The Social Security Administration's Cloud Computing Environment
A-14-14-24081

SOCIAL SECURITY ADMINISTRATION
OIG

December 2014 **Office of Audit Report Summary**

Objective

To evaluate the Social Security Administration's (SSA) cloud computing technologies with commercial cloud service providers.

Background

Cloud computing offers the potential for significant cost savings through faster deployment of computing resources, a decreased need to buy hardware or build data centers, and enhanced collaboration capabilities. To accelerate the Government's use of cloud computing strategies, the Office of Management and Budget (OMB) requires that agencies adopt a "Cloud First" policy when considering information technology purchases and evaluate secure, reliable, and cost-effective cloud-computing alternatives when making new information technology investments.

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) initiated a project to evaluate select agencies' progress in adopting cloud services. CIGIE will use the results of the reviews conducted by participating Offices of the Inspectors General (OIG) to prepare a comprehensive report and inform agency heads and lawmakers on how well the Government has adopted and leveraged cloud computing.

Findings

In a prior review, we found that SSA had identified Citizen Access Routing Enterprise (CARE) Through 2020 as the Agency's only service in a public cloud. However, in February 2014, SSA informed us it had identified CARE Through 2020 as a private cloud, with a commercial vendor serving as the cloud service provider. Then, in May 2014, the Agency identified CARE Through 2020 as a private cloud with the Agency itself being the cloud service provider.

Because CIGIE's project focused only on commercially provided cloud services and SSA identified itself as the cloud service provider, we determined the Agency did not have applicable cloud services to include in the CIGIE review (however, we still provided CIGIE with SSA's Cloud Computing Initiative survey responses).

CARE Through 2020 is an Ordering Agreement against a contract established by the General Services Administration. We found that neither the Ordering Agreement nor the underlying contract included provisions for granting the OIG direct access to contractor documents and facilities for audit and investigative purposes and lacked non-disclosure agreements from contractor personnel.

Furthermore, there was confusion about whether SSA must comply with Federal Risk and Authorization Management Program (FedRAMP) with its private cloud solutions, including CARE Through 2020.

Matters for Consideration

Given SSA's plans for cloud computing and the confusion about the applicability of FedRAMP at SSA, we believe the Agency should consult with OMB and conclusively determine whether it must comply with FedRAMP requirements. Additionally, as SSA adopts new cloud services, it should ensure contracts comply with Federal guidance and include (1) provisions that grant OIG direct access to vendor documents and facilities and (2) non-disclosure agreements.