OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

CLOUD COMPUTING AT THE SOCIAL SECURITY ADMINISTRATION

September 2012   A-14-12-11226

EVALUATION REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: September 24, 2012 Refer To:

To: The Commissioner

From: Inspector General

Subject: Cloud Computing at the Social Security Administration (A-14-12-11226)

OBJECTIVE

Our objectives were to (1) assess the Social Security Administration's (SSA) 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.

BACKGROUND

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

According to the National Institute of Standards and Technology (NIST), cloud computing is a model for enabling convenient, on-demand access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1] The cloud may be owned, managed, and operated by an organization, a third party, or a combination of the two, and it may exist on or off the organization's 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 a specific community of individuals from organizations that have shared concerns (for example, mission, security requirements, policy, and compliance considerations);
- public cloud that is used by the general public; or
- hybrid mix of any of the above.

[1] NIST, Special Publication 800-145, *The NIST Definition of Cloud Computing*, p. 2, September 2011.

In a December 2010 publication,[2] the Office of Management and Budget (OMB) mandated a shift to a Cloud First Policy.[3] Each agency's Chief Information Officer (CIO) was required to identify three computer services that must move to a cloud and create a project plan for migrating to a cloud solution and retiring the associated legacy systems.[4] At least one of the three services was required to be fully migrated to a cloud within 12 months [by December 2011][5] and the remaining two computer services within 18 months [by June 2012].[6]

When evaluating options for new IT deployments, OMB requires that agencies default to a cloud-based solution when there is a secure, reliable, cost-effective cloud option.[7] Additionally, OMB stated each migration plan will include major milestones, execution risks, adoption targets, and required resources as well as a retirement plan for legacy systems once cloud solutions are online.[8]

In February 2011, OMB published its *Federal Cloud Computing Strategy,*[9] which required that agencies modify their IT portfolios to fully take advantage of the benefits of cloud computing to maximize capacity use, improve IT flexibility and responsiveness, and minimize cost. Specifically, OMB required that each Federal agency reevaluate its technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process.[10]

SSA submitted its initial Cloud First Plan to OMB in February 2011. That Plan identified three initiatives the Agency planned to migrate to a cloud: Citizen Access Routing Enterprise (CARE) Through 2020,[11] email services, and electronic *Freedom of Information Act* (eFOIA).[12] However, because of budget constraints and additional

[2] OMB, *25 Point Implementation Plan to Reform Federal Information Technology (IT) Management,* December 9, 2010.

[3] "Cloud First" Policy is part of OMB's *25 Point Implementation Plan to Reform Federal IT Management*, Section A, Part 3, pp. 6 through 8. This three-part strategy revolves around using commercial cloud technologies where feasible, launching private Government clouds, and using regional clouds with State and local governments where appropriate. OMB, supra at p. 7.

[4] Id.

[5] Id.

[6] Id.

[7] Id.

[8] OMB, supra at p. 8.

[9] OMB, *Federal Cloud Computing Strategy*, p. 2, February 8, 2011.

[10] Id.

[11] The CARE Through 2020 is replacing SSA's existing Call Center Network solution contract—which provides SSA with National 800 Number Network call center services. For additional details on CARE Through 2020, see Appendix C, pp. 13 and 14.

[12] An automated electronic system used to process FOIA requests and administrative appeals.

analysis, SSA withdrew email services and eFOIA and substituted eVerify[13] and American Association of Motor Vehicle Administrators (AAMVA)/Help America Vote Verification (HAVV).[14] SSA submitted its revised Cloud First Plan to OMB on December 2, 2011. The Plan included CARE Through 2020 as a service in a public cloud and eVerify and AAMVA/HAVV as services in private clouds.

To accomplish our objectives, we interviewed SSA management and staff; compared SSA's cloud computing plan to OMB guidance and standards published by NIST; researched cloud computing benefits and limitations; and contacted other Federal agencies on their cloud experiences. We also identified risks associated with moving computer services to a cloud. We did not limit our identification of risks to the three computer services SSA identified to move to a cloud. For more information on our scope and methodology, see Appendix B.

RESULTS OF REVIEW

Based on our interviews with SSA staff, analysis of the Agency's Cloud First Plan, and inquiries with other Federal agencies, we determined that SSA's Cloud First Plan generally complied with OMB requirements. However, we found the Agency needs to develop a service-based methodology to identify and track costs related to moving computer services to a cloud. For example, for the two computer services implemented in the cloud and the remaining computer service scheduled for implementation in December 2012, the Agency cannot demonstrate that it received an equal or greater return of investment (ROI) when moving these computer services to a cloud. The Agency does not have methodology to identify and track the costs associated with its cloud implementations including the costs associated with the retirement of its legacy systems.

Further, we found the Agency identified execution risks, as required by OMB,[15] for the three computer services planned for cloud implementation, but additional risks may affect the Agency's data and legacy systems.[16] Finally, we determined the Agency had already partnered with some agencies; however, other opportunities existed.

[13] eVerify provides employers (and certain others) an automated link to Federal databases to help employers determine employment eligibility of new hires and to ensure the Social Security number matches the employee's name. For additional details on eVerify, see Appendix C, pp. 15 and 16.

[14] AAMVA /HAVV fulfills the Social Security Number Verification services requirement for State Motor Vehicle Administrations and State-level Voter Registration Services. To meet these parallel requirements, State Motor Vehicle Administrations and Voter Registration offices must verify the applicant's name, date of birth, and Social Security number with SSA. For additional details on AAMVA /HAVV, see Appendix C, pp. 17 and 18.

[15] OMB, *25 Point Implementation Plan to Reform Information Federal IT Management*, § A, p. 8.

[16] We define legacy systems as systems or applications that have been inherited from languages, platforms, and techniques earlier than current technology. For example, this would include applications programmed in Common Business Oriented Language.

Although we identified some concerns, we applaud the Agency for cautiously moving services to the cloud. SSA needs to decide whether the risks associated with moving computer services to a cloud outweigh the benefits to maximize capacity, improve IT flexibility and responsiveness, and minimize cost.

SSA's Cloud First Plan Generally Met Federal Requirements but Could be Improved with the Development of a Service-Based Methodology for Identifying and Tracking Costs

During our review, we found SSA's Cloud First Plan generally complied with Federal requirements. However, we believe the Agency needs to develop a methodology to identify and track costs associated with its cloud implementations.[17]

In its revised Cloud First Plan, the Agency proposed to move three computer services to a cloud:

- CARE Through 2020,[18]
- eVerify,[19] and
- AAMVA/HAVV.[20]

The Agency stated that eVerify and AAMVA/HAVV existed before OMB's Cloud First Policy was issued and were selected to comply with OMB's mandated timeframes.[21] We requested documentation of OMB's approval of SSA's cloud first plan. SSA management stated that based on discussions with OMB, the Agency's plan was approved. However, we determined that OMB never formally approved SSA's plan.

OMB Circular A-130[22] states that Federal agencies must demonstrate a projected return on investment (ROI) that is clearly equal to or better than alternative uses of available public resources. However, SSA's revised Cloud First plan did not document whether moving its computer services to a cloud achieved an equal or greater ROI than maintaining its legacy systems because it did not have an appropriate service-based methodology to identify and track costs associated with its cloud implementations. For example, SSA identified costs for two projects, CARE Through 2020 and eVerify;

[17] OMB, *25 Point Implementation Plan to Reform Information Federal IT Management*, § A, pp. 7 and 8.

[18] The infrastructure is complete, but the transition to SSA's site will not be completed until December 2012.

[19] Service operational January 2011.

[20] Service operational January 31, 2012.

[21] Each agency's CIO was required to identify three computer services that must move to a cloud and create a project plan for migrating to a cloud solution and retiring the associated legacy systems. At least one of the three computer services must be fully migrated to a cloud by December 2011 and the remaining two computer services by June 2012.

[22] OMB, Circular A-130, *Management of Federal Information Resources*, § 8.b(1)(b)(v), p. 12.

however, the Agency identified projected costs rather than actual or service-based costs.[23] Furthermore, SSA did not calculate an ROI for eVerify or AAMVA/HAVV.

We question whether the Agency could calculate an accurate ROI because the Agency does not have an appropriate service-based methodology to identify and track costs associated with moving computer services to a cloud. According to industry best practices, an IT service-based cost approach provides the total cost for a computer service. The service-based cost methodology identifies and tracks IT costs or expenditures and assigns, distributes, or allocates those costs/expenditures to the IT services that generated them. If SSA had a service-based cost methodology, the Agency could determine the cost of the computer service being moved to the cloud. At the time of this review, the Agency could not identify and track costs associated with its cloud initiatives.

SSA identifies and tracks IT project costs using data and inputs from a variety of systems.[24] For many years, we have been concerned about the Agency's inability to identify and track the cost of its systems or IT projects. For example, our 2008 report on the *Reliability and Accuracy of the SSA's Exhibit 300 Submissions to the Office of Management and Budget*[25] stated SSA did not ensure the total costs for its major IT projects were properly estimated and reported in Exhibits 300 to OMB. In one instance, estimated costs were based on incomplete analysis, which made the total estimated project cost significantly different than the actual cost. In another instance, $18.8 million in historical costs for planning was excluded as project cost. Furthermore, our report on *SSA's Software Modernization and Use of Common Business Oriented Language*[26] stated, "SSA *provided no documentation* that its current modernization approach created any additional efficiencies or stabilized its service delivery costs. Nor could SSA provide an allocation between the cost to maintain its legacy systems and its total IT maintenance cost." Without this information, we could not determine whether SSA's investments in IT infrastructure created any additional efficiencies or reduced operation costs. OMB estimates that about $20 billion of the Government's $80 billion in IT spending is potentially targeted for moving computer services to a cloud.

SSA management stated that the Agency built its cloud strategy on a highly virtualized[27] environment, which creates the impression of a device or resource, such as a server or operating system, where the framework divides the resource into multiple execution

[23] See pages C-14 and C-16 in Appendix C.

[24] Indirect and direct cost is administered for IT Systems Cost, Government and Contractor Labor using Automated Purchase Requisition System, Resource Accounting System/Mainframe Time and Attendance System, and Contractor Actuals Reporting System.

[25] SSA OIG, *Reliability and Accuracy of the SSA's Exhibit 300 Submissions to the Office of Management and Budget* (A-14-08-18018), September 30, 2008.

[26] SSA OIG, *The Social Security Administration's Software Modernization and Use of Common Business Oriented Language* (A-14-11-11132), May 17, 2012.

[27] Virtualization is the concept of masking IT resources in a way that the physical nature and boundaries of those resources are hidden from resource users. An IT resource can be a server, a client, storage, networks, applications or operating systems.

environments. Partitioning a hard drive is considered virtualization because one drive is divided into two hard drives. Virtualization is a characteristic of cloud computing; however, it does not fully incorporate all aspects of cloud computing.

Cloud computing uses virtualization to provide computing resources as a service or utility over public, semi-public, or private infrastructures.[28] Virtualization software allows one physical machine to run multiple operating systems. For example, SSA could run Microsoft and UNIX operating systems on the same server thereby reducing the number of servers required for its operations. Moreover, the virtualization software helps provide complete and ongoing cost information to assist SSA in managing its IT budgetary resources and align IT initiatives with Agency business goals.

According to OMB, agencies should take steps during migration to ensure they fully realize the expected value from provisioning cloud services.[29] Further, OMB guidance states that, ". . . [f]rom an efficiency standpoint, legacy applications and servers should be shut down and decommissioned or repurposed."[30] With CARE Through 2020, SSA stated that its National 800-Number Network[31] and Call Center Network Solution[32] were retired. SSA identified sections of its existing eVerify system that were replaced. However, for AAMVA /HAVV, the Agency did not retire any of its legacy systems. To further demonstrate the Agency's operating savings for moving computer services to a cloud, SSA should track and account for cost savings derived from retiring its legacy systems or using them for other purposes. SSA could reinvest the costs saved or realize cost savings by using segments or entire legacy systems to meet other needs that would otherwise require additional outlays.

In summary, we found SSA's Cloud First plan generally complied with Federal requirements. However, since Federal agencies are encouraged to acquire secure, reliable, and cost-effective cloud options, SSA needs to develop a service-based methodology that identifies and tracks the cost for moving computer services to a cloud. This would include the costs of retiring a segment or an entire legacy system. Therefore, we recommend SSA develop a service-based methodology[33] to identify and track costs including the costs of retiring segments or entire legacy systems for all IT initiatives so the Agency can determine whether moving computer services to a cloud provides an equal or greater ROI than keeping the status quo.

[28] Virtualization Special Interest Group PCI Security Standards Council, *Information Supplement: PCI DSS Virtualization Guidelines*, Virtualization Overview, 2.2.6 Cloud Computing, p. 9, June 2011.

[29] OMB, *Federal Cloud Computing Strategy*, pp. 15-16, February 8, 2011.

[30] OMB, *Federal Cloud Computing Strategy*, p. 16, February 8, 2011.

[31] SSA's National 800 Number Network provides toll-free telephone service to members of the public.

[32] SSA's Call Center Network solution allows routing of calls to the next available agent at any network site.

[33] The Agency should first determine whether the service-based cost allocation methodology is cost effective.

Risks to Agency Data When Moving Computer Services to a Cloud

SSA met OMB requirements by identifying execution risks associated with moving CARE Through 2020, eVerify, and AAMVA /HAVV to a cloud (see Table 1).

Table 1: SSA Identified Execution Risks

Risk Description	CARE Through 2020	eVerify	AAMVA/HAVV Verification
Acquisition or installation of storage to support the new node is not timely			•
Database migration failure		•	
Incomplete management information systems	•		
Incomplete supporting application development and testing	•		
Internet Data Center construction incomplete or not-operational	•		
Load balancing configurations failure		•	
Network connectivity not completed timely			•
Production execution scripts failure		•	
Routing configurations failure		•	
Scope change requests	•		
SSA data processing fails to account for transactions flow through the Second Support Center [34]			•
SSA's recipient master file data replication incomplete.			•
System migration failure		•	

SSA needs to consider all potential risks to its data or legacy systems when moving computer services to a cloud. To assist the Agency, we provide a list of the risks associated with moving computer services to a cloud in Appendix D. The list is not all-inclusive; therefore, SSA should continue to consider all potential risks to its data or legacy systems before moving future computer services to a cloud.

Opportunities to Partner with Other Federal Agencies

SSA partnered with the Department of Homeland Security (DHS) and State MVAs on eVerify and AAMVA/HAVV. In addition, SSA had data exchange agreements with DHS and State agencies to access and match SSA's data. Moreover, SSA provided network

[34] The Second Support Center is a co-processing facility that works hand-in-hand with the National Computer Center to process critical agency workloads, and each center acts as the disaster backup for the workloads of the other center.

and IT support services to the Office of Child Support Enforcement and limited IT support and services to the Railroad Retirement Board and Centers for Medicare and Medicaid Services.

We contacted nine Federal agencies[35] to obtain their experiences and lessons learned from moving computer services to a cloud. Two of the nine agencies implemented a public cloud service while seven agencies moved computer services to either a private, community, or hybrid cloud. SSA implemented a private cloud service for eVerify and AAMVA/HAVV. This was consistent with the nine agencies we contacted. Agency representatives provided their experiences and lessons learned from moving computer services to a cloud. These experiences and lessons learned were as follows.

- Realizing consumption of cloud services requires a shared responsibility and governance.
- Understanding accountability and compliance with Government requirements cannot be outsourced.
- Understanding the division of security responsibilities between provider and client, and the ability to verify that both are met.
- Realizing certification and accreditation process is new for cloud vendors as well as time consuming.
- Adhering to directives, legislation, policy, and procedures to ensure appropriate analysis, reviews, and procedures are conducted.
- Involving end user community in the decision process for migrating computer services to a cloud.
- Completing documentation ahead of time for any service level agreements and Request for Information.[36]

Cloud Initiatives of Other Federal Agencies

Other Federal agencies have implemented cloud computing services. The Department of the Interior implemented an Infrastructure as a service[37] offering called the National Business Center Grid,[38] which allowed end users to procure a variety of servers and

[35] The Agency for International Development; DHS; Departments of Agriculture, Commerce, the Interior, and Veterans Affairs; Environmental Protection Agency; General Services Administration; and Internal Revenue Service.

[36] A Request for Information is a standard business process used to collect written information about the capabilities of various suppliers.

[37] Infrastructure as a service refers to a hosting, software, hardware, procurement, and services needed to run a cloud.

[38] Hannah Wald, *Cloud computing for the Federal Community*, IAnewsletter, (13/2), Vol. 13, No. 2, (Spring 2010). http://iac.dtic.mil/iatac/download/Vol13_No2.pdf.

operating systems through a single cloud portal. DHS implemented SharePoint as a service offering and implemented more than 50,000 emails to a cloud.[39]

The National Oceanic and Atmospheric Administration contracted with a Maryland company to unify its email and collaboration tools using Google Apps for Government. The National Oceanic and Atmospheric Administration's email and collaboration tools serve about 25,000 users. The Securities and Exchange Commission reduced the time to resolve cases by up to 75 percent by migrating the Office of Investor Education and Advocacy to Salesforce.com, a customer relationship management software. This software cloud initiative allowed its employees to handle customer queries from any location and manage their workflows. The National Archives and Records Administration contracted with a technology firm to build a self-service Website for citizens who need help resolving eFOIA proposal requests.[40]

Federal Risk and Authorization Management Program

The Federal Risk and Authorization Management Program (FedRAMP) was established on December 8, 2011 via an official memorandum from the Federal Chief Information Officer to all Federal CIOs. FedRAMP was operational as of June 2012. FedRAMP is a Governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will save costs, time, and staff required to conduct redundant agency security assessments. FedRAMP could provide the SSA with a Governmentwide, standardized approach for security assessments, ongoing assessments, authorizations, and continuous monitoring of cloud service providers, if needed.

We applaud SSA for its outreach and partnering with other agencies. However, we believe more outreach opportunities exist that could provide additional experiences and lessons learned from moving computer services to a cloud. Therefore, we recommend SSA continue reaching out to officials responsible for FedRAMP; other Federal, State, and local government agencies; as well as private industry to obtain best practices and lessons learned before moving its computer services to a cloud.

CONCLUSION AND RECOMMENDATIONS

Each Federal agency is required to re-evaluate its technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process.[41] SSA's Cloud First Plan generally complied with Federal requirements, but improvements are needed in estimating and tracking costs. Additionally, SSA identified execution risks for each of its three proposed cloud initiatives as required by OMB.

[39] *Cloud Computing, Front and Center*, CIO.gov, (June 15, 2012) http://www.cio.gov/pages.cfm/page/Cloud-Computing-Front-and-Center .

[40] *5 Big Cloud Migration Projects*, Government Executive, (March 1, 2012) http://www.govexec.com/reports/five-big-cloud-migration-projects/41288/.

[41] OMB, *Federal Cloud Computing Strategy*, p. 2, February 8, 2011.

However, we identified additional risks to the Agency's data or legacy systems that SSA should consider when expanding computer services to a cloud. Finally, the Agency partnered with other agencies, but additional opportunities exist for the Agency to partner in the future. Therefore, as the Agency continues to develop its cloud computing implementation plans, we recommend SSA:

1. Develop a service-based methodology to identify and track costs including the costs of retiring segments or entire legacy systems for all IT initiatives so the Agency can determine whether moving computer services to a cloud provided an equal or greater ROI than keeping the status quo.

2. Consider all potential risks to its data or legacy systems before moving future computer services to a cloud.

3. Continue reaching out to FedRAMP program officials; other Federal, State, and local government agencies; as well as private industry to obtain best practices and lessons learned before moving its computer services to a cloud.

AGENCY COMMENTS

SSA disagreed with our recommendations. See Appendix E for the full text of the Agency's comments.

In reference to Recommendation 1, the Agency stated it disagreed with our recommendation because SSA is currently investigating the feasibility and cost effectiveness of implementing a service-based cost allocation methodology to complement the Agency's existing IT cost tracking mechanism. SSA further stated it intends to identify the most productive, technically feasible, and cost-effective strategies for the development and deployment of the processes and tools that may be required to identify and track the costs of IT business services delivered to the Agency's community.

In reference to Recommendation 2, the Agency stated it disagrees with our recommendation because it has taken comprehensive measures to ensure appropriate and effective risk assessment and mitigation for all IT projects. Additionally, the security and privacy control deployed to protect information assets incorporates and exceeds the additional risk categories identified in the report.

Finally, in reference to Recommendation 3, the Agency stated it disagreed with our recommendation because it actively engages in efforts to identify and refine private industry cloud computing best practices. Further, the Agency stated that it evaluates lessons learned from early adopters at any level of Government or the private sector. Additionally, SSA stated that industry best practices and lessons learned play a prominent role in the evolution of its cloud computing strategies and implementation plans.

OIG RESPONSE

Although the Agency response to Recommendations 1 and 3 indicate disagreement, the planned course of action addresses the concerns we have raised. For Recommendations 1 and 3, the Agency's detailed response contradicts its "disagreement" to our recommendations. For Recommendation 1, SSA disagrees with developing a service-based methodology when the Agency's is in fact ". . . investigating the feasibility and cost effectiveness of implementing a service-based cost allocation methodology . . . ." Further, for Recommendation 3, SSA disagreed to continue its outreach efforts, but stated in its response ". . . we actively maintain an ongoing relationship with the General Services Administration, OMB, and the Federal Risk and Authorization Management Program (FedRAMP) officials to ensure that our cloud computing initiatives and activities remain consistent with Federal policies, guidelines, and security provisions."

While SSA stated that it disagreed with Recommendation 2, the Agency's detailed response stated

> We have an existing private cloud IT environment protected by a comprehensive defense-in-depth security architecture. . . . We have taken comprehensive measures to ensure appropriate and effective risk assessment and mitigation for all IT projects. The security and privacy controls we deployed to protect our information assets, incorporate and exceed the additional risk categories identified in the report.
>
> . . . we also recognize the immaturity of public cloud computing offerings. . . . Therefore, we continue to maintain a highly vigilant posture with respect to the effective protection of these systems and assets since the deployment of any cloud-based solution may affect them.
>
> . . . Our current security controls and standards continue to apply whether we deliver IT services through our internal, private cloud; through an external, public cloud; or through some hybrid of both.
>
> Our cloud computing strategy continues to address relevant statutory and policy requirements associated with Federal IT systems, including IT security and risk management; privacy; data integrity; legal issues; records management; OMB and the National Institute of Standards and Technology guidelines and recommendations; and other applicable requirements.

The OIG believes that as long as these efforts are completed timely and effectively, they will address this recommendation.

Patrick P. O'Carroll, Jr.

Appendices

Appendix A

Acronyms

AAMVA	American Association of Motor Vehicle Administrators
CARE	Citizen Access Routing Enterprise
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
DHS	Department of Homeland Security
eFOIA	Electronic *Freedom of Information Act*
FedRAMP	Federal Risk and Authorization Management Program
GAO	Government Accountability Office
HAVV	Help America Vote Verification
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ROI	Return on Investment
SP	Special Publication
SSA	Social Security Administration

Scope and Methodology

To accomplish our objective, we limited our review to the three computer services the Social Security Administration (SSA) identified as moving to the cloud. We identified risks associated with moving any type of computer service to a cloud. We did not limit our identification of risks to the three computer services SSA identified to move to the cloud.

We also:

- Interviewed SSA Systems staff responsible for the Agency's cloud computing services.
- Obtained and reviewed SSA's original and revised Cloud First Plan.
- Interviewed personnel at nine Federal agencies.
    - Agency for International Development
    - Department of Agriculture
    - Department of Commerce
    - Department of Homeland Security
    - Department of the Interior
    - Department of Veteran Affairs
    - Environmental Protection Agency
    - General Services Administration
    - Internal Revenue Service

We also examined:

- Office of Management and Budget (OMB), *Federal Cloud Computing Strategy*, February 8, 2011.
- OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management,* December 9, 2010.
- OMB, Circular A-130. *Management of Federal Information Resources,* November 28, 2000.
- OMB, Circular A-11, Section 210, *Preparing and Submitting an Agency Strategic Plan*, August 18, 2011.
- OMB, Circular A-11, Section 300, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, August 18, 2011.

- OMB, Circular A-11, Section 53, *Information Technology and E-Government*, August 18, 2011.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011.
- NIST, SP 500-291*, NIST Cloud Computing Standards Roadmap*, July 2011.
- NIST, SP 500-292*, NIST Cloud Computing Reference Architecture*, September 2011.
- NIST, SP 800-146, *FINAL Cloud Computing Synopsis and Recommendations*, May 2012.

We performed our evaluation during September 2011 through June 2012 in Baltimore, Maryland. The entity evaluated was the Office of the Deputy Commissioner for Systems. We conducted our review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Appendix C

SSA's Cloud First Plan

Cloud First Plan

(Revised and Updated)

December 2, 2011

TABLE OF CONTENTS

1. Executive Summary

In December, 2010 Vivek Kundra published his Twenty-Five Point Plan for Reforming Federal IT Management. In that Plan, OMB mandated that:

Each Agency CIO will be required to identify three "must move" services and create a project plan for migrating each of them to cloud solutions and retiring the associated legacy systems. Of the three, at least one of the services must fully migrate to a cloud solution within 12 months and the remaining two within 18 months.

Each migration plan will include major milestones, execution risks, adoption targets, and required resources, as well as a retirement plan for legacy services once cloud services are online.

In February, 2011, the Social Security Administration (SSA) submitted its original Cloud-First Plan to OMB and identified three initiatives that the Agency planned to migrate to a cloud solution or that represented an extension of, or enhancement to, an existing cloud solution:

- CARE Through 2020
- eMail Services
- eFOIA

Due to subsequent budget developments and additional analysis, SSA is removing eFOIA and the Agency's eMail services from its Cloud-First Plan at this time and substituting the eVerify and American Association of Motor Vehicle Administrators (AAMVA) solutions for its Cloud First Plan. This decision is based on multiple factors in each case.

eFOIA

An automated electronic system (eFOIA) supports SSA's management of its obligations under the Freedom of Information Act (FOIA). The Agency's staff use the eFOIA system to process requests and administrative appeals within the timeframes mandated by the statute and to minimize backlogs at the end of each fiscal year. The existing eFOIA system is an internally developed and maintained system that uses Global 360 (G360) – a custom tailored, commercially available software (customized COTS) solution. Software licenses and associated infrastructure are supplied under existing, competitive-procurement vehicles. The eFOIA system is based on aging architecture and infrastructure. Future costs are expected to increase and the long term viability of the system will diminish. The existing system needs to be retired as soon as it is feasible to do so. However, it does continue to meet its baseline goals and to deliver its expected benefits.

In expectation of a near-term replacement of the Agency's existing eFOIA system, SSA personnel evaluated the five-year life cycle costs of seven options/alternatives to the existing system. Cost estimates for the proposed alternatives were based on market research of the potential offerors specializing in FOIA COTS. In addition, SSA evaluated each of these alternatives on the basis of qualitative measures.

This analysis indicates that a COTS product – which could be deployed under one of multiple cloud-based model options – would have the greatest qualitative value for the Government. SSA understands that other Federal agencies (e.g., HUD and VA) have developed and/or deployed an eFOIA system that might, with minimal adaptation, meet SSA's existing and future needs. It was further noted that such an approach would be fully consistent with OMB's Cloud First policies.

However, severe limitations in funding and staff resources necessitate suspending the project for FY 2012. SSA's existing eFOIA system continues to meet its base requirements and the Agency has no alternative but to allocate its limited resources to other initiatives that have more critical or urgent needs and that must therefore take a higher priority.

eMail Services

Subsequent to submission of SSA's original Cloud First Plan, additional planning and analysis concluded that the Agency's existing eMail services are not a good candidate (at this time) for migration to a public cloud model for several reasons:

- They are deeply integrated with other services applications, processes and functions – including identity verification services, user authentication and authorization services, access controls, collaboration and communications services, etc.;
- They are an integral component of SSA's unified communications service strategy and architecture;
- They are used for mission-critical case processing management services and functions;
- Users and user groups are not well segmented with common requirements within each segment – a basic requirement for successful migration to a public cloud solution;
- Personally identifiable information (PII) – some of which includes highly sensitive medical records – cannot be exposed to a potential breach of privacy by allowing such information to reside anywhere other than within SSA's own environment;
- SSA's existing eMail service cost less than the projected costs for similar services from a public cloud provider.

SSA will continue to extend and enhance its eMail services within the context of its broader unified communications suite of services. These ongoing activities extend beyond the timeframes specified by OMB in the 25 Point Plan. Accordingly, the Agency must withdraw eMail (as a stand-alone utility) from consideration as a Cloud-First initiative.

SSA is continuing its implementation of CARE Through 2020 – a cloud telephony service that will significantly enhance the Agency's public services.

To replace eFOIA and eMail services as Cloud First initiatives, SSA identified two other initiatives, each of which is a component of the Agency's SSN Verification Services. These initiatives are described in the relevant section below.

SSA 's Overall Cloud Computing Strategy

SSA considers the advent of Cloud Computing as an effective and evolutionary model to enhance and extend the information and IT services it delivers to its end-users, business partners, and customers. Going forward, SSA's strategy is to adopt Private Cloud Computing as the model that is most consistent with its mission and its business operations models. This strategy allows SSA to leverage Cloud Computing in order to extend the service capabilities of its existing IT environment. The use of the Cloud Computing model – consistent with the Agency's risk management framework and its certification and accreditation standards – is encouraged within the framework of SSA's centrally managed enterprise architecture governance as well as its IT service acquisition and source selection processes.

- The Agency's current security controls and standards will continue to apply – no matter what hosting/sourcing decision is being made – i.e., whether IT services are being delivered through the Agency's internal, private cloud; through an external, public cloud; or through some hybrid combination of both.
- SSA's Cloud Computing strategy will continue to address relevant statutory and policy requirements associated with Federal IT systems – including IT security and risk management; privacy; data integrity; legal issues (e.g., Terms of Service); records management; OMB and NIST guidelines and recommendations; and other applicable requirements.

SSA's commitment to protecting personally identifiable information (PII) remains a key component of the Agency's Cloud Computing strategy and is built into the operation and management of its existing private cloud services environment.

2. Background

SSA is utilizing Cloud Computing as an effective and evolutionary model to enhance and extend the information and IT services it delivers to its end-users, business partners, and customers.

SSA is a single-mission Agency. Its core business processes (i.e., Enumeration, Earnings, Claims, Post-Entitlement, Informing the Public, and Identity/SSN Verifications) are tightly inter-woven. They are also highly complex in their information flow and relationships. The data and information requirements of these core business processes, and their mutual inter- dependencies, require an IT service environment that provides information and services based on common platforms, re-usable service modules, robust any-to-any network systems and back-end IT infrastructure. Additionally, given the sensitive nature of the highly personal information and data within SSA's systems of records, data integrity and security as well as the protection of individual privacy are critical IT service requirements.

The design and management of SSA's IT service environment have evolved over time. As a result of that evolution, the environment has substantially taken on the characteristics of a Private Cloud Computing model as defined by the National Institute of Standards and Technology (NIST):

- Utilizing SSA's IT services environment, end-users do not need to determine their exact resource requirements. Through secure access to the Agency's network systems, they are provided the necessary communications and computing resources they require, on demand;
- Through effective monitoring systems, load-balancing mechanisms and automatic failover capabilities, the design and operation of SSA's IT infrastructure and platforms – hosted in two highly virtualized data centers – provide for streamlined and optimized resource utilization and management;
- IT service resources are pooled to a significant degree. They are shared across large numbers of application and organizational configurations and serve a broad spectrum of service consumers;
- SSA's Service Orchestration and Management model leverages SSA's highly configured and largely virtualized data centers, allowing the Agency to consolidate workloads and applications on a centrally managed and operated IT infrastructure;
- The capacity of network and telecommunications systems and computing services is provisioned to respond to variations in demand across programmatic and administrative applications;
- Systems capacity requirements are efficiently planned for, and pro-actively acquired, to meet increasing workload demands through effective management of Resource Allocations and Controls;

- Redundant resources support high availability and reliability as well as to provide IT operational assurance, even in the event of a catastrophic outage within a specific data center.

SSA’s IT services are centrally managed through:

- Deployment, configuration, management and operation of programmatic and administrative software applications in such a manner that these services are provisioned at expected service levels;
- Management of computing services, storage, and network systems infrastructure and platforms such as servers, databases, runtime software execution stacks, and middleware components;
- Provision of integrated pre-production environments for both programmatic and administrative application development, validation and testing;
- Change Management and Production-Release Management processes applied to infrastructure, platforms, applications and services;
- Provisioning and acquisition management of mainframe, open/distributed servers, network system components, storage, and application and database hosting infrastructure;
- Provisioning and management of a robust Security and Privacy architecture for the protection of SSA’s sensitive and personally identifiable information (PII).

The SSA community represents multiple groups of service consumers/end-users with many needs and requirements. SSA accordingly delivers a broad range of IT services that are carefully orchestrated to meet the needs of each of these groups. SSA’s end-users, partners and customers have a broad range of network access options to obtain an equally broad range of IT services and computing capabilities tailored to their specific needs. Services are provided on demand (as appropriate) at each of the service layers to which the individual end-user or customer has access.

To a substantial degree, the Agency’s IT resources are pooled to meet the needs of these multiple users. Through the deployment of load balancing and automatic failover capabilities, IT resources can be dynamically allocated to adjust to variations in peak end-user/customer demand. SSA’s IT service capabilities – particularly within its highly virtualized mainframe environment – can be rapidly and elastically provisioned. SSA’s various cloud systems monitor, control and optimize IT resource utilization.

The following are some of the services SSA currently provides to its end-users, customers, or business partners:

- Programmatic application services directly associated with SSA's core business processes;
- A unified communications suite including eMail, video-teleconferencing, video training, collaboration environments, etc.;
- Document Management Services;
- Office Productivity and Workload Management Services;
- Integrated Case Processing Management Services;
- Communication and Collaboration Services;
- Remote Access Services;
- Project Management Services;
- Business Intelligence Services;
- Financial Management Services;
- Database Access and Management Services;
- Application Development, Validation and Testing Services;
- Application Deployment Services;
- Integration and Interoperability Testing Services;
- Disaster Recovery Services;
- Backup and Recovery Services;
- Information and Data Storage Services;
- Platform Hosting Services;
- Computing Services;
- Identity Verification Services; and
- Authentication Services.

SSA has substantially improved resource utilization; streamlined demand management; increased the availability, reliability and responsiveness of the services it delivers. The evolution of SSA's shared-service IT environment toward a Private Cloud Computing model has allowed the Agency to capitalize its benefits in terms of efficiency, agility, and innovation. By further leveraging Private Cloud Computing principles, SSA will continue to exploit significant economies of scale, provisioning its IT resources to meet increasing service delivery demands with minimal overhead while leveraging the underlying capacity of the Agency's enterprise-level IT resources through a state-of-the-art network architecture.

3. SSA's Cloud Computing Strategy

SSA is adopting a Private Cloud Computing model because it is seen as most consistent with its mission and its business operations models. This strategy allows the Agency to effectively leverage the Cloud Computing model in order to extend the service capabilities of its existing IT environment. Resources permitting, SSA's planned Cloud Computing initiatives include, but
are not limited to:

- Further enhancing dynamic scaling capabilities and processing capacity provisioning by continuing with network virtualization and server virtualization/consolidation initiatives;
- Incorporating highly sophisticated technological enhancements to the IT infrastructure, systems and platforms – including statelessness, low coupling, modularity, and semantic interoperability;
- Improving the provisioning, performance, agility, resilience and scalability of SSA's network systems through unified cabling infrastructure, and network convergence and virtualization;
- Enhancing IT service measurement capabilities through greater instrumentation of the infrastructure and the applications, data and services it supports.

SSA will continue to ensure that existing mission-critical services, strategic goals and business operation requirements are delivered at levels that meet or exceed requirements while simultaneously protecting the security, integrity and privacy of information and data assets. The Agency's commitment to protecting personally identifiable information (PII) is a key component of its Cloud Computing strategy.

SSA encourages the use of the Cloud Computing model, consistent with its:

- Risk management framework;
- Certification and accreditation standards;
- Centrally-managed enterprise architecture governance model; and
- IT service acquisition and source selection processes.

SSA's current security controls and standards will continue to apply – no matter what hosting/sourcing decision is being made – i.e., whether IT services are being delivered through the Agency's internal, private cloud; through an external, public cloud; or through some hybrid combination of both. The Agency's Cloud Computing strategy must continue to address relevant statutory and policy requirements associated with Federal IT systems – including IT security and risk management; privacy; data integrity; legal issues (e.g., Terms of Service); records management; OMB and NIST guidelines and recommendations; and other applicable requirements.

Multiple strategic and operational considerations will govern the way SSA leverages and extends the capabilities of its existing IT environment as it continues its migration to a Private Cloud Computing environment:

Workload Optimization

SSA's computing services platform and its network infrastructure will be configured for optimized workload management.

- Mainframe and distributed platform environments will continue to leverage their respective strengths;
- The mainframe platform will continue to be favored for dense, mission-critical, high volume batch operations;
- Applications will be hosted on the platform most suited to the data they must access and the type of work (I/O, user interface, transaction-based) they must perform;
- State-specific applications are being consolidated or replaced in favor of Service Oriented Architecture (SOA) model services that can be reused and assembled to suit state-specific processes;
- Distributed platform components will continue to be virtualized and consolidated to provide higher levels of availability, resource utilization, and elasticity of capacity.

IP-based Network Service Delivery

The Agency's any-to-any, dual-stack, IPv4/IPv6 network architecture will continue as a hybrid public/private cloud infrastructure.

- Network systems will converge toward a single infrastructure supporting data, voice, and video traffic;
- Utilizing the Internet Protocol (IP), the Agency's converged network will provide enhanced features in terms of telephone services, video capabilities, and data exchange and analysis.

Utilization of Public Cloud Resources Where Appropriate and Cost Effective

Sourcing options for the delivery of IT services include consideration of critical requirements. SSA continues to include consideration of cloud-based services that may be more cost- effectively delivered through an external resource – either another Government Agency or a commercial provider/vendor, as long as:

- There is no Personally Identifiable Information (PII) or other mission critical data involved; AND
- The choice of a public/hybrid cloud model is cost-effective with a clear and demonstrable Return on Investment (ROI) to the Agency.

As with any IT service/sourcing project, the use of public or hybrid clouds requires a formal cost-benefit analysis to demonstrate a positive value (i.e., return on investment (ROI)) as well as appropriate security and privacy review and approval where PII may be a concern.

Utilization of Technologies Related to Cloud Computing

SSA's IT planners and engineers continue to focus their efforts on evaluating and deploying enhanced IT solutions that leverage network-delivered, web-based services to users and to the public through a broad spectrum of end-user devices and network interfaces.

The Agency's existing IT environment will continue to leverage the benefits of virtualization, consolidation, and workload optimization to increase resource utilization and processing efficiency.

On an ongoing basis, the Agency will continue to enhance the flexibility and agility of its existing IT services and infrastructure through deployment of new technologies as they are found to support and enhance SSA's service delivery models and channels.

SSA continues to evaluate IT services and business operations activities to identify those that that might be better provided by external partners whose services and capabilities meet the specific requirements of the Agency and the Federal Government at large. This evaluation focuses on areas where the existing IT environment is not well suited to meet exigent demands.

Leveraging Cloud-based IT Service Delivery and Management

- IT operations management will continue its emphasis on service delivery and management.
- New and evolving technologies will be evaluated and deployed based on their value in enhancing and extending the services provided to SSA’s end-user communities.
- Consideration and evaluation of IT service delivery include an assessment of activities or services that might be good candidates for greater standardization, outsourcing, and/or deployment within a Cloud Computing service model.
- Consideration of Cloud Computing resources will continue to represent one of the available means to provide, extend and enhance high quality IT services to the Agency’s end-users.

Implementing Cloud-based IT Acquisitions Policies and Procedures

- IT acquisition and sourcing policies and procedures ensure that valid and demonstrable business value remains the foundation for all decisions regarding the deployment of IT services and solutions (including those that are cloud-based).
- The development, acquisition, and deployment of IT solutions and services will continue to be based on robust and mature business value considerations – specifically a thorough analysis of costs, benefits, and expected return on investment (ROI).
- While SSA’s IT services environment is highly cost-effective, senior managers and Agency executives continue to evaluate IT-related proposals in terms of the most cost-effective delivery model and will consider the costs and benefits of Cloud Computing solutions within strategic planning and source modeling.

By coordinating these strategic elements within planning and IT service delivery and operations management, SSA expects to continue to reap the benefits of the Cloud Computing model.

4. Designated Cloud-First Projects

In response to OMB's December 2010 directive, SSA has identified three initiatives, which are described in the following sections.

4.1. CARE Through 2020

On September 30, 2010, the CARE Through 2020 contract was awarded to at&t. CARE Through 2020 is a cloud telephony solution that is replacing National 800 Number (N8NN) and the Call Center Network Solution (CCNS). CARE Through 2020 allows SSA to achieve a number of economies by consolidating the two existing contracts into a single acquisition vehicle.

CARE Through 2020 is being deployed to provide and enhance the telephone services the Agency provides to the public. The infrastructure for the CARE Through 2020 system is being deployed on the contractor's network and is flexible enough to support future computer- telephony integrated (CTI) services, such as click to talk, web co-browse, and web chat technologies. These services will significantly increase the public's options to interact with the Agency's contact centers.

The public cloud services architecture of CARE Through 2020 includes:

- A vendor-hosted IP voice call/contact center;
- All functionality currently provided by FTS2001 and CCNS;
- Approved new functionality as offered in SSA's Telephone Services Strategic Plan;
- Capability to integrate additional agent contact channels upon approval of funding.

Scheduled implementation of CARE Through 2020 is on target for completion in the May/June, 2012 timeframe.

<u>Major Milestones</u>

SSA's original Cloud Computing Strategy Plan projected that the initial rollout of the CARE Through 2020 project would be completed by the end of December, 2011. However, issues related to the final contract award delayed the start of the project. As a result, the current projected date of completion is the third quarter of FY 2012 (i.e., approximately the May/June timeframe).

Execution Risks

- Internet Data Center construction incomplete or not-operational
- Scope Change Requests
- Supporting application development and testing incomplete
- Management information systems incomplete

Lifecycle Cost Estimate

Initial Acquisition:	$ 20,674,000
Transition Costs:	$ 38,381,000
FY 2012 Operations & Maintenance:	$ 58,088,000
FY 2013 Operations & Maintenance	$ 59,290,000
FY 2014 Operations & Maintenance	$ 60,635,000
FY 2015 Operations & Maintenance	$ 62,754,000
FY 2016 Operations & Maintenance	$ 64,941,000
FY 2017 Operations & Maintenance	$ 67,215,000
FY 2018 Operations & Maintenance	$ 69,571,000
FY 2019 Operations & Maintenance	$ 71,997,000
Total	$573,546,000

NOTE: SSA's initial cost estimate for CARE Through 2020 ($ 630,344,000) included $56,798,000 Operations and Maintenance costs for FY 2011. Because of delays in contract award, the transition period was extended into FY 2012. The estimate above does not therefore include the planned FY 2011 Operations and Maintenance costs.

Legacy Retirement Plan

With the deployment of CARE Through 2020, SSA's existing N8NN and CCNS solutions will be retired in favor of the single, streamlined service.

4.2. eVerify High Availability Platform

eVerify provides employers (and certain others) an automated link to federal databases to help employers determine employment eligibility of new hires and to ensure the Social Security number matches the employees name. It is currently free to employers and is available in all 50 states. eVerify is operated by the U.S. Citizenship and Immigration Services (USCIS) – a component of the Department of Homeland Security (DHS) – in partnership with the Social Security Administration (SSA).

In operational terms, DHS/USCIS provides eVerify's front-end interface with the customer (i.e., the employers and certain others). SSA provides DHS/USCIS the back-end infrastructure and database systems that actually perform the verification. This back-end infrastructure, platform and software/database system is comprised of a physical layer and an abstraction layer. The physical layer is designed to provide load balancing between SSA's data centers and features fully automatic fail-over, dynamic capacity allocation capability, etc. This back-end infrastructure is accessed by DHS/NSCIS over a secure Internet connection. The abstraction layer is designed to support the software and database systems that operate across the physical layer (i.e., the hardware and network connections).

A Service Level Agreement (SLA) between SSA and DHS/NSCIS governs the operation of this verification service. The latter Agency reimbursed SSA for the design, construction and deployment of the isolated environment in which the back-end eVerify system operates. It reimburses SSA on an annual basis for maintenance, operations and administration of the system.

SSA has completed the deployment of a second eVerify node in its Second Support Center (SSC) to enhance the availability, performance and reliability of the services provided to DHS/NSCIS. The creation of this second node in a geographical dispersed location eliminates planned downtime and enhances the performance availability and reliability of the system.
The implementation of this project was completed in January, 2011.

<u>Major Milestones</u>

- Target Architecture Design Completion: 06/30/2010
- Complete Required Hardware/Software Acquisitions: 11/30/2010
- Begin Construction of Integration Region on High Availability Sysplex: 12/01/2010
- Begin Construction of Production Region on High Availability Sysplex: 12/11/2010
- Complete Migration from MISF to HAF/iHAF: 01/15/2011
- Verify operational status on HAF/iHAF: 01/17/2011
- Configure Global Load Balancing: 01/22/2011
- Evaluate Performance and Response Times: 01/31/2011

Lifecycle Cost Projections

SSA's life cycle cost estimate for fiscal years 2010 through 2015 of almost $66 million includes:

- Approximately $14 million in costs that have already been incurred for developing the Isolated Environment, which was designed for dedicated use by DHS;
- $18 million for fiscal years 2010 through 2013 to maintain this system; and
- $34 million for fiscal years 2010 through 2015 to provide administrative support to SSA field offices and a toll-free number to respond to inquiries.

Under the terms of the SLA with DHS, SSA is fully reimbursed for these costs. Execution Risks

- Production Execution Scripts Fail
- Routing Configurations Fail
- Load Balancing Configurations Fail
- System Migration Failure
- Database Migration Failure

Legacy Retirement Plan

The instances of eVerify in the Integration and Production regions of the MISF have been removed.

4.3. AAMVA/HAVV Verification Services

State Motor Vehicle Administrations (MVAs) which are responsible for the issuance of driver's licenses and state-certified identification cards must verify an individual applicant's identity prior to issuing the license or identification card. To do so, the MVA's must verify the applicant's name, date of birth, and Social Security Number (SSN) with SSA. Similarly, State- level Voter Registration Services require the same type of verification services.

To meet these service demands, under a series of written agreements, SSA and the American Association of Motor Vehicle Administrators (AAMVA) have established cloud-based system that allows state-level motor vehicle and voter registration offices to verify the identity of individuals applying for a driver's license, identification card or who are seeking to register to vote. As with eVerify, AAMVA provides the front-end web-service through which State MVA's and Voter Registration offices are able to access SSA's SSN verification services. SSA provides and maintains the back-end infrastructure and verification services.

A Service Level Agreement (SLA) between SSA and AAMVA governs this SSN verification service. The architecture of the AAMVA platform provides a broad range of features and functionality.

To enhance the availability, performance and reliability of the services provided, SSA is establishing a second AAMVA node in its Second Support Center (SSC. The creation of this second node in a geographical dispersed location provides for automatic load balancing and failover/recovery capability – ensuring the availability and reliability of the system in providing the critical services required by AAMVA and its clients/customers. Additional enhancements to the infrastructure and platform provide greater performance and reduced response times.

The implementation of this project is nearing completion. The second node will be fully operational by January 31, 2012.

<u>Major Milestones</u>

- Finalize Network Connectivity Requirements: 06/30/2011
- Finalize Storage Capacity Requirements: 07/15/2011
- Storage installed and configured: 09/30/2011
- Configuration of Integration region completed: 09/30/2011
- Integration region configuration validated and verified: 10/15/2011
- Configuration of Production region completed: 10/31/2011
- Acquisitions/procurements completed: 10/31/2011
- Production region configuration validated and verified: 12/15/2011
- Verification service applications tested operational: 01/31/2012

Lifecycle Costs

There were no new ITS costs associated with this project. SSA utilized existing infrastructure, platform and data service capabilities to provision the second AAMVA node in the SSC.

Under the terms of the SLA, AAMVA reimburses SSA for the costs of delivering this service to AAMVA and its client agencies.

Execution Risks

- Network connectivity is not completed (timely).
- Storage to support the new node is not acquired or installed (timely).
- SSA data processing fails to account for transactions flowing through the SSC.
- NUMIDENT data replication infrastructure incomplete.

Legacy Retirement Plan

Not applicable. There is no legacy system to retire in this instance.

Risks Associated with Moving Computer Services to a Cloud

The National Institute of Standards and Technology (NIST), the Inspector General (IG) community, the Government Accountability Office (GAO), and cloud subject matter experts have identified the following risks associated with moving computer services to a cloud. This list is not all-inclusive; therefore the Social Security Administration (SSA) should consider all potential risks to its data or legacy systems before moving future computer services to a cloud.

NIST

NIST Special Publication 800-146[1] discusses various risks related to moving services to a cloud. These risks include the following.

Computer Performance – Different types of computer applications require different levels of system performance. For example, email is generally tolerant of short service interruptions, but industrial automation and real-time processing generally require both high performance and a high degree of predictability. Cloud computing has similar performance issues that include time delays, off-line data synchronization, and data storage management.

Cloud Reliability - Reliability refers to the probability that a system will function without failure for a specified period of time within a specified environment. For the cloud, reliability is broadly a function of the reliability of four components: (1) the hardware and software facilities providers offer; (2) the provider's personnel; (3) connectivity to the subscribed services; and (4) the subscriber's personnel. Cloud reliability depends on several factors, including network dependency, cloud provider service or utility outages, and safety-critical workload processing.

Economic Goals - Cloud computing offers an opportunity to use computing resources with small or modest up-front costs. The related risks are business continuity, service-level agreement evaluations, portability of workloads, interoperability between cloud providers, and disaster recovery.

Compliance - The subscriber retains the responsibility for compliance when data or processing is moved to a cloud but the provider (having direct access to the data) may be in the best position to enforce compliance rules. Therefore, compliance should be

[1] NIST Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*, §§ 8.1 – 8.5, pp. 8-1 through 8-9, May 2012.

addressed contractually and include terms related to lack of visibility into how clouds operate, physical data location, jurisdiction and regulation pertaining to clouds (that is, *Health Information Protection and Accountability Act, Federal Information Security Management Act of 2002*, etc.), and support for forensics in a cloud.

Information Security - Pertains to protecting the confidentiality and integrity of data and ensuring data availability. Information security risks includes those risks associated with unintended data disclosure, data privacy, system integrity, multi-tenancy[2] clouds, browser use, hardware support, and management of cryptographic keys.

IG Community

The Council of Inspectors General on Integrity and Efficiency (CIGIE) identified similar risks as NIST. These risks included data security and regulatory compliance in moving services to a cloud. Furthermore, the IG community identified the following areas of concerns when moving services to the cloud.

- Access to information
- Asset availability
- Software maintenance
- Intellectual property language

CIGIE stated Federal agencies should have access to real time and archived data facilitating the agency's ability to audit and investigate without incurring additional cost. Additionally CIGIE expressed concerns about vendor compatibility with agency cloud services. CIGIE also noted issues with estimating outage time for hardware and software updates, fulfilling certification and accreditation requirements, and addressing patch management and version control. Moreover, CIGIE stated agencies need to include cloud agreement language that protects the Government while setting vendor boundaries.[3]

GAO

GAO cited concerns about potential information security risks associated with cloud computing. These concerns were identified through information collected and analyzed from industry groups, private sector organizations, and NIST as well as a survey of 24 Federal agencies. Specifically, GAO reported the risks to moving computer services to a cloud included

[2] In cloud computing, multi-tenancy is the phrase used to describe multiple customers using the same public cloud.

[3] IT Investigations Subcommittee of the Council of Inspectors General on Integrity and Efficiency Cloud Computing Working Group, pp. 1-6, 2011, *Cloud Computing Contracting Concerns*.

- the possibility that vendor security controls may be ineffective or noncompliant,
- potential loss of governance and physical control of agency data,
- cloud provider insecure or ineffective deletion of agency data, and
- inadequate background and security investigations for service provider employees.

Additionally, GAO noted concerns about the increased risk associated with multi-tenancy resources and risk of data interception resulting from the increase in data transmission volume.[4]

Cloud Subject Matter Experts

Cloud Subject Matter Experts identified risks associated with moving computer services to a cloud. These risks include

- resolution of cyber security risk;[5]
- failure to move entire legacy system application, functions, and features;[6]
- failure of cloud solution to meet its financial objectives;
- difficulty to develop and integrate cloud services due to the complexity of the service;
- failure to recover cloud services after a disaster; and[7]
- loss of customization.[8]

[4] GAO, Information Security, Testimony before the Committee on Oversight and Government Reform and Its Subcommittee on Government Management, Organization and Procurement, House of Representatives, pp. 3 and 4, July 1, 2010.

[5] TechAmerica, TechAmerias's Twenty-First Annual Survey of Federal Chief Information Officers, Section Cybersecurity, p. 2, May 2011.

[6] Id. at p. 25.

[7] ZDNet, *Eight cloud computing risks, and how to quash them*, September 28, 2011. http://www.zdnet.com/blog/service-oriented/eight-cloud-computing-risks-and-how-to-quash-them/7752.

[8] Barrie Sosinsky, Wiley Publishing, *Cloud Computing Bible*, p. 18, 2011.

Appendix E

Agency Comments

Social Security

MEMORANDUM

Date:	September 11, 2012	Refer To: S1J-3
To:	Patrick P. O'Carroll, Jr. Inspector General	
From:	Dean S. Landis /s/ Deputy Chief of Staff	
Subject:	Office of the Inspector General Draft Report, "Cloud Computing at the Social Security Administration" (A-14-12-11226)—INFORMATION	

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Amy Thompson at (410) 966-0569.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "CLOUD COMPUTING AT THE SOCIAL SECURITY ADMINISTRATION" (A-14-12-11226)

General Comment

At the top of page 5, the report states, "...OMB never formally approved SSA's plan." We believe this statement should be qualified, as it has been a matter of standard practice that the Office of Management and Budget (OMB) does not provide such formal, written approvals. By omitting this information, it infers that OMB chose to withhold its approval and that our cloud computing efforts are somehow deficient. While we do not dispute the strictly factual accuracy of the statement, we do object to its negative implication when made outside a context that ignores OMB's standard practice.

Response to Recommendations

Recommendation 1

Develop a service-based methodology to identify and track costs including the costs of retiring segments or entire legacy systems for all IT initiatives so the Agency can determine whether moving computer services to a cloud provided an equal or greater ROI than keeping the status quo.

Response

We disagree. As we presented several times during the course of this review, we previously identified the need for service-based cost allocation models and methodologies. We are currently investigating the feasibility and cost effectiveness of implementing a service-based cost allocation methodology to complement our existing Information Technology (IT) cost tracking mechanisms. We are obtaining the input and support of subject matter experts through one of our existing contract vehicles. In addition, we intend to identify the most productive, technically feasible and cost-effective strategies for the development and deployment of the processes and tools that may be required to identify and track the costs of IT business services delivered to our community.

Recommendation 2

Consider additional potential risks to its data or legacy systems before moving future computer services to a cloud.

Response

We disagree. We have an existing private cloud IT environment protected by a comprehensive defense-in-depth security architecture. These mechanisms will continue as critical elements of our cloud computing strategy as noted in our Cloud First Plan. We have taken comprehensive measures to ensure appropriate and effective risk assessment and mitigation for all IT projects. The security and privacy controls we deployed to protect our information assets, incorporate and exceed the additional risk categories identified in the report.

In addition to our comprehensive and robust risk assessment and mitigation, we also recognize the immaturity of public cloud computing offerings. This immaturity represents a substantial and concrete risk to the security, confidentiality, privacy, and integrity of the highly sensitive personal and acquisition-related data and information housed within our systems. Therefore, we continue to maintain a highly vigilant posture with respect to the effective protection of these systems and assets since the deployment of any cloud-based solution may affect them.

Finally, we continue to maintain the policy that interdicts the deployment of any cloud solution that could potentially jeopardize the security, privacy, confidentiality, or integrity of personally identifiable information by allowing it to reside beyond the protection of our own security authorization boundaries. Our current security controls and standards continue to apply whether we deliver IT services through our internal, private cloud; through an external, public cloud; or through some hybrid of both.

Our cloud computing strategy continues to address relevant statutory and policy requirements associated with Federal IT systems, including IT security and risk management; privacy; data integrity; legal issues; records management; OMB and the National Institute of Standards and Technology guidelines and recommendations; and other applicable requirements.

Recommendation 3

Continue reaching out to FedRAMP program officials; other Federal, State, and local government agencies; as well as private industry to obtain best practices and lessons learned before moving its computer services to a cloud.

Response

We disagree. As we presented during this review, we actively maintain an ongoing relationship with the General Services Administration, OMB, and the Federal Risk and Authorization Management Program (FedRAMP) officials to ensure that our cloud computing initiatives and activities remain consistent with Federal policies, guidelines, and security provisions.

We actively engage in efforts to identify and refine private industry cloud computing best practices. We also evaluate lessons learned from early adopters at any level of government or the private sector. Industry best practices and lessons learned play a prominent role in the evolution of our cloud computing strategies and implementation plans.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Mary Ellen Moyer, Audit Manager

Acknowledgments

In addition to those named above:

Cheryl Dailey, Auditor-in-Charge

For additional copies of this report, please visit our Website at http://oig.ssa.gov/ or contact the Office of the Inspector General’s Public Affairs Staff at (410) 965-4518. Refer to Common Identification Number A-14-12-11226.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations,
House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.