OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Evaluation Report

The Social Security Administration's Cloud Computing Environment

A-14-14-24081 | December 2014

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: December 17, 2014

Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration’s Cloud Computing Environment (A-14-14-24081)

The attached final report presents the results of our review. Our objective was to evaluate the Social Security Administration’s cloud computing technologies with commercial cloud service providers.

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O’Carroll, Jr.

Attachment

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.

TABLE OF CONTENTS

ABBREVIATIONS

CARE	Citizen Access Routing Enterprise
CIGIE	Council of the Inspectors General on Integrity and Efficiency
FedRAMP	Federal Risk and Authorization Management Program
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OIG	Office of the Inspector General
SSA	Social Security Administration

OBJECTIVE

Our objective was to evaluate the Social Security Administration's (SSA) cloud computing technologies with commercial cloud service providers.

BACKGROUND

Cloud computing is a general term for delivering hosted technology services over the Internet. The term cloud computing was inspired by the cloud symbol that is often used to represent the Internet in flowcharts and diagrams.

Cloud computing enables on-demand access to shared computing resources (for example, shared networks, servers, storage, and applications) that can be rapidly provided and released with minimal management effort or service provider interaction. The cloud may be owned, managed, and operated by an organization, third party, or combination of the two, and it may exist on or off their premises. Cloud computing can be implemented as a

- **private cloud** that is used by a single organization comprising multiple users (for example, businesses);
- **community cloud** that is used by organizations that have shared concerns (for example, shared missions, security requirements, policy, and compliance considerations);
- **public cloud** that is used by the general public; or
- **hybrid cloud**, which is a mix of any of the above.

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.

Federal Requirements

To accelerate the Government's use of cloud-computing strategies, the Office of Management and Budget (OMB) issued a plan in December 2010 requiring that agencies adopt a "Cloud First" policy when considering information technology purchases by evaluating secure, reliable, and cost-effective cloud-computing alternatives when investing in new information technology.[1] The plan requires that each Federal agency (1) identify three computer services that must move to a cloud and (2) create a project plan for migrating to a cloud solution and retiring the existing systems.[2]

On December 8, 2011, the Federal Chief Information Officer issued a memorandum to all Federal Chief Information Officers establishing the Federal Risk and Authorization Management Program (FedRAMP).[3] FedRAMP, which became operational in June 2012, is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach is expected to save costs, time, and staff required to conduct redundant agency security assessments. FedRAMP could provide SSA with a Government-wide, standardized approach for security assessments, ongoing assessments, authorizations, and continuous monitoring of cloud service providers, if needed.

SSA's Response to "Cloud First"

SSA's Cloud First Plan, issued to OMB in December 2011, identified three cloud initiatives.

1. **Citizen Access Routing Enterprise** (CARE) **Through 2020** provides the Agency with National 800-Number Network call center services. SSA identified CARE Through 2020 as a service in a public cloud.

2. **eVerify** provides employers (and certain others) an automated link to Federal databases to help employers determine whether new hires are authorized to work in the United States. SSA identified eVerify as a service in a private cloud.

3. **American Association of Motor Vehicle Administrators/Help America Vote Verification** fulfills the Social Security number verification services requirement for State Motor Vehicle Administrations and State-level Voter Registration Services. SSA identified this as a service in a private cloud.

[1] OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management*, December 9, 2010.

[2] In September 2012, we issued our evaluation report, *Cloud Computing at the Social Security Administration* (A-14-12-11226). Our objectives were to (1) assess SSA's plan to move computer services to a cloud, (2) determine the risks associated with moving computer services to a cloud, and (3) identify opportunities to save monies by partnering with other Federal agencies in moving computer services to a cloud.

[3] OMB, Memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011, p.1.

Scope and Methodology

In December 2013, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) initiated a project to evaluate select agencies' progress in adopting cloud services. CIGIE planned to 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. Specifically, CIGIE asked participating Inspectors General to obtain an inventory of agencies' cloud service contracts with commercial cloud service providers and select a sample for testing. The participating Inspectors General answered questions on each selected cloud service contract related to terms of service, non-disclosure agreements, service-level agreements, service provider monitoring, cloud service centralized management, and FedRAMP compliance.

To accomplish our objective, we met with SSA staff and requested documentation to complete the CIGIE Cloud Computing Initiative survey. See Appendix A for additional information about our scope and methodology.

RESULTS OF REVIEW

In a prior review, we found that SSA identified 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.[4]

While conducting our review, we identified some issues that we want to bring to the Agency's attention.

Cloud Services Contracts

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 access to contractor documents and facilities for audit and investigative purposes and
- acquiring non-disclosure agreements from contractor personnel.

[4] However, we still provided CIGIE with SSA's Cloud Computing Initiative survey responses.

CIGIE found that participating Federal agencies did not fully consider and implement Federal guidance, agencies' policies, and best practices when developing requirements for cloud-computing contracts. OIG should have access to cloud service providers' facilities and Federal information to perform statutory oversight roles.[5] Further, Federal agencies should require that cloud service providers allow forensic investigation for criminal and non-criminal purposes.[6,7] According to Federal guidance, Federal agencies should ensure contractors sign and adhere to non-disclosure agreements.

Without these provisions, OIG may not be able to ensure contractors meet SSA's security control requirements and collect evidence for criminal investigations should it be necessary to do so. In addition, SSA will not be able to guarantee contractors are safeguarding the Agency's sensitive information.

Federal Risk and Authorization Management Program

SSA personnel informed us that they believed the Agency did not need to comply with FedRAMP because SSA deployed its cloud services in a private cloud. SSA cited the following exception.

> Executive departments or agencies that: (i) select a private cloud deployment model (i.e., the cloud environment is operated solely for the use of their organization); (ii) implement the private cloud on premise (i.e., within a Federal facility); and (iii) are not providing cloud services from the cloud-based information system to any external entities (including bureaus, components, or subordinate organizations within their agencies), are exempted from the FedRAMP requirements.[8]

We contacted the General Services Administration, which informed us that FedRAMP requirements apply to "All cloud deployment models (e.g., Public Clouds, Community Clouds, Private Clouds, and Hybrid Clouds) as defined by the National Institute of Standards and Technology."[9] Therefore, there is confusion about whether SSA must comply with FedRAMP requirements with its private cloud solutions, including CARE Through 2020.

[5] CIGIE, *The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative*, September 2014.

[6] Chief Information Officers Council and Chief Acquisition Officers Council guidance, *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*, February 24, 2012.

[7] CIGIE Information Technology Committee drafted clauses that would ensure OIG audit and investigative access and proposed including the clauses in the Federal Acquisition Regulation to the Federal Acquisition Regulation Council in January 2012.

[8] OMB, Memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011, p.2, Footnote 4.

[9] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011.

MATTERS FOR CONSIDERATION

On June 2, 2014, SSA established a cloud-computing workgroup to develop a hybrid cloud computing strategy for administrative and non-critical workloads. Given SSA's plans for cloud computing and the confusion about the applicability of FedRAMP requirements, 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, the Agency should ensure that contracts comply with Federal guidance and include (1) provisions that grant OIG direct access to vendor documents and facilities and (2) non-disclosure agreements.[10]

[10] In response to our draft report, SSA stated it plans to consult with OMB by the end of the first quarter of 2015 to determine whether it is required to comply with FedRAMP requirements. The Agency will incorporate any suggestions as SSA continues developing its cloud computing strategy. In addition, the Agency stated it will include proper OIG audit access and non-disclosure provisions in applicable contracts.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

Our objective was to evaluate the Social Security Administration's (SSA) cloud computing technologies with commercial cloud service providers.

To accomplish our objective, we

- obtained SSA's cloud computing implementation;
- obtained a copy of the Agency's most recent *Federal Managers' Financial Integrity Act*, PortfolioStat, Exhibit 53C, and Agency Financial Report - Annual Performance Review submissions;
- obtained a copy of the Citizen Access Routing Enterprise Through 2020 Statement of Work and the Authority to Operate the Enterprise Wide Mainframe and Distributed Network Telecommunications Services and System;
- reviewed applicable Federal laws, regulations, and guidelines;
- compared the Agency's documentation to Federal laws, regulations, and guidelines; and
- interviewed SSA subject matter experts to obtain responses to the Council of Inspectors General on Integrity and Efficiency's questions.

We conducted our review between December 2013 and June 2014 in Baltimore, Maryland. We conducted our review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. The principal entity evaluated was the Office of the Deputy Commissioner for Systems.

Appendix B – MAJOR CONTRIBUTORS

Jeffrey Brown, Director

Mary Ellen Moyer, Audit Manager

Cheryl Dailey, Auditor in Charge

Mission

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

Connect with Us

The OIG Website (http://oig.ssa.gov/) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "Beyond The Numbers" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.

Watch us on YouTube

Like us on Facebook

Follow us on Twitter

Subscribe to our RSS feeds or email updates

Obtain Copies of Audit Reports

To obtain copies of our reports, visit our Website at http://oig.ssa.gov/audits-and-investigations/audit-reports/all. For notification of newly released reports, sign up for e-updates at http://oig.ssa.gov/e-updates.

Report Fraud, Waste, and Abuse

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website:	http://oig.ssa.gov/report-fraud-waste-or-abuse
Mail:	Social Security Fraud Hotline P.O. Box 17785 Baltimore, Maryland 21235
FAX:	410-597-0118
Telephone:	1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time
TTY:	1-866-501-2101 for the deaf or hard of hearing