responsibilities under those standards and OMB Bulletin 22-01 are further described in the Auditor's Responsibilities for the Audits of the Financial Statements and Internal Control Over Financial Reporting section of our report. We are required to be independent of the Agency and to meet our other ethical responsibilities in accordance with the relevant ethical requirements relating to our audits. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinions.

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.

Responsibilities of management for the financial statements and internal control over financial reporting

Management is responsible for the preparation and fair presentation of the consolidated financial statements and sustainability financial statements in accordance with accounting principles generally accepted in the United States of America and for 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 assessing 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, 2022, included in the accompanying Acting Commissioner's Assurance Statement.

Auditor's responsibilities for the audit of the financial statements and internal control over financial reporting

Our objectives are to obtain reasonable assurance about whether the consolidated financial statements and sustainability financial statements as a whole are free from material misstatement, whether due to fraud or error, and about whether effective internal control over financial reporting was maintained in all material respects, and to issue an auditor's report that includes our opinions.

Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with US GAAS, *Government Auditing Standards,* and OMB 22-01 will always detect a material misstatement or a material weakness when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the consolidated financial statements or sustainability financial statements.

In performing an audit of financial statements and an audit of internal control over financial reporting in accordance with US GAAS, Government Auditing Standards, and OMB 22-01, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit.
- Identify and assess the risks of material misstatement of the consolidated financial statements and sustainability financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements and sustainability financial statements.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances.
- Obtain an understanding of internal control over financial reporting relevant to the audit of internal control over financial reporting, assess the risks that a material weakness exists, and test and evaluate the design and operating effectiveness of internal control over financial reporting based on the assessed risk.
- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the consolidated financial statements and sustainability financial statements.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control-related matters that we identified during the audit.

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

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

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

Required supplementary information
Accounting principles generally accepted in the United States of America require that the information in Management's Discussion and Analysis from pages 5 to 36 and the combining schedule of budgetary resources, and the required supplementary social insurance information from pages 90 to 102 be presented to supplement the consolidated financial statements and sustainability financial statements. Such information is the responsibility of management and, although not a required part of the consolidated financial statements and sustainability 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 consolidated financial statements and sustainability financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with US GAAS. 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 consolidated financial statements and sustainability financial statements, and other knowledge we obtained during our audit of the consolidated financial statements and sustainability 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
Management is responsible for the other information included in the annual report. The other information comprises the Acting Commissioner's Message on page 1 and the other information on pages 2 through 4, 37 through 42, 86 through 89, and 120 through 178, but does not include the consolidated financial statements, sustainability financial statements and our auditor's report thereon. Our opinions on the consolidated financial statements and sustainability financial statements do not cover the other information, and we do not express an opinion or any form of assurance thereon.

In connection with our audit of the consolidated financial statements and sustainability financial statements, our responsibility is to read the other information and consider whether a material inconsistency exists between the other information and the consolidated financial statements and sustainability financial statements, or the other information otherwise appears to be materially misstated. If, based on the work performed, we conclude that an uncorrected material misstatement of the other information exists, we are required to describe it in our report.

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

As part of obtaining reasonable assurance about whether the Agency's financial statements are free from material misstatement, we performed tests of its compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements consistent with the auditor's responsibility discussed below, in accordance with *Government Auditing Standards*.

Results of our tests of compliance
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.

Basis for results of our tests of compliance
We performed our tests of compliance in accordance with auditing standards generally accepted in the United States of America; *Government Auditing Standards*; and OMB Bulletin No. 22-01.

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

Auditor's responsibilities for tests of compliance
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 financial statements, and to perform certain other limited procedures. We did not

test compliance with all laws, regulations, contracts, and grant agreements. Noncompliance may occur that is not detected by these tests.

Agency's response to findings
Government Auditing Standards requires the auditor to perform limited procedures on the Agency's response to the findings identified in our audit and described on page 119 of this Agency Financial Report. The Agency's response was not subjected to the other auditing procedures applied in the audit of the consolidated financial statements and sustainability financial statements, and accordingly, we express no opinion on the Agency's response.

Intended purpose of report on compliance
The purpose of this report is solely to describe the scope of our testing of compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements, 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 10, 2022

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 technology (IT) to administer 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.

Our internal control testing included IT general and application controls. Testing IT general controls 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. Our audit was conducted for 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 in the *Federal Information Security Modernization Act of 2014*. These standards, combined with National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, *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 that could result 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 deficiencies in access controls, network security controls, and configuration management that contributed 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. SSA has developed several plans, strategies, and initiatives to address control deficiencies; however, these deficiencies continued to exist because of one, or a combination, of the following:

- SSA was in the process, but had not fully implemented, automated mechanisms for monitoring compliance with key control activities as well as within their security assessment and authorization processes;
- SSA had not remediated control deficiencies noted in prior audits; and
- the design of enhanced or newly designed controls had not completely addressed risks identified 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, modified, and/or disclosed by unauthorized persons, which may affect the accuracy of the financial statements. Our testing identified weaknesses related to logical access controls at disability determination services (DDS), including logical access policy and procedures and segregation of duties issues. We also noted physical access control weaknesses related to physical access reviews/recertification. Our testing at SSA Headquarters identified control weaknesses related to the identification and review of logical access for privileged users and removal of mainframe profiles with access to financial datasets. At Headquarters, SSA implemented a secondary user identification process to give programmers access to production data through a monitored, time-limited process. During testing, we determined this control was not operating effectively, as SSA was not reviewing and approving the access timely. Finally, we identified control weaknesses related to the timely removal of logical access for separated SSA personnel.

Network Security Controls

Critical components of effective network security controls include, but are not limited to, configuration management, limiting access based on need-to-know/least privileged, and logging and monitoring sensitive activities. Related processes and controls must be designed to prevent or detect such weaknesses as misconfigurations and vulnerabilities to combat internal and external cyber-threats, exploitations, and unauthorized access. We identified network security and inventory deficiencies, many of which persisted from prior audits.

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 system's 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 SSA needed to improve its controls over (1) hardening security configuration baselines (that is, providing prescriptive guidance on deploying and operating IT securely); (2) determining adherence to these baselines and guides through periodic monitoring; and (3) assessing, remediating, and/or justifying, and approving deviations (if applicable).

While these findings did not have a material impact on the financial statements, a lack of appropriately designed or implemented internal controls for information systems and technology increases the risk of unreliable data and misstatements whether due to fraud or error.

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 weaknesses, 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 identified IT control gaps.

Grant Thornton Response

Grant Thornton reviewed the additional context provided in management's response on page 119 of this Agency Financial Report. Management's response does not affect the assessment of the significant deficiency.

Significant Deficiency in Information Systems Risk Management

Overview

A dynamic, flexible, and robust information system and technology risk management program is essential to managing 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 essential mission support services are available. Further, IT risk management 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 and 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 must also be integrated, deployed, and communicated throughout the entity, divisions, operating units, and functions. SSA executive oversight, management, and personnel are responsible for information security and privacy. Office of Management and Budget (OMB) Circular Number A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, states:

> *Risk management is a series of coordinated activities to direct and control challenges or threats to achieving an organization's goals and objectives. ERM is an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos….*

Deficiencies in Control Design and/or Operational Effectiveness

We noted improvement in SSA's communication of IT risks and control requirements across its offices and its commitment to integrity and oversight of internal controls. For example, SSA implemented a security review board to assess control deficiencies and prioritize remediation, implemented a compliance dashboard, deployed Information System Security Officers (ISSO) strategically throughout its organization, and implemented procedures for performing oversight and monitoring of some DDS control requirements. However, we continue to identify recurring issues regarding processes, people, and technology in place to support SSA's IT risk management function that persist from prior audits.

- Processes – 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, there were control weaknesses related to regional office security assessment and authorization processes; performance of risk assessments; implementation of NIST SP 800-53, revision 5, requirements; and issuance and monitoring of plans of action and milestones (POA&M). Furthermore, as part of our Headquarters testing, we cited control deficiencies related to the information security monitoring and enforcement for contractor systems, control weaknesses in the vulnerability management program, completeness and accuracy of information system inventories and system boundaries, common control inheritance considerations, a lack of completed requirements in security assessment and authorization packages, and a lack of completing an organization-wide cyber-security risk assessment or considering the results of this assessment and system level risk assessments in the categorization and selection of controls to manage this risk at the system and organization levels.
    - A clear and concise cyber-risk dashboard or tools to monitor risk, risk response types, risk dependencies to support informed risk response.
- 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." SSA's Information System Security Officers (ISSOs) were deployed to the regional offices in Fiscal Year 2021. However, in Fiscal Year 2022, roles and responsibilities had not yet been developed for the ISSOs to include consideration of risks identified in regional office security assessments of field office and DDS sites in SSA's overarching Risk Management Strategies and risk response decisions.
- Technology – We noted 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 configuring software in many instances. For example, we continued to note issues with information system hardware and software inventory management, automation and tools for managing security configurations, and comprehensive tools to evaluate and communicate risks. Further, SSA had not yet fully implemented a comprehensive Network Access Control (NAC) technology solution.

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; approving authorization to operate packages for the system without an appropriate understanding of risks; and/or not authorizing systems that are operating in production.

Recommendations

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

1. Implementing and revising, as needed, the 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 Agency-wide. In addition, develop and implement a consistent approach to risk management within its security architecture and continue efforts to revise system boundaries and control inheritance as part of the Agency's effort to transition to ongoing authorization of its information systems.
2. Continue efforts to integrate deployed 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.

Grant Thornton Response

Grant Thornton reviewed the additional context provided in management's response on page 119 of this Agency Financial Report. Management's response does not affect the assessment of the significant deficiency.

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

Overview

A benefit overpayment exists when beneficiaries receive payments beyond their entitled amount. When SSA detects a benefit overpayment, it 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 nationwide. Overpayment detection, calculation, and documentation occur in various places throughout SSA, including approximately 1,200 field offices, 8 processing centers, and various functional areas within SSA's 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 the benefit overpayment 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 the Supplemental Security Income Accounts Receivable Ledger

OMB Circular A-123, Appendix D, *Compliance with Federal Financial Management Improvement Act* (OMB Circular A-123), requires that the United States Government Standard General Ledger be applied at the transaction level. For 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. As in prior years, our current-year testing revealed 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.

System limitations prevent SSA from reconciling the SSI differences between the detail and summary-level information in the subsidiary ledger. This could lead to misstatements in the financial statements; however, the unreconciled differences are immaterial to the financial statements and the accounts receivable with the public line items.

Deficiencies in Benefit 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 benefit overpayment balances or sufficient evidence to support approval of waived overpayments. The *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, 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, our inquiries of management since these enhancements, including inquiries made during the current year, revealed that improvements in the operating effectiveness of this internal control process were not expected.

Professional standards dictate that, when an auditor deems a control to have been ineffective in the prior year, and management indicates there has been no improvement, the auditor need not test it in the current year. Therefore, we did not test a separate sample of new overpayments or waived overpayments identified in Fiscal Year 2022 for internal control effectiveness. In prior years, our testing disclosed that SSA did not follow established policy or maintain proper documentation to support overpayments and waivers. This 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.

To test the recorded amount of accounts receivable with the public, we selected a statistical sample of outstanding OASDI and SSI overpayment balances and noted overpayment calculation errors in 6 (30 percent) of 20 sampled OASDI items and 2 (7 percent) of 27 sampled SSI 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

Beneficiaries can request to repay overpayment balances in monthly installments as withholdings from monthly benefit payments. Depending on the amount of the overpayment balance and the amount of each installment payment, 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, (for example, 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 understating accounts receivable balances. In addition, the impact of this issue will continue growing 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 the SSI Accounts Receivable Ledger

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 Benefit 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 overpayment processing management information to consider risk-based factors such as current overpayment balances, manual intervention required, and age.
3. Consider implementing 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 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.

SOCIAL SECURITY

The Commissioner

November 10, 2022

Grant Thornton LLP
111 S. Calvert Street, Suite 2320
Baltimore, MD 21202

Dear Sir or Madam:

We have reviewed the Report of Independent Certified Public Accountants concerning our fiscal year (FY) 2022 financial statements. We are pleased we received our 29th consecutive unmodified opinion on our financial statements, an unmodified opinion that our internal control over financial reporting was operating effectively, and we had no reportable instances of noncompliance with laws, regulations, contracts, and grant agreements, or other matters tested.

In this year's financial statement audit, you cited three significant deficiencies identified in prior years. The significant deficiencies concern internal control over certain financial information systems controls, information systems risk management, and internal control over accounts receivable with the public (benefit overpayments).

As noted in your report, we made progress in remediating elements of these significant deficiencies; however, we continue to face challenges such as the ever-changing cybersecurity landscape in which we operate. Your assessment of the significant deficiencies does not fully account for our improved performance in critical areas where cybersecurity was substantially strengthened. We remain committed to resolving the deficiencies identified by audits through risk-based corrective action plans to mitigate risks and strengthen our control environment. Many elements of our remediation plans will take time to implement.

We appreciate both your efforts and the efforts of the Office of the Inspector General. The independent audit process continues to provide us with valuable recommendations, and we remain committed to excellence in financial management.

If members of your staff have any questions, they may contact Christian Hellie, Associate Commissioner for the Office of Financial Policy and Operations, at 410-965-9511.

Sincerely,

Kilolo Kijakazi

Kilolo Kijakazi, Ph.D., M.S.W.
Acting Commissioner

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

This page was intentionally left blank.