ANALYSIS OF SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

Management Assurances

Fiscal Year 2024 Commissioner's Assurance Statement

SSA management is responsible for managing risks and maintaining effective internal control and financial management systems (FMS) to meet the objectives of Sections 2 and 4 of the *Federal Managers' Financial Integrity Act* (FMFIA). We conducted our assessment of risk and internal control in accordance with the requirements of Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Our assessment considered the design and operating effectiveness of our data quality controls to ensure they support *Digital Accountability and Transparency Act* reporting objectives as outlined in our *Data Quality Plan*. Based on the assessment results, we can provide reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 2024.

The agency's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with U.S. Generally Accepted Accounting Principles. Management is also responsible for designing, implementing, and maintaining effective internal control over financial reporting. An entity's internal control over financial reporting includes those policies and procedures that: (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the entity; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with U.S. Generally Accepted Accounting Principles, and that receipts and expenditures of the entity are being made only in accordance with authorizations of management and those charged with governance; and (3) provide reasonable assurance regarding prevention, or timely detection and correction, of unauthorized acquisition, use, or disposition of the entity's assets that could have a material effect on the financial statements.

We conducted our assessment of the effectiveness of internal control over financial reporting, based on criteria established in the *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States. Based on the assessment results, we concluded that, as of September 30, 2024, SSA's internal control over financial reporting is effective.

The *Federal Financial Management Improvement Act of 1996* (FFMIA) requires Federal agencies to implement and maintain FMSs that comply substantially with: 1) Federal FMS requirements; 2) applicable Federal accounting standards; and 3) the U.S. Standard General Ledger at the transaction level. We assessed our FMSs in accordance with the requirements of OMB Circular No. A-123, Appendix D, *Management of Financial Management Systems – Risk and Compliance*. Based on the assessment results, we determined our FMSs substantially comply with FFMIA and conform to the objectives of FMFIA. In making this determination, we considered all available information, including the auditor's opinion on our fiscal year 2024 financial statements, the report on the effectiveness of internal controls over financial reporting, and the report on compliance with laws and regulations. We also considered the results of the FMS reviews and management control reviews conducted by the agency and its independent contractor.

Martin O'Malley
Commissioner
November 13, 2024

Agency Federal Managers' Financial Integrity Act Program

We have a well-established, agency-wide management control and financial management systems (FMS) program as required by the *Federal Managers' Financial Integrity Act* (FMFIA). We accomplish the objectives of the program by:

- Integrating management controls into our business processes and FMSs at all organizational levels;
- Reviewing our management controls and FMS controls on a regular basis; and
- Developing corrective action plans for control weaknesses and monitoring those plans until completion.

We incorporate effective internal controls into our business processes and FMSs through the life cycle development process. We incorporate the necessary controls into the user requirements, certify the controls are in place by having management review the new or changed processes and systems, and test the controls prior to full implementation to ensure they are effective.

We identify management control issues and weaknesses through audits, reviews, studies, and observations of daily operations. We conduct internal reviews of management and systems security controls in our administrative and programmatic processes and FMSs. These reviews evaluate the adequacy and efficiency of our operations and systems, and provide overall assurance that our business processes are functioning as intended. The reviews also ensure management controls and FMSs comply with the standards established by FMFIA, the *Federal Financial Management Improvement Act of 1996*, and Office of Management and Budget (OMB) Circular Nos. A-123 and A-130. Throughout the fiscal year, management control issues and weaknesses are reviewed individually and in the aggregate to determine if a reportable condition exists.

Our managers are responsible for ensuring effective internal control in their areas and communicating possible reportable conditions as necessary. We require senior-level executives to submit annual statements to the Commissioner providing reasonable assurance that functions and processes under their areas of responsibility were functioning as intended and that there were no major weaknesses that would require reporting, or a statement indicating they could not provide such assurance. This executive accountability assurance provides an additional basis for the Commissioner's annual assurance statement.

Our Executive Internal Control Committee, consisting of senior managers, ensures our compliance with FMFIA and other related legislative and regulatory requirements. The Executive Internal Control Committee evaluates identified major control weaknesses to determine if they are material, and if the Commissioner must make a final determination on whether to report them.

For more information, please refer to the Summary of Financial Statement Audit and Management Assurances located in the *Other Information* section of this report.

Management Control Review Program

In compliance with OMB Circular No. A-123, we have an agency-wide review program for management controls in our administrative and programmatic processes. The reviews encompass our business processes, such as enumeration, earnings, claims and post-entitlement events, and debt management. We conduct these reviews at our field offices, processing centers, hearings offices, and at the State disability determination services. These reviews indicate our management control review program is effective in meeting management's expectations for compliance with Federal requirements.

Financial Management Systems Review Program

The agency maintains an FMS inventory and conducts reviews of the FMSs to ensure they meet Federal requirements. In addition to our financial systems, we include all major programmatic systems in the FMS inventory. On a three-year cycle, an independent accounting firm performs detailed reviews of our FMSs. During fiscal year (FY) 2024, the results of these reviews did not disclose any significant weaknesses that would indicate noncompliance with laws, Federal regulations, or Federal standards.

Government Accountability Office's, Standards for Internal Control in the Federal Government

In FY 2024, we engaged an independent accounting firm, separate from our independent auditor, to assess our compliance with the Government Accountability Office's (GAO), *Standards for Internal Control in the Federal Government*. The standards provide the internal control framework and criteria that Federal managers should use to design, implement, and operate an effective internal control system that will provide us with reasonable assurance that we will achieve our operations, reporting, and compliance objectives. Based on the procedures performed, the independent accounting firm concluded we have an adequately designed system of internal controls that meets the GAO's standards.

Enterprise Risk Management

We continue to mature our Enterprise Risk Management (ERM) program in accordance with OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. We have implemented a multi-year strategy that will further integrate our existing internal control and risk management frameworks with our strategic planning and review processes. During FY 2024, we continued to expand on our *Risk Evaluation, Assessment, and Considerations Handbook* that provides guidance in incorporating risk assessments and analyses into agency projects, initiatives, and decision memorandums. We incorporated more continuous monitoring into our risk profile process, providing more frequent updates to our risk response and proposed actions sections along with considerations of which risks to include. The risks included in our risk profile align with the Inspector General's report on the agency's "Major Management and Performance Challenges" and are discussed bi-weekly in various agency SecurityStat sessions. More information on SecuritySTAT can be found at SSA.gov/securitystat.. Finally, we are constantly reaching out beyond our Program Partners to integrate ERM with various risk functions throughout the agency.

Financial Statement Audit

The Office of the Inspector General (OIG) contracted with Ernst & Young LLP (EY) for the audit of our FY 2024 financial statements. EY opined that the Consolidated Financial Statements are presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles (GAAP) for Federal entities.

EY also opined that the Sustainability Financial Statements, which comprise the Statement of Social Insurance as of January 1, 2024, and the Statement of Changes in Social Insurance Amounts for the period January 1, 2023 to January 1, 2024, are presented fairly, in all material respects, in accordance with U.S. GAAP.

EY opined that we maintained, in all material respects, effective internal control over financial reporting as of September 30, 2024, based on the criteria established in the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States.

In this year's financial statement audit, EY cited two significant deficiencies identified in prior years. These significant deficiencies concern internal controls over certain financial information systems and internal control over accounts receivable with the public (benefit overpayments). We are working to resolve the deficiencies identified by audits through risk-based corrective action plans to mitigate risks and strengthen our internal control environment.

For more information on the auditors' findings and our plans to correct the findings, please refer to the *Report of Independent Auditors* and *Agency Response to the Report of Independent Auditors* sections of this report.

Federal Information Security Modernization Act

The *Federal Information Security Management Act of 2002* (FISMA), as amended by the *Federal Information Security Modernization Act of 2014*, requires Federal agencies to ensure adequate security protections for Federal information systems and information. Under this act, Federal agencies must submit annual FISMA reports to OMB. We submitted this year's report timely. Our report summarizes the results of our security reviews of major information systems and programs, our progress on meeting the Administration's cybersecurity priorities, and the results of other work performed during the reporting period using government-wide cybersecurity performance measures.

For the FY 2024 FISMA audit, EY identified a number of recommendations to mature the cybersecurity posture of the agency, including process improvements associated with the integration of our enterprise and cybersecurity risk management programs, leading EY to issue an overall Not Effective rating for our program. While we agree with the auditor's high-level recommendations for continuous program improvement, we regard our program as Effective, especially when factoring in our real-world experience and performance with protecting our network and systems from multiple critical threats and vulnerabilities impacting the Federal enterprise. While the Inspector General (IG) FISMA Metrics are strongly encouraged for use as evaluation criteria, it is our understanding that they were not designed to be the sole determinant of maturity. As established in OMB's FY 2023-2024 IG FISMA Reporting Metrics, "IGs should

consider both their and the agency's assessment of unique missions, resources, and challenges when determining information security program effectiveness." Additionally, it states, "Therefore, an IG has the discretion to determine that an agency's information security program is effective even if the agency does not achieve a Level 4 (Managed and Measurable)."

We concur with EY's Effective rating for our Incident Response program, further demonstrating our commitment to ensure incident detection and handling are in place to battle an evolving threat landscape. Our response to these evolving threats amid well publicized exploits of corporate and government entities in FY 2024 demonstrates our capabilities to protect the agency's information technology (IT) assets. Additionally, we agree with EY's Effective rating for the Information Security Training program. Significant improvements were made in our phishing and training programs that resulted in receiving the Innovative Solutions Award during the 34th Federal Information Security Educators Conference.

As evidenced by our improved FY 2024 scores, we continuously enhance our cybersecurity and privacy controls that elevates our maturity levels. Fifty-four percent of all metrics are rated L3 Consistently Implemented or higher. We understand the importance of strong enterprise cyber governance and managing associated cyber risks are of utmost importance to our agency and we will continue our efforts to further improve our performance across all FISMA domains. For this reason, we strengthened and expanded our Information System Security Officer (ISSO) program by adding Information System Security Engineer staff to assist the ISSOs in providing improved front line security oversight for agency components, regions, and distributed sites. Additionally, we implemented a Cybersecurity Risk Program Management Office (PMO) and established an enhanced cybersecurity risk dashboard. Continued efforts in this area will assist in raising scores in all FISMA domains.

In terms of our strategy to achieve a Level 4 Effective rating, we are developing maturation plans to elevate all FISMA domains to at least level 3 or level 4 specifically targeting the Identify and Detect domains. To that end, we established the Cyber Risk PMO and dashboard. The PMO will define metrics and drive performance measures needed to ensure all agency software include appropriate security controls and manage cybersecurity risks.

The agency will continue to prioritize our efforts based on risk-based decisions in implementing all recommended cybersecurity program improvements, however it is important to note that many of our initiatives require multi-year investments to fully meet the criteria established for an Effective program, as designated by the metrics.

Financial Management Systems Strategy

Over the years, we have worked hard to improve our financial management practices. We continue to develop initiatives to enhance the existing financial and management information systems. Our actions demonstrate discipline and accountability in the execution of our fiscal responsibilities as stewards of the Social Security programs. Going forward, our goal is to achieve government-wide and internal financial management milestones established for improvement.

Annually, we review and update our FMS inventory to reflect the status of our systems modernization projects. We categorize our inventory of FMSs under the broad headings of

Program Benefits, Debt Management, or Financial/Administrative and continue the long-term development of our FMSs following a defined strategy.

For the Financial/Administrative systems category, the Social Security Online Accounting and Reporting System (SSOARS) has been our accounting system of record since implementation in 2003. Every agency financial transaction is recorded in SSOARS. SSOARS is subject to extensive audit testing procedures by the independent auditors contracted by OIG in accordance with the *Chief Financial Officer's Act of 1990*.

SSOARS is a federally certified accounting system based on Oracle Federal Financials and consists of core accounting, payables, purchasing, receivables, iStore, WebCenter, Business Intelligence (BI) Publisher, Service Oriented Architecture Suite, and Single Sign-on (SSO) services. SSOARS produces management information reports and provides real-time integration with administrative and programmatic systems for obligations and payments, which significantly improves reporting accuracy and timeliness.

In FY 2024, we began migrating SSOARS to new hardware. The move to the new hardware entails a change from Solaris to LINUX operating systems. This will achieve more compliance with the agency's Office of the Chief Information Officer (OCIO)-recommended technologies upon retirement of the Oracle hardware in December. We achieved significant results with G-Invoicing releases and patches. SSOARS interfaces fully as a requestor in the governmentwide G-Invoicing system. This achieves compliance with a government mandate to use G-Invoicing.

We provided a replacement application for Oracle's BI Publisher and WebCenter with agency supported WebFOCUS reporting which allows SSOARS to utilize an agency supported reporting system instead of two Oracle commercial off-the-shelf software applications for reporting. This will achieve more compliance with the agency's OCIO-recommended technologies upon retirement of Oracle's BI Publisher and WebCenter in December. We implemented Multi-Factor Authentication (MFA)-compliant SSO for SSOARS users which achieves compliance with the agency's OCIO MFA requirements. Finally, we monitored and resolved multiple Known Exploited Vulnerabilities (KEV), which are risks identified by the Cybersecurity and Infrastructure Security Agency (CISA). This achieves compliance with the CISA rules for Federal agencies to speedily patch KEVs as published by CISA.

Throughout FY 2025, we will complete the SSOARS migration to the new hardware using the LINUX operating system. We plan to continue execution of G-Invoicing releases and patches. We will retire BI Publisher and WebCenter. To determine the best approach to fully implement SSOARS to a next generation Treasury-approved Financial Management Quality Service Management Office (FM QSMO) offering, we will analyze and compare FM QSMO offerors.

As CISA identifies risks and vulnerabilities, we will monitor and resolve the associated KEVs. We will conduct research and analysis for the implementation of OMB and Treasury requirements such as: Program Activity Reporting Key code implementation and Treasury Account Symbol revisions. We will also conduct major infrastructure patching of SSOARS.

Digital Accountability and Transparency Act

We submitted and certified the required reports for the *Digital Accountability and Transparency Act of 2014* (DATA Act) for the fourth quarter of FY 2023 and the first, second, and third quarters of FY 2024. These reports were submitted monthly as required by OMB Memorandum M-20-21, *Implementation Guidance for Supplemental Funding Provided in Response to the Coronavirus Disease 2019 (COVID-19)*. Additionally, we have submitted the required reports for July, August, and September 2024.

We are continuing to engage with the DATA Act community to develop improvements to the Governmentwide Spending Data Model (GSDM) formerly known as the DATA Act Information Model Schema. We participate in workgroups to develop policy, guidance, and new reporting requirements. The DATA Act effort will continue to enhance our transparency through improved consistency. In addition, we are providing more detailed data to USASpending.gov and additional data to Treasury. For FY 2024, we implemented GSDM 1.0.1.

In compliance with OMB Memorandum M-18-16, *Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk,* we have developed a *Data Quality Plan* to ensure we have effective internal controls over the input and validation of data submitted to USAspending.gov. We leverage our existing FMFIA program activities to identify critical risk points and corresponding mitigating controls and assess the design and operating effectiveness of our data quality controls to ensure they support DATA Act reporting objectives. We also consider the results of our assessment in our FMFIA annual assurance statement process.

The DATA Act has provided the agency a tool to remove the silos for the various lines of business that are impacted by the DATA Act. There is a coordinated effort between finance, budget, acquisition, and financial assistance to make sure our spending data links between the various systems. This allows a link from budget formulation to award issuance to funds disbursement.

USAspending.gov displays the number of unlinked awards submitted for each period for both contracts and financial assistance. In FY 2024, we had 669 unlinked awards and 95 percent of these awards were either zero dollar or micro-purchase. These unlinked awards link internally, but due to reporting requirements, do not link externally on USAspending.gov. In FY 2023, we had 484 unlinked awards and 93 percent of these awards were either zero dollar or micro-purchase. The unlinked awards on USAspending are dynamic and can change from submission to submission as new data is submitted.

Since the first DATA Act reporting period, second quarter of FY 2017, we have reported on every Treasury Account Symbol and have not had a reporting difference in obligations.

This page was intentionally left blank.