ANALYSIS OF SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

Management Assurances

Fiscal Year 2025 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, 2025.

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, 2025, 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 2025 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.

Frank J. Bisignano
Commissioner
January 15, 2026

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) 2025, 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 2025, 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 2025, 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." We updated our risk appetite statement to reflect the changes to our risk posture, aligning with agency leadership. 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 2025 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, 2025, and the Statement of Changes in Social Insurance Amounts for the period January 1, 2024 to January 1, 2025, 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, 2025, 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). Efforts are underway to rectify deficiencies identified through audits by using 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 *Reports of Independent Auditors* and *Agency Response to the Reports 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 data. In accordance with this mandate, agencies must submit annual FISMA reports to OMB. We submitted this year's report on time, providing a comprehensive summary of our security reviews for major information systems and programs, our progress in meeting the Administration's cybersecurity priorities, and the results of other activities conducted during the reporting period, as measured by government-wide cybersecurity performance metrics.

For the FY 2025 FISMA audit, EY identified several recommendations to further mature the agency's cybersecurity posture, including process improvements related to the integration of our enterprise and cybersecurity risk management programs. Based on their assessment, EY issued an overall "Not Effective" rating for our program.

We recognize that strong enterprise cyber governance and effective management of cyber risks are critical to our mission, and we remain committed to continuous improvement across all FISMA domains. To support this, we established an Analytics and Improvements component to centralize authority for data inventory, leveraging existing tools and services such as the Enterprise Data Catalog, with full implementation targeted by January 2026. Additionally, we

have continued to mature our Cybersecurity Risk Program Management Office and have developed a cyber risk taxonomy aligned with the agency's ERM Program. These ongoing efforts will enhance our performance in all FISMA domains and support strategic decision-making.

Furthermore, we are transitioning to a new platform to centralize our governance, risk, and compliance (GRC) activities. This transition will streamline operations, improve service delivery, and enable the migration of all asset inventories to a centralized location, supporting seamless integration with the GRC program.

We concur with EY's "Effective" rating for our Incident Response program, which further demonstrates our commitment to robust incident detection and response capabilities in an evolving threat landscape. Our response to emerging threats, including high-profile exploits affecting both corporate and government entities in FY 2025, highlights our ability to safeguard the agency's information technology assets. We have successfully completed the majority of initial onboardings for enterprise logging (EL) Level 1 assets, set forth in OMB Memorandum 21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents." We are actively onboarding information systems that qualify for EL Level 2.

The agency will continue to prioritize risk-based decision-making in implementing recommended cybersecurity program improvements. It is important to note that many of these initiatives require multi-year investments to fully meet the criteria for an "Effective" program, as defined by the relevant 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 its 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 general ledger, payables, purchasing, receivables, iStore, 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 purchasing, payables, and receivables, which significantly improves reporting accuracy and timeliness.

In FY 2025, we migrated SSOARS to new hardware. The move to the new hardware entailed a change from Solaris to LINUX operating systems. This hardware migration supported improved cadence of monthly hardware and operating system patching. This also achieved more compliance with the agency's Chief Information Officer (CIO)-recommended technologies upon retirement of the Oracle hardware in December.

We achieved significant results with Executive Order (E.O.) 14168 compliance by applying two different patches. We reimplemented Multi-Factor Authentication (MFA)-compliant SSO for invoice approval system users which achieves compliance with the agency's CIO MFA requirements. 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 KEV as published by CISA. We replaced de-supported commercial off-the-shelf Preventive Controls Governor software with agency-developed custom configurations achieving form and field changes and validations. We addressed prior year financial audit findings related to timely user removal and system scan result remediation. We implemented a General Ledger upload solution to replace Oracle technology reliant on ActiveX. We improved System Life Cycle environments with the addition of a development environment and made all environments more production-like.

Throughout FY 2026, we plan to continue execution of G-Invoicing releases and patches, with the intention to support G-Invoicing 7600EZ functionality ahead of its use by Go.gov. We will implement multiple new real-time interfaces with the new Federal Travel System, Go.gov. We will analyze and compare Financial Management Quality Service Management Office (FM QSMO) offerors to determine the best offering for the agency. Based on that analysis, and in compliance with E.O. 14249, our goal is to procure an FM QSMO core financial system and related implementation services in FY 2026. If that procurement timeframe is met, FM QSMO system implementation tasks will run through FY 2027 and FY 2028 with tentative cutover at the beginning of FY 2029. We will continue working on E.O. 14222, for payment justifications, and E.O. 14247, working to reduce administrative check payments. We will continue to monitor and resolve issues as CISA identifies risks and vulnerabilities and apply patching for the associated KEV. We will continue to 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* (DATA Act) for the fourth quarter of FY 2024 and the first, second, and third quarters of FY 2025. 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 2025.

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 (DAIMS). 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.

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 2025, we had 2,512 unlinked awards and 98 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. 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.