



Cloud First Plan

(Revised and Updated)

December 2, 2011

TABLE OF CONTENTS

- 1. Executive Summary..... 3
- 2. Background..... 6
- 3. SSA’s Cloud Computing Strategy 9
- 4. Designated Cloud-First Projects 13
 - 4.1. CARE Through 2020 13
 - 4.2. eVerify High Availability Platform 15
 - 4.3. AAMVA/HAVV Verification Services 17

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 initial deployment of CARE Through 2020 will provide a one-for-one/like-for-like replacement of current features and capabilities of the existing N8NN system. It also provides a platform that will enable the future deployment of additional features as they are approved and funding is available. 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.

Major Milestones

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/USCIS 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/USCIS 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/USCIS. 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, 2012.

Major Milestones

- 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.

Major Milestones

- 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.