Systems and Controls

Federal Managers' Financial Integrity Act

Federal Managers' Financial Integrity Act (FMFIA) Program

SSA has a well established agencywide management control and financial management systems program as required by FMFIA. The Agency accomplishes the objectives of the program by:

- Integrating management controls into its business processes and financial management systems at all organizational levels;
- Reviewing its management controls and financial management systems controls on a regularly recurring basis; and,
- Developing corrective action plans for control weaknesses and monitoring those plans until the weaknesses are corrected.

For the second year in a row, SSA has no FMFIA material weaknesses to report. Agency managers are responsible for ensuring that effective controls are implemented in their areas of responsibilities. At the senior manager level, the Agency's Executive Internal Control (EIC) Committee ensures SSA compliance with the requirements of FMFIA and other related legislative and regulatory requirements. The Committee provides executive oversight of the management control program, addresses management control issues that have a substantial impact upon the Agency's mission, monitors the progress of actions to correct management control weaknesses, ensures SSA's critical infrastructure is protected and ensures the Agency has a viable continuity of operations plan.

Effective internal controls are incorporated into the Agency's business processes and financial management systems through the life cycle development process. The user requirements include the necessary controls and the new or changed processes and systems are reviewed by management to certify that the controls are in place. The controls are then tested prior to full implementation to ensure they are effective.

The controls of the new or changed processes or systems are monitored to ensure they remain effective. Management control issues and weaknesses are identified through audits, reviews, studies and observation of daily operations. SSA conducts internal reviews of management and systems security controls in its administrative and programmatic processes and financial management systems. The reviews are conducted to evaluate the adequacy and efficiency of the Agency's operations and systems to provide an overall assurance that the Agency's business processes are functioning as intended. The reviews also ensure that management controls and financial management systems comply with the standards established by FMFIA and Office of Management and Budget (OMB) Circulars A-123, A-127 and A-130. The reviews encompass SSA's business processes such as enumeration, earnings, claims and postentitlement events, debt management and SSA's financial management systems. SSA develops and implements corrective action plans for weaknesses found through the reviews and audits and tracks the corrective actions until the weaknesses are corrected.

Management Control Review Program

SSA has an agencywide review program for management controls in its administrative and programmatic processes. The Agency requires that a minimum of 10 percent of field offices (FO) be reviewed each fiscal year (FY). The FOs are chosen for review by considering performance measures in selected critical processes and by using the experience and judgement of the regional security personnel. During FY 2003, SSA's managers and contractors conducted reviews of 215 FOs and two Program Service Centers (PSC).

SSA has also taken great strides to strengthen the administrative, programmatic and security controls at the State Disability Determination Services (DDS). During FY 2003, SSA issued the revised DDS Security Document which requires each DDS to prepare a security plan and, on an annual basis, perform a self review using the Security Review Checklist prepared by SSA. Additionally, SSA's Regional Offices (RO) perform an independent security review of the DDSs using this same review checklist. The ROs develop a 5-year review plan in which each State DDS is reviewed at least once to ensure adherence to SSA's policies. During FY 2003, SSA conducted reviews of 21 DDS sites.

SSA contracted with an independent public accounting firm to review the Agency's management control program, evaluate the effectiveness of the program and make recommendations for improvement. During FYs 1999-2003, the contractor reviewed operations at SSA's central office, processing centers, all 10 ROs, 162 FOs and 6 PSCs. The contractor's efforts have indicated that SSA's management control review program appears to be effective in meeting management's expectations for compliance with Federal requirements. The contractor did not find any significant weaknesses during this 5-year period.

Financial Management Systems (FMS) Review Program

OMB Circular A-127 requires agencies to maintain an FMS inventory and to conduct reviews to ensure FMS requirements are met. In addition to financial systems, SSA also includes all major programmatic systems in this FMS inventory. Within a 5-year period, SSA conducts both a detailed review and a limited review of each system. An independent contractor conducts the detailed review at audit level standards including transaction testing and the system manager conducts the limited review.

During FY 2003, SSA's contractor conducted detailed reviews of the Debt Management System and the Recovery of Overpayments, Accounting and Reporting System. The systems managers conducted limited reviews of the Social Security Number Establishment and Correction System, the Earnings Record Maintenance System and the Supply System. The results of these reviews did not disclose any significant weaknesses that would indicate noncompliance with laws, Federal regulations or Federal standards.

Federal Financial Management Improvement Act

On July 25, 2003, the Commissioner determined that SSA's financial management systems were in substantial compliance with Federal Financial Management Improvement Act (FFMIA) for FY 2002. In making this determination, she considered all the information available, including the auditor's opinion on the Agency's FY 2002 financial statements, the report on management's assertion about the effectiveness of internal controls and the report on compliance with laws and regulations. She also considered the results of the financial management systems reviews and management control reviews conducted by the Agency and its independent contractor and the progress made in addressing the weaknesses identified in the audit and review reports. That progress is discussed in the section below entitled "Financial Statement Audit."

Under Section 803(c)(2) of FFMIA, the determination for FY 2003 shall be made no later than 120 days after the earlier of (A) the date of receipt of an agencywide audited financial statement or (B) the last day of the fiscal year following the year covered by such statement. We expect to receive the final management letter report(s) for the FY 2003 audit in February 2004.

Federal Information Security Management Act

Federal Information Security Management Act (FISMA) requires Federal agencies to conduct an annual self-assessment review of their information technology security program, to develop and implement remediation efforts for identified security weaknesses and vulnerabilities, and to report to OMB on the Agency's compliance. As in prior years, SSA employed the services of a public accounting firm to perform an independent review of SSA's self-assessments of its 17 sensitive systems. The contractor's evaluation indicated that SSA's self-assessment methodology was consistent with established FISMA requirements. SSA's Office of Inspector general also performed an independent review of SSA's compliance with FISMA and concluded that, with the exception of procedural areas needing improvement, SSA had complied with FISMA requirements. SSA submitted its annual FISMA report to OMB on September 22, 2003.

Financial Statement Audit

The OIG contracted for the audit of SSA's FY 2003 financial statements as it has for the last 7 years. For the tenth year in a row the auditor found that the principal financial statements were fairly stated in all material respects and issued an unqualified opinion. The auditor also found management's assertion that SSA's systems of accounting and internal controls were in compliance with OMB's internal control objectives to be fairly stated in all material respects. Although the auditor identified a reportable condition involving internal controls in FY 2003, it was not identified as material weakness as defined by the American Institute of Certified Public Accountants and OMB Bulletin No. 01-02.

The reportable condition read "SSA needs to further strengthen controls to protect its information." The auditor indicated that SSA had made significant progress in addressing information protection issues raised in prior years. The auditor particularly noted that SSA had implemented enhanced risk models to standardize platform security configurations, implemented new tools and procedures to monitor adherence to standards, reduced the number of servers with known high risk security weaknesses, maintained strong access-based rule settings and standardized monitoring and logging procedures for firewalls, continued progress in implementing a program to monitor and control system user access requirements, continued progress on implementing dataset naming standards and establishing data ownership, and continued progress in planning for continuity of operations in field activities.

Although the auditor noted significant progress in strengthening security controls, it also noted the need for further progress regarding (1) the review of security access assignments, including vetting of access assignments for access to transactions and data, (2) establishment and full use of dataset naming conventions for datasets, (3) establishment of a dataset dictionary for existing datasets and transactions, and (4) enforcement of the new dataset naming rules and standards for sensitive systems. The auditors also note the need for high level test exercises to ensure the viability of the newly drafted high level procedures to move workloads between RO/PSC and DDS sites for continuity of operations purposes.

The auditors recommended that SSA:

- Continue the acceleration of the Standardized Security Profile Project program to ensure that sensitive systems, as defined by the SSA systems accreditation and certification process, are adequately addressed regarding proper access assignments, dataset naming standards, and inclusion in the dataset dictionary;
- Continue to improve physical security controls for the DDS sites; and
- Continue to enhance continuity of operations activities, including testing of newly developed procedures for RO/PSC and DDS sites.

SSA will continue to work with the auditor to improve controls in those areas.