LIMITED DISTRIBUTION

Security of the Social Security Administration's Cloud Environment
A-14-18-50498

SOCIAL SECURITY ADMINISTRATION
OIG

August 2019 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration's (SSA) cloud environment protected the Agency's sensitive information.

Background

Cloud computing enables convenient, on-demand access to shared computing resources, including networks, servers, storage, applications, and services. As of September 2018, SSA had deployed its on-site-private cloud environment and 22 systems in external cloud environments hosted by 11 cloud service providers. The Agency established an infrastructure system in Amazon Web Services, called Agency Cloud Initiative-Amazon Web, where many of SSA's cloud systems reside. Seventeen of these cloud systems collect, process, maintain, transfer, or store sensitive information.

The Federal Risk and Authorization Management Program (FedRAMP) standardizes how the *Federal Information Security Modernization Act* (FISMA) applies to cloud computing services. When granting security authorizations under FISMA, agencies must ensure all cloud systems that process, transmit, or store Federal information use the FedRAMP baseline security controls by using the *FedRAMP Security Assessment Framework*.

Findings

SSA established policies and procedures to protect its sensitive information in the cloud environment. However, we identified areas of the Agency's cloud security program that needed improvement. Specifically, we identified weaknesses related to risk management, access controls, configuration management, contingency planning, and contract security clauses.

Recommendations

We made 10 recommendations concerning the protection of SSA's sensitive information. Most notably, we recommend SSA:

- Evaluate its procedures to ensure its cloud system inventory is complete and accurate.
- Complete actions to ensure timely and proper assessment, authorization, and re-authorization of cloud systems.
- Enhance guidance for, and oversight of, systems owners and security authorization managers regarding System Security Plan preparation and maintenance of cloud systems, including training for authorization managers on their responsibilities.
- Complete implementation of its continuous monitoring program for cloud environments and educate security authorization managers and system owners of their responsibilities.
- Assess the risk of root accounts for one cloud service provider and implement controls to address the requirements.
- Implement controls to restrict global administrator accounts within one cloud environment and examine whether unauthorized activity occurred.
- Ensure its new procurement guidance integrates appropriate Federal requirements and includes FedRAMP's recommended contract clauses for contracts with cloud service providers.

SSA agreed with our recommendations.