



# SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

## MANAGEMENT ASSURANCES

### Fiscal Year 2019 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, 2019.

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, 2019, 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 conducted an assessment of 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 2019 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.

Andrew Saul  
Commissioner  
November 12, 2019



## 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.

Our managers are responsible for ensuring effective internal control in their areas of responsibility. We require senior-level executives to submit an annual statement 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. If we identify a major control weakness, the Executive Internal Control Committee determines if the weakness is a material weakness that they would need to forward to our agency head for a final determination on whether to report a material weakness.

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 an 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.

For more information, please refer to the Summary of Financial Statement Audit and Management Assurances located in the *Other Reporting Requirements* 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 also 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) 2019, 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 2019, we engaged an independent accounting firm to assess the agency's 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 the requirements of OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. We are developing a multi-year strategy that will further integrate our existing internal control and risk management frameworks, and strategic planning and review processes. In FY 2020, we will continue enhancing our ERM program, further integrating business practices outlined in our ERM framework, and continue updating our risk profile and promoting risk awareness throughout the agency.

### FINANCIAL STATEMENT AUDIT

The Office of the Inspector General contracted with Grant Thornton LLP (Grant Thornton) for the audit of our FY 2019 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 for Federal entities.

Grant Thornton also found that the sustainability financial statements, which comprise the Statement of Social Insurance as of January 1, 2019, and the Statement of Changes in Social Insurance Amounts for the period January 1, 2018 to January 1, 2019, are presented fairly, in all material respects, in accordance with U.S. Generally Accepted Accounting Principles.

Grant Thornton found we maintained, in all material respects, effective internal control over financial reporting as of September 30, 2019, 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, which contained elements identified in prior years. These significant deficiencies concern internal control over certain financial information systems controls, information systems risk management, and accounts receivable with the public (benefit overpayments). We successfully remediated the significant deficiency identified in prior years concerning the reliability of information used in certain control activities and are committed to resolving the remaining deficiencies through risk-based corrective action plans designed to 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 2019 FISMA audit, Grant Thornton assessed our overall maturity at Level 2 – Defined, acknowledging the agency’s establishment of an agency-wide information security program, including our risk-based approach to strengthening controls over our information systems.

In FY 2019, we made substantial improvements in enhancing the overall effectiveness of our cybersecurity program by increasing application security controls, leveraging cloud platforms, making substantial improvements for our asset and vulnerability management programs, strengthening our network and incident response capabilities, and focusing on security training delivery and completeness. We also increased emphasis on governance and oversight of the cyber program at the executive level by involving subject matter experts and leaders from components outside our information technology (IT) department, creating greater awareness of overarching issues and the related risk mitigation activities, and establishing more accountability for completion of programs of objectives and milestones. We are conducting regular bi-weekly cyber dialogue with agency senior leadership and responsible managers from these components, and we will continue to accelerate activities to remediate identified risks, and elevate cybersecurity awareness and accountability across all levels. We believe cybersecurity is not just an IT function; it is a strategic imperative for the agency to create coordinated agency-level attention across all organizational components.

The agency handles all auditor findings with the utmost importance, and we will continue to aggressively pursue an accelerated risk-based remediation approach to address the remaining findings and mature the agency’s security posture. The agency will continue to practice a defense in-depth cyber strategy that employs a strong set of security controls, technologies, policies, and procedures to manage risk reasonably and to protect the confidentiality, integrity, and availability of information system resources. Properly securing the agency’s information systems and protecting the public’s personally identifiable information is our highest priority.

To improve our processes and capabilities, we will continue to design and implement new and enhanced security controls; however, it takes time for these controls to mature and effectively achieve the next level of maturity in the agency’s security posture. While undergoing this process, we remain vigilant in our efforts by evaluating risk, deploying security controls, and keeping abreast of the ever-evolving threat landscape to safeguard the personally identifiable information that we have been entrusted with by every citizen and non-citizen.

We look forward to elevating our cybersecurity program to Level 4 maturity through a holistic approach, demonstrating progress through planned improvements to our cybersecurity program, enhancing our security posture with risk based decisions, and aggressive remediation of significant audit findings and program deficiencies.

## **FINANCIAL MANAGEMENT SYSTEMS STRATEGY**

Over the years, we have worked hard to improve our financial management practices. We continue to develop new 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 most recent status of our systems modernization projects. We categorize our inventory of nine FMSs under the broad categories 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 a multi-year initiative to develop a modernized enterprise Debt Management System. The Debt Management Product will modernize our Debt Management Systems with a comprehensive build that will enable us to collect, store, monitor, manage, and report our program debt activity with accuracy and timeliness. This modernization effort is an agile investment using modern technology to create an enterprise authoritative source of debt management data; increase collection opportunities; bring efficiencies to and eliminate operational workloads; and resolve compliance and audit recommendations.



In FY 2019, we continued expanding the Debt Management System and began development of an Intranet Waiver application that provides technicians, via an intranet webpage, the capability to capture, document, and support processing waiver requests. In FY 2020, we will continue development of the Intranet Waiver application and prepare for deployment of the new Debt Management System in FY 2021.

For the Financial/Administrative systems category, the Social Security Online Accounting and Reporting System (SSOARS) has been the agency's 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, and receivables. SSOARS produces management information reports and provides real-time integration with administrative and programmatic systems. We were the first Federal agency to successfully implement Oracle's Federal Financials Release 12. Release 12 contained important system software that helped us meet new, required Federal accounting functionality and standards.

In FY 2019, we began to implement three important upgrades to the SSOARS application and database. We are upgrading the application to Version 12.2.8 and the database to Version 12c. These upgrades are required to maintain adequate Oracle support for their products and to allow for critical quarterly software patching. Additionally, we are upgrading several Oracle software products that support SSOARS's ability to share data with other application systems. We will complete all upgrades in FY 2020.

## DIGITAL ACCOUNTABILITY AND TRANSPARENCY ACT

The agency submitted the required reports for the *Digital Accountability and Transparency Act of 2014* (DATA Act) for the fourth quarter of FY 2018 and the first, second, and third quarters of FY 2019. The agency is continuing to engage with the DATA Act community in developing better data definitions. The DATA Act effort will enhance the agency's transparency through improved consistency. In addition, through our DATA Act efforts, we will provide more detailed data to the [USA Spending public website \(www.USAspending.gov\)](http://www.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](http://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.

## NATIONAL ANTI-FRAUD COMMITTEE

Our National Anti-Fraud Committee (NAFC) provides a forum for senior leadership to collaborate and provide strategic oversight on fraud challenges and solutions. NAFC's mission is to support national and regional strategies to combat fraud, waste, and abuse. The committee directs our fraud risk management activities at the agency level by determining the levels of risk tolerance and the amount of investment we will commit to mitigate the identified risks. NAFC supports our goal to promote accountability to taxpayers by ensuring superior financial performance, budget management, and integrity in all payments, records, and processes.

For more information on NAFC, and our other anti-fraud efforts, please refer to the Fraud Reduction and Data Analytics Act Report located in the *Other Reporting Requirements* section of this report.



This page was intentionally left blank.