

ANALYSIS OF SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

MANAGEMENT ASSURANCES

FISCAL YEAR 2022 ACTING 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, 2022.

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, 2022, 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, *Compliance with the Federal Financial Management Improvement Act of 1996*. 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 2022 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.



Kilolo Kijakzi, Ph.D., M.S.W.
Acting Commissioner
November 10, 2022

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 Acting 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 Acting 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 Acting 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 contractor performs detailed reviews of our FMSs. During fiscal year (FY) 2022, 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 2022, we engaged an independent accounting firm to assess our compliance with the revised 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 2022, we began developing a training series to increase awareness of ERM and risk concepts among different levels of the agency and explain how to apply the training content to further ERM maturity. The first training, ERM 101, is planned for release in FY 2023. Additionally, we are having more robust risk discussions at all levels of the organization, including roundtable discussions at the executive and staff levels. We have improved documentation surrounding risk discussions and have identified gaps within our risk hierarchy that we are working to correct.

FINANCIAL STATEMENT AUDIT

The Office of the Inspector General (OIG) contracted with Grant Thornton LLP (Grant Thornton) for the audit of our FY 2022 financial statements. Grant Thornton found we present fairly the basic financial statements, in all material respects, in conformity with U.S. Generally Accepted Accounting Principles (GAAP) for Federal entities.

Grant Thornton also found that the sustainability financial statements, which comprise the Statement of Social Insurance as of January 1, 2022, and the Statement of Changes in Social Insurance Amounts for the period January 1, 2021 to January 1, 2022, are presented fairly, in all material respects, in accordance with U.S. GAAP.

Grant Thornton found we maintained, in all material respects, effective internal control over financial reporting as of September 30, 2022, 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, Grant Thornton cited three significant deficiencies identified in prior years. These 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). We resolve the deficiencies identified by audits through risk-based corrective action plans to mitigate risks and strengthen our control environment.

For more information on the auditors' findings and our plans to correct the findings, please refer to the *Report of Independent Certified Public Accountants* section 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 2022 FISMA audit, Grant Thornton acknowledged our risk-based approach to strengthening the agency's information system security program and recognized our continued efforts to improve and mature our information security program and practices to protect against cybersecurity threats. For FY 2022, they issued an overall Not Effective rating for our program. According to the FY 2022 Core Inspector General (IG) FISMA Metrics criteria, Level 4, Managed and Measurable, is considered to be an effective level of security at the overall program level. While we agree with many of Grant Thornton'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 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 2022 Core IG Metrics Implementation Analysis and Guidelines document, "While the determination of effectiveness can be established based on the results of the IG metrics, IGs should continue to consider their own assessment of unique missions, resources, and challenges faced by the agency when assessing the maturity of information security programs."

New for FY 2022, we earned Effective ratings in the Data Protection & Privacy and Security Training domains. Our improvement in these areas affirms our consistent and effective implementation of related programs. We concur with Grant Thornton's continued acknowledgement of an Effective rating for our Incident Response program, further demonstrating our commitment to ensure protections are in place to battle an evolving threat landscape. Our response to these evolving threats and well publicized exploits of corporate and government targets in FY 2022 demonstrates our capabilities to protect the agency's information technology (IT) assets.

As evidenced by our improved FY 2022 scores, we continuously enhance our cybersecurity controls and elevate our maturity levels. We understand the importance of effective enterprise cyber governance and oversight, and in FY 2022, we leveraged our Information System Security Officers (ISSO) to enhance security governance throughout headquarters as well as our distributed sites. During the fiscal year, our ISSOs documented the critical security controls and developed system security plans for our regional systems. We directly attribute many of our improved FISMA scores to the hard work and diligence of our ISSO program.

As part of our cybersecurity planning, we work in close cooperation with our senior management, budget and procurement stakeholders, and program leads to plan and prioritize the required funding and staffing resources. Through FY 2023, we will continue to support multiple investments in key areas of Risk Management, Configuration Management, Identity and Access Management, and Continuous Monitoring. Many of these initiatives require multi-year investments to fully meet the criteria established for an Effective program, as designated by the metrics. Through these investments, we continue to make substantial improvements and progress in enhancing the overall effectiveness of our cybersecurity program.

We are confident that our proactive planning, coupled with responsiveness to external assessments, strong executive support, and continuous process improvement, provide the foundation for achieving higher maturity ratings. We look forward to continued engagement with our OIG on our shared goal of protecting the confidentiality, integrity, and availability of our IT assets.

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.

In FY 2018, we began modernization efforts to build a new Debt Management System (DMS). This IT investment is a multi-year effort that will build a comprehensive overpayment system enabling us to record, track, collect, and report our overpayments more efficiently.

The Debt Management Product is a modernization effort focused not only on a new DMS, but also on modernizing the way we do business and offer services to the public. This includes updating our accounting and reporting for delinquent and unproductive debts, streamlining our current manual remittance process, and providing modern platforms and electronic services for those individuals seeking to pay the agency, such as utilizing online payment methods. These actions will make it easier for our recipients to interact with us.

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. SSOARS is a federally certified accounting system based on Oracle Federal Financials and consists of core accounting, payables, purchasing, receivables, iStore, and WebCenter. SSOARS produces management information reports and provides real-time integration with administrative and programmatic systems for obligations and payments.

In FY 2022, we implemented Unique Entity Identifier compliance for the System for Award Management vendor information. We moved to Edge support for SSOARS, meaning all SSOARS components are now native Edge compliant, and we implemented our initial release of G-Invoicing functionality. We upgraded the Fusion Middleware (FMW) version for WebCenter and Business Intelligence Publisher and the Service Oriented Architecture database version. Additionally, SSOARS was upgraded to handle the increased size of Disaster Emergency Fund Codes (DEFC) values, and we made related changes to *Digital Accountability and Transparency Act of 2014* (DATA Act) reporting to use the new DEFC values.

In FY 2023, we plan to upgrade the underlying Oracle E-Business Suite database version from 12c to 19c and complete the last components of FMW patching. We expect additional releases to G-Invoicing to support functionality fixes, recent patches from Oracle, and late FY 2022 Treasury changes to G-Invoicing to support G-Invoicing changes expected in FY 2023. Finally, we will work with a vendor to complete an analysis of SSOARS rehosting options, as some of the current SSOARS hardware is approaching 10 years of age.

DIGITAL ACCOUNTABILITY AND TRANSPARENCY ACT

We submitted and certified the required reports for the DATA Act for the fourth quarter of FY 2021 and the first, second, and third quarters of FY 2022. 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 2022.

We are continuing to engage with the DATA Act community to develop improvements to 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](https://www.usaspending.gov) and additional data to Treasury. For FY 2022, we implemented DAIMS 2.1 and 2.1.2. We have already implemented the changes for DAIMS 2.2 and 2.2.1, which are required for FY 2023.

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 2022, we had 1,114 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 2021, we had 1,273 unlinked awards and 98 percent of these awards were either zero dollar or micro-purchase.

Since the first DATA Act reporting period, 2nd 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.