The Social Security Administration's Information Security Program and Practices for Fiscal Year 2026 142603

September 2026 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration's (SSA) information security program and practices were effective and consistent with the *Federal Information Security Modernization Act of 2014* (FISMA) requirements, as defined in the Inspector General (IG) FISMA reporting metrics as of July 31, 2026.

Background

FISMA requires that SSA develop, document, and implement an Agency-wide information security program. The Commissioner of SSA is responsible for providing information security protections commensurate with the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of Agency information and information systems.

FISMA requires that the Office of the Inspector General, or an independent external auditor as determined by the IG, annually evaluate the Agency's information security program and practices to determine their effectiveness.

We engaged Ernst & Young LLP (Ernst & Young) to conduct this performance audit in conjunction with the audit of SSA's Fiscal Year (FY) 2026 Financial Statements.

Results

Ernst & Young found that SSA had made progress in maturing its cybersecurity posture by defining and implementing roadmaps to improve its cybersecurity program. Based on the IG FISMA reporting Metrics guidance, Ernst & Young concluded SSA's overall security program was Consistently Implemented but "Not Effective" for FY 2026.

Recommendations

1. **Inventories:** Continue refining the enterprise architecture system inventory as well as software, hardware, data, and metadata inventories.
2. **Risk Management:** Continue implementing the cybersecurity risk management strategy to obtain a comprehensive assessment of risks to the Agency and follow a standardized process to accept and monitor these risks.
3. **Continuous Monitoring:** Continue assessing applications to ensure SSA includes all its assets within the continuous monitoring scope and improve the vulnerability management process.
4. **Configuration Management:** Continue improving the process for integrating and formalizing risk-based decisions into cybersecurity program monitoring activities.
5. **Privileged Account Management:** Continue improving oversight and management of user accounts.

Office of the Inspector General Comments

In FY 2026, SSA demonstrated a commitment to addressing longstanding challenges to its information security program, which resulted in notable improvements. However, cyber-threats evolve rapidly. As such, it is imperative that SSA ensure its information security controls are appropriately designed and operating effectively.

Agency Comments

SSA stated it will continue to modernize its capabilities, strengthen its controls, rapidly address identified risks, and hold itself accountable for results.