ANALYSIS OF SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

Management Assurances

Fiscal Year 2026 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, 2026.

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, 2026, 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 2026 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
November 13, 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 outside accounting firm, separate from our independent auditor, performs detailed reviews of our FMSs. During fiscal year (FY) 2026, 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 2026, we engaged an outside 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 outside accounting firm concluded we have an adequately designed system of internal controls that meets the GAO's standards.

Enterprise Risk Management

In FY 2026, we revised our Enterprise Risk Management (ERM) approach in response to the OMB Circular revisions repositioning ERM from Internal Controls (OMB Circular A-123, Management's Responsibilities for Internal Control) to Strategic and Performance Planning (OMB Circular A-11, Part 6, The Federal Performance Framework for Improving Program and Service Delivery). Our revised ERM approach encompasses:

- **Focus:** ERM uses a systematic process to identify, assess, and manage risks that may impact the achievement of the agency's strategic objectives, including those related to mission delivery, operations, compliance, and public trust.
- **Alignment:** ERM aligns with agency strategic and performance planning to promote risk aware, data-driven decision-making, enabling the agency to manage, mitigate, or avoid risks that may impact our strategic goals and objectives.

- **Governance:** While responsibilities for managing risks are shared throughout the agency, from the highest levels of executive leadership to the service delivery staff, our ERM activities are overseen by a governance structure – to establish risk appetite and tolerance levels, ensure effective strategies for managing significant risks, and assess the efficacy of overall ERM actions and activities.
- **Risk Portfolios:** ERM provides a portfolio view of risks, offering insight into all areas of organizational exposure to risk – such as reputational, programmatic performance, financial, information technology, acquisitions, and human capital – to identify the most significant risks, reduce the likelihood of unanticipated outcomes, and better assess risks associated with changes in the internal and external risk environment.
- **Risk Profiles:** ERM develops risk profiles as part of the annual strategic review, documenting the highest impact risks from mission and mission-support operations, and providing a comprehensive analysis to inform changes to agency planning and implementation strategies.
- **Targeted Risk Assessments:** ERM conducts coordinated, agency-wide risk assessment activities to address challenges or threats to achieving our goals and objectives, giving leaders better insight into how to prioritize and manage risks to mission delivery, resulting in more resilient and effective programmatic operations.

Overall, the revised ERM approach reflects the agency's forward-looking principles and practices, balancing risks and returns to enhance value to the taxpayer and increase the agency's ability to achieve its strategic goals and objectives.

Financial Statement Audit

The Office of the Inspector General (OIG) contracted with Ernst & Young LLP (EY) for the audit of our FY 2026 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, 2026, and the Statement of Changes in Social Insurance Amounts for the period January 1, 2025 to January 1, 2026, 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, 2026, 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 one significant deficiency identified in prior years concerning internal control over accounts receivable with the public (benefit overpayments). Efforts are underway to rectify deficiencies identified through audits by using corrective action plans to mitigate risks and strengthen our internal controls. This year we successfully remediated a longstanding significant deficiency concerning internal controls over certain financial information systems demonstrating our commitment to maintaining effective

information technology internal controls and strengthening the integrity of our financial reporting 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.

FY 2026 marked the most significant advancement in cybersecurity in the Social Security Administration's history. We strengthened leadership accountability, established a governance structure, applied risk-management tools, and delivered measurable improvements across our cybersecurity program. Cybersecurity at the agency is a zero-fail mission and one of our highest priorities. To elevate accountability, we established a Chief of Security and Resiliency with direct oversight of cybersecurity that reports directly to the Commissioner. We also instituted stronger governance, clearer lines of responsibility, and greater executive visibility into cybersecurity risk, performance, and remediation.

The results of our FY 2026 FISMA audit demonstrate the impact of these reforms. EY found that we made progress in maturing our cybersecurity posture by defining and implementing roadmaps to improve our cybersecurity program. Based on the IG FISMA reporting metrics guidance, EY concluded our overall security program was "Consistently Implemented" but "Not Effective" for FY 2026. We concur with EY's "Effective" rating in the Govern, Protect, and Respond functions. In FY 2026, we increased maturity scores in the three cybersecurity domains mentioned above, with no decreases in any domain or metric. Five metrics improved, representing a 20 percent increase in metrics assessed. We closed 43 of 51 prior-year findings, 13 of which were superseded by new issues identified in FY 2026, and an overall 40-percent reduction in total findings issued. We also fundamentally improved how the agency identifies, manages, and addresses cybersecurity risk by consolidating previously siloed processes into a centralized risk-management tool launched in FY 2026. Continued migration to and refinement of this platform will provide greater consistency, visibility, accountability, and enterprise-wide management of cybersecurity risk.

These improvements are not simply about achieving higher scores or satisfying compliance requirements; they represent a fundamental strengthening of how the agency governs and manages cybersecurity. An agency entrusted with the records, personal information, and benefits of hundreds of millions of Americans must operate a cybersecurity program equal to that responsibility. We will continue to modernize our capabilities, strengthen our controls, rapidly address identified risks, and hold ourselves accountable for results. Our objective is not merely

to meet Federal cybersecurity standards, but to exceed them and establish the agency as a model for cybersecurity excellence across the Federal Government. Cybersecurity is mission security, and the historic progress achieved in FY 2026 establishes a stronger foundation for protecting the American people and the systems on which they depend.

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 Management 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 services. SSOARS produces management information reports and provides real-time integration with administrative and programmatic systems for purchasing, payables, and receivables, which significantly improve reporting accuracy and timeliness.

In FY 2026, the SSOARS team delivered several significant accomplishments:

- Monitored and resolved multiple SSOARS related Known Exploited Vulnerabilities (KEV), as identified by the Cybersecurity and Infrastructure Security Agency (CISA), ensuring compliance with CISA requirements for Federal agencies to promptly remediate published KEVs for SSOARS.
- Made substantial resource investments to prepare for implementing Go.Gov, a new, government-wide, cloud-based travel and expense management system provided by the General Services Administration, which is expected to move into production in November 2027. Go.Gov will streamline travel bookings, approvals, and reimbursements.
- Implemented cumulative G-Invoicing upgrades in support of 7600EZ, Mulesoft endpoints, and JavaScript Object Notation.

- Completed market research and requirements gathering for a new Financial Management Quality Service Management Office core financial system, which will standardize financial management across Federal agencies.
- Reduced the cost and scope of the Social Security Electronic Remittance System by removing credit card devices with expired PCI-DSS certification.
- Migrated to new cloud endpoints for Invoice Processing Platform, a secure, web-based service provided by Treasury to help Federal agencies manage the full invoicing lifecycle, and Treasury Payment Automation Manager (PAM) processing.
- Continued compliance efforts for related Executive Orders (E.O.), including Do Not Pay (DNP) Connect and Treasury PAM file updates required for DNP verification.

Throughout FY 2027, we plan to:

- Continue deploying G-Invoicing releases and patches.
- Implement multiple new real-time interfaces for Go.gov.
- Continue advancing compliance efforts for E.O. 14222 (payment justifications), E.O. 14247 (reducing administrative check payments), and E.O. 14249/M-25-32 (DNP).
- Continue monitoring and resolving CISA-identified risks and vulnerabilities, ensuring timely patching of related KEVs.
- Apply necessary application, database, and infrastructure upgrades and patches.
- Continue research and development of a new customer-driven digital collection system.
- Begin work to implement the new M-26-14 memorandum.

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 2025 and the first, second, and third quarters of FY 2026. 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 2026.

We are continuing to engage with the DATA Act community to develop improvements to the Governmentwide Spending Data Model. 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.

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 2026, we had 702 unlinked awards and 96 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.gov are dynamic and may change 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.