The Social Security Administration's Information Security Program and Practices for Fiscal Year 2025 142501

September 2025 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the *Federal Information Security Modernization Act of 2014* (FISMA) requirements, as defined in the Fiscal Year 2025 Inspector General FISMA reporting metrics as of July 31, 2025.

Background

Under FISMA, SSA must develop, document, and implement an Agency-wide information security program. The Commissioner of Social Security 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 Inspector General, 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 2025 Financial Statements.

Results

Based on the Inspector General FISMA reporting metrics, Ernst & Young concluded SSA's overall security program was "Not Effective." Ernst & Young made this determination because SSA did not meet the *Managed and Measurable* maturity level for five of the six functions: Govern, Identify, Protect, Detect, and Recover.

Recommendations

In addition to the recommendations provided during the performance audit, Ernst & Young recommended SSA focus on five core areas to strengthen its enterprise-wide, cybersecurity program.

1. Continue refining the enterprise architecture system inventory as well as software, hardware, data, and metadata inventories.
2. 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. Implement ongoing authorization to ensure it continuously assesses Agency-wide systems.
4. Continue improving the process for integrating and formalizing risk-based decisions into cybersecurity program monitoring activities.
5. Improve oversight and management of user accounts.

Office of the Inspector General Comments

SSA must improve its risk-management processes and ensure its information security controls are appropriately designed and operating effectively.

Agency Comments

SSA agreed with Ernst & Young's recommendations.