Security Assessment and Authorization Process
A-14-21-51093

September 2024 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration (SSA) was managing its Security Assessment and Authorization (SA&A) process in accordance with Federal and Agency requirements.

Background

The *Federal Information Security Modernization Act of 2014* and Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, require that all Federal agencies institute an agency wide program to secure the information and systems that support their operations and assets, and implement the Risk Management Framework described in National Institute of Standards and Technology Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

SSA's Division of Compliance and Assessments oversees the Agency's SA&A and risk management processes. It monitors the Agency's existing systems, tests selected security controls, and assesses systems every 3 years or when major changes are made. Before SSA releases a new, or significantly revised existing, information system into production, system owners must conduct an SA&A to ensure the information system is operating under an acceptable level of risk and obtain/renew an Authority to Operate.

Results

SSA was managing the following aspects of its SA&A process in accordance with Federal and Agency requirements:

- System owners identified the missions, business functions, and mission/business processes each system was intended to support; the types of information the system was to process, store, and transmit; and all stages of the information life cycle for each information type the system processed, stored, or transmitted.
- The Agency selected the appropriate assessor, who achieved the appropriate level of independence. Additionally, system owners provided the assessor the documentation they needed to conduct the assessments.

However, SSA was not managing the following aspects of its SA&A process in accordance with Federal and Agency requirements:

- The Agency did not apply updated security and privacy controls and had not implemented privacy requirements.
- The Agency had not performed an Agency-level risk assessment, and system owners were not conducting system-level risk assessments.
- The organization-wide continuous monitoring strategy did not identify the required information and had not been approved by a senior Agency official.
- Some Agency personnel did not follow Agency policies and procedures.
- Agency policy and processes did not include the level of detail necessary to ensure stakeholders were aware of their responsibilities.

Recommendations

We made 19 recommendations to help ensure SSA manages its SA&A process in accordance with Federal and Agency requirements.

Agency Comments

SSA agreed with our recommendations.