OFFICE OF THE CHIEF INFORMATION OFFICER

CLOUD SERVICES GUIDANCE

Version: 4.1

Date: 2/25/2025

# Purpose

# Identify the deployment models for cloud computing at SSA and document process and guidelines for acquiring cloud services. This guidance supports efforts to ensure security and privacy while striving to streamline processes.

# Background

# SSA is actively using cloud services and will continue to acquire and use cloud services to extend our infrastructure and improve delivery of customer services to the public, employees, and businesses. Providing flexible building blocks that can be set up quickly, cloud services enable the continual improvement and efficient delivery of services.

# This Chief Information Officer (CIO) Guidance declares that SSA will maintain a multi-cloud deployment consisting of:

# an on-premises cloud supporting infrastructure-as-a-service and platform-as-a-service; and

# multiple external cloud services supporting infrastructure-as-a-service, platform-as-a-service, and software-as-a-service.

SSA uses a fit-for-purpose approach, considering cloud first to determine the appropriate platform for a project. Projects should explore all cloud deployment (software-, platform-, and infrastructure-as-a-service) and cloud hosting models (public, private, internal, and external). Considerations such as cost, proximity to data and other services used, and customer base will determine the appropriate deployment and hosting platform.

Security is a primary concern as SSA uses cloud services. Regardless of the service model, where the cloud is hosted, or the services used, security and privacy risk assessments of the environment are required.

Definitions of cloud services and models are available from NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.

# Applicability

This guidance applies to the acquisition (or development) and deployment of all IT solutions across all components of SSA. This includes purchases via Office of Acquisition and Grants (OAG), purchase card acquisitions, and cloud procurements that are done by a contractor on the agency’s behalf regardless of funding source.

# Authority

This Guidance is established under the authority of the SSA CIO. The CIO retains sole authority to alter, amend or rescind this Guidance. The application of this guidance is mandatory and applies to all components of the SSA enterprise.

This Guidance is consistent with:

Clinger-Cohen Act

Federal Information Security Modernization Act of 2014 (FISMA 2014)

Federal Information Technology Acquisition Reform Act (FITARA)

Privacy Act (1974)

Office of Management and Budget M-14-04

Electronic Government Act of 2002

# Requirements

All sponsors of cloud solutions, regardless of deployment and hosting model, must:

1. Follow the Enterprise Architecture assessment process.

# As part of the Enterprise Architecture assessment process, SSA architects will evaluate the project and determine documentation or approvals necessary to proceed.

# For external cloud services FedRAMP certification is required prior to production implementation. If no FedRAMP-certified solution can be identified, the CIO must be consulted. The CIO will engage the Office of Information Systems and other components as necessary to weigh time, cost, and staffing considerations to determine and provide the requesting component a plan of action.

Enterprise Architecture approval of an acquisition or use of cloud services is not equivalent to an Authority to Operate (ATO). Prior to proceeding to implementation with production data, projects must complete all necessary and appropriate security risk assessments as outlined in relevant Agency Information Security guidance and other government mandates.

If a project was not originally considering cloud computing options, but discovers or considers cloud later in the process, sponsors must promptly notify Enterprise Architecture Staff.

1. Provide documentation from the Enterprise Architecture assessment process to the OAG prior to any potential cloud service acquisition.
2. Complete an Office of Information Security (OIS) security risk assessment and an Office of Privacy and Disclosure (OPD) privacy assessment to ensure security, privacy, and confidentiality.
3. Comply with all current laws, regulations, IT security, and risk management guidance
4. Obtain an Authority to Operate (ATO) prior to implementation in production.
5. Adhere to cloud cost savings activities such as but not limited to the following:
   1. Cost Monitoring and Budgeting:
      1. Monitor monthly Showback usage and cost analysis reports and dashboards. Cloud Usage and Showback Reports
      2. Provide yearly estimates via SSA’s control process and maintain active cost center approvers. Annual Estimate Summary
   2. Continually review optimization dashboards and implement rightsizing recommendations for low-utilized instances. Cloud Optimization Dashboards
   3. Manage and follow the established instance shutdown windows for ‘Cloud Test Accounts’.
      1. All Cloud Tests Account instances must be shutdown 7 days a week from the hours of 12:30am to 4:30am. In addition, project teams should evaluate if the established timeframe can be expanded to increase their cost savings capabilities. If project teams determine they can expand the shutdown window beyond the 12:30am to 4:30am timeframe they should do so.
      2. If cloud customers need to opt out of the approved shutdown window, they should submit an exception form to obtain approval. Exceptions can be submitted here. EC2 Shutdown Exception

Optional: Cloud Customers can use the ‘Instance Parking with Turbonomic’ feature to assist with their shutdown and start up activities.

# Guidelines

There are numerous considerations when obtaining and using cloud services. For acquisition and use of cloud services refer to the “Guidance and Supplemental Information for Agency Cloud Guidance”.

# Responsibilities

Responsibilities associated with the guidance.

| **Roles** | **Responsibilities** |
| --- | --- |
| **Enterprise Architecture Staff** | * Identify or verify if project has cloud computing characteristics. * Document business case, OCIO reviews and decisions, and solicit input from SSA architects, including Cloud Architects. |
| **Chief Information Officer (CIO)** | * Review external cloud proposal for consistency with this Guidance. Request reviews as needed from CTO, Chief Architect, CISO/OIS, or Cloud Architects. * Notify OIS and OAG of new cloud initiatives. * Approve or deny request to pursue external cloud initiative. |
| **Chief Architect** | * Review and recommend action for cloud proposals for the OCIO. * Ensure cloud proposals comply with existing cloud guidance. |
| **Cloud Architects** | * Review and advise OCIO on cloud proposals for Cloud Service Guidance compliance, recommend approval/denial of cloud proposals, track cloud proposals and implementations. * Other cloud related duties as requested by OCIO. |
| **Architecture Review Board (ARB)** | * Identify or verify if a project has cloud computing characteristics and refer to the EA Staff and Chief Architect. * Ensure the project has approval of the OCIO, if proposed use is in an external cloud. |
| **Infrastructure Review Board (IRB)** | * Identify or verify if a project has cloud computing characteristics and refer to the EA Staff and Chief Architect. * Ensure the project has approval of the OCIO, if proposed use is in an external cloud. |
| **OAG** | * Request submission of OCIO approval as part of any new acquisition request that may be cloud related. * Notify the OCIO regarding such requests; request assistance to clarify possible external cloud projects, as needed. |
| **OIS/CISO**  Office of Information Security, Chief Information Security Officer | * Provides guidance and oversight to ensure that components seeking to procure cloud computing services comply with SSA security requirements. |
| **OIS/DCA**  Office of Information Security, Division of Compliance and Assessments (OIS/DCA) | * Conduct security risk assessments * Provide guidance on matters concerning compliance with FISMA, FedRAMP, and SSA security guidance requirements * Act as liaison to other OIS Divisions as needed |
| **OPD** | * Conduct Privacy Impact Assessment (PIA) * Provide guidance on matters concerning Privacy Act data in cloud computing environments |

# Approvals

| **Approved** |
| --- |

# Change History

| Version | Date | Reason for Change |
| --- | --- | --- |
|  |  | Developed using Version 3.0 of the Office of Systems Document Template dated 01/02/09. |
| V1.1 | 4/16/2013 | Approved OCIO Cloud Computing Document w/final edits |
| V1.2draft | 3/01/2015 | DRAFT OCIO Cloud Service Document |
| V1.2c revised | 4/27/2015 | Revised OCIO Cloud Service Document |
| V2.0 | 4/28/2015 | Revised OCIO Cloud Service Document – for Release |
| V3.0draft | 9/21/2017 | DRAFT OCIO Cloud Service Document |
| V3.1draft | 12/11/2017 | Incorporated comments from OIS |
| V3.2draft | 4/3/2018 | Incorporated comments from OAG, OPD, and others |
| V3.3draft | 5/14/2018 | Reference to government mandates/acts and question |
| V3.4draft | 5/21/2018 | Updated with additional comments from OIS |
| V3.41draft | 6/1/2018 | Corrected signature line and footer |
| V4.0 | 11/15/23 | Added cloud cost savings requirements |
| V4.1 | 02/21/25 | Fixed “Application Review Board” to “Architecture Review Board” on Page 4 |

# Appendix - Additional Guidance

SSA Policy 8045.01 – Cloud Services Vision and Strategy

This document outlines the vision and strategy for ***cloud services*** procured and administered by the Social Security Administration (SSA). This policy provides high level direction to guide implementation plans, as well as guidance on operational considerations.

[SSAPOL 8045.01 Cloud Services Vision and Strategy\_v1.0.pdf](https://www.ssa.gov/digitalstrategy/policyarchive/SSAPOL%208045.01%20Cloud%20Services%20Vision%20and%20Strategy_v1.0.pdf)