General Services Administration (GSA)

Federal Acquisition Service (FAS)

Cloud Computing Services Program Management Office (CCS PMO)

Cloud Migration and Data Center Consolidation

Statement of Objectives Template for the Department of Defense

Phase 1-3: Inventory, Application Mapping / Transaction Profiling, and Migration Planning

March 2016

Introduction and Instructions[1]

This Statement of Objectives (SOO) describes the objectives and tasks for cloud migration planning and data center consolidation services for Department of Defense (DoD) agencies.

Offerors shall use this SOO with other applicable portions of the RFP as the basis for preparing their proposal. Offerors shall ensure that all aspects of the SOO are thoroughly addressed in their proposals with particular regard to Inventory (Users, Applications, Infrastructure, Security and Privacy, Service Management); Application Mapping / Transaction Profiling; and Migration Planning.

Points of Contact

DoD Agency / Office:

[Point of Contact Name and Title]
Phone: *[(XXX) XXX-XXXX]*
Email: *[xxxx@agency.gov]*

[1] This DoD-specific cloud migration services SOO template is derived from those appearing on https://gsa.gov/cloud.

Contents

Purpose

This Statement of Objectives (SOO) describes the goals that the DoD/DISA expects to achieve with regard to planning the migration of DoD applications or services to the cloud - including legacy and new applications - and planning for future development of new cloud applications. The primary goal of this acquisition is to prepare DoD/DISA for moving applications to the cloud which will result in improvements in efficiency, agility, and innovation.

Scope

This SOO addresses work associated with the following cloud migration planning activities:

1. Conducting an inventory (including Users, Applications, Infrastructure, Security and Privacy, and Service Management)]
2. Application Mapping / Transaction Profiling
3. Data management assessment / evaluation
4. Conducting a suitability analysis, identifying appropriate service models (e.g. SaaS, PaaS, IaaS) and deployment models (e.g. private, public, hybrid, community
5. Providing recommendations to the government for the industry/service model
6. Developing the business case to quantify cost and benefits
7. Migration planning, including developing the migration roadmap
8. Data center consolidation planning

The offeror will provide support and services in compliance and in alignment with Federal Risk and Authorization Management Program (FedRAMP) standardized security assessment, authorization, and continuous monitoring policies in migration planning services, as required by the scope of the project.

The offeror's solution should also align to the strategy of the Federal Data Center Consolidation Initiative (FDCCI), seeking to curb the unsustainable increase in the number of data centers by reducing the cost of data center hardware software and operations; shifting IT investments to more efficient computing platforms; promoting the use of Green IT and increasing the IT security posture of the government.

Since not all data is encapsulated in an application, migration planning of applications and data should be considered two separate efforts in this project, with the exception of E-mail.

Migration Execution, Decommissioning Services, Equipment Disposition, and Facility Disposition are not included in the scope of this SOO. *[List additional services here that will support DoD/DISA in these activities].*

Period and Place of Performance

The base Period of Performance will be *[xx (xx)]* months from date of award with *[xx (xx) xx (xx)]* year options. Services will be provided at *[specify location].*

The offeror will provide pricing information where migration planning services are conducted in the United States and/or where services could be conducted outside of the United States. The locations where any services will be conducted must be identified and ordering activity data must be located.

It should be noted that U.S. Based Prices are prices where the services and all data-at-rest (either primary storage or replicated storage) are conducted and located within the United States. Worldwide Prices are prices where the services and any data-at-rest (either primary storage or replicated storage) are conducted and/or located outside the United States). [2]

Background

The two main drivers of this effort are the increasing benefits and mandates for cloud migration and data center consolidation.

Cloud Migration: Produced by the Office of Management and Budget (OMB), the February 2011 Federal Cloud Strategy outlines the impetus and benefits of migrating to cloud services. Based on the December 2010 25 Point Plan to reform Federal Information Technology Management, also from OMB, each Federal agency CIO has been directed to leverage this strategy to begin planning the migration of their IT services to cloud solutions. The cloud deployment model type and service categories to be used are up to each agency. Some may wish to pursue public, private, or a blend of both architectures such as hybrid cloud. The proliferation of public cloud networks may have an acceleration of data center outsourcing compared to that of private clouds, which tend to provide more data center optimization and a better utilization of existing infrastructure. Agencies should select the cloud deployment model based on the benefits they seek to achieve, as each model offers different benefits. Clearly, not all applications and data may be practical for migration. Agencies should ensure they complete an inventory of applications and data, and compare the operation of the “as-is” and the “to-be” state to determine whether migration is prudent.

Data Center Consolidation: The Federal Data Center Consolidation Initiative (FDCCI) was initiated by the Federal Chief Information Officer to reduce the IT footprint for agencies through the consolidation of traditional data centers to promote the use of Green IT, reduce the cost of data center hardware, increase the overall IT security posture of the government, and shift IT investments to more efficient computing platforms and technologies.

These two drivers, as well as OMB mandates such as Cloud First, Three to the Cloud, Shared First, and Future First, highlight the importance of harnessing these fundamental shifts in IT investment patterns to increase IT efficiencies and cut IT costs. Prior to migrating to the cloud or consolidating data centers,

[2] Worldwide pricing is only applicable if the work location is not based at the customer’s site

it is critical to have an understanding of the current IT environment and make informed decisions about moving applications to the cloud. The first step of The Federal Data Center Consolidation Initiative as described in the Federal Government's 25-point plan, calls for a complete inventory of data center assets and the development of a plan for consolidation. Agencies may be prudent to evaluate the current architecture and the design for the next-generation architecture, including cloud.

DoD/DISA is in the process of *[readying workloads and applications to migrate to the cloud].* The DoD/DISA target operating model is to *[migrate x services or x percentage]* to the cloud and/or 1. Promote the use of "Green IT" by reducing the overall energy and real estate footprint of government data centers; 2. Reduce the cost of data center hardware, software, and operations; 3. Increase the overall IT security posture of the government; and 4. Shift IT investments to more efficient computing platforms and technologies. Therefore DoD/DISA seeks services to encompass the cloud migration phases for all DoD/DISA applications, related users, processes, security, and service management.

The proposed services will support desired outcomes, including:

- Comprehensive analysis and understanding of the current environment, and analysis of which on-premise technical resources are best suited for the cloud.
- Comprehensive planning for migration to the cloud that supports cost-effective, secure, and agile IT management.

The proposed services will consist of determining the current inventory, assessing the current environment to determine which workloads and applications are appropriate for migration, determining the service and deployment models, developing the business case, and developing the Cloud Migration Strategy and Plan. These services will list all capabilities necessary to effectively support cloud migration. All services delivered will be required to meet offeror-offered Service Level Agreements (SLAs) as well as the performance criteria described later in section 6.

Current Environment

[Provide a brief, high-level description of DoD/DISA's current environment. Examples of current environment factors are listed below]:

- *[Strategic operations or mission objectives]*
- *[Description of IT organization, infrastructure, etc.]*
- *[Prevalence of on-premise or off-site hosting]*
- *[Current cloud initiatives and strategy]*
- *[Budget constraints]*
- *[Related programs that could impact cloud migration (e.g. refresh schedules, large acquisitions).]*

The Department of Defense (DoD) is the single largest energy consumer in the nation. As the largest owner of federal data centers, with 772, the DOD has more than twice as many centers as any other agency as of April, 2013. In FY 2007, DoD accounted for 63% of the energy consumed by federal buildings/facilities at an annual cost of $3.4 billion. By consolidating some of its data centers, DoD could

have a significant positive impact on energy savings for the federal government. DoD has instituted a number of policy directives, as have all federal agencies that influence energy use in its data centers.

Within the context of the FDCCI, DoD's efforts are intended to address concerns about rising energy demands and costs of data centers, associated increases in carbon emissions, expanding real-estate footprints of data centers, and rising real-estate costs. According to DoD, the Department plans to reduce the number of its data centers by about 30% by 2013, and the number of servers by 25%. DOD intends to use savings generated from consolidation to pay the consolidation costs. DoD also plans to use cloud migration as part of its savings effort and to ensure compliance with White House's Cloud First policy.

The offeror should contribute to the savings effort by providing:

- More efficient use of servers, storage, and staff, including reductions in energy consumed by idle servers
- Reductions in redundancy of hardware, software, and operations requirements, including HVAC
- Increased flexibility in use of servers
- Freed up floor space for other purposes
- Increased reliability of service
- Improved security

Objectives

The overall objective is to assess the migration of workloads and applications to the cloud, supported by comprehensive cloud migration planning services. To achieve this, these cloud migration planning services must meet applicable business, technical, security, management, and administrative objectives. Cloud migration services should be aligned with objectives of the enterprise service delivery model, and support the DoD's/DISA's ability to deliver future sustainable services. If an objective corresponds to a particular program phase, it appears in a subsection labeled: Inventory (Phase 1), Application Mapping / Transaction Profiling (Phase 2), or Migration Planning (Phase 3). Migration Execution (Phase 4), Decommissioning Services, Equipment Disposition, and Facility Disposition (Phase 5), objectives will be described in separate SOOs.

Business Objectives

- The offeror will enable strategic decisions by DoD/DISA to effectively migrate applications to the cloud, maximizing cost reduction and efficiency of IT environment.
- The offeror will provide maximum alignment to FDCCI requirements and cloud migration mandates and requirements, amplifying DoD or DISA's ability to achieve management objectives.
- The offeror will provide cloud migration services that accommodate considerations from an enterprise perspective including impact on DoD/DISA's business units, contracts, management, and technical components (application, infrastructure, and security).

- The offeror will provide all support operations necessary to fully develop and deliver services for the appropriate phases *(Inventory, Application Mapping / Transaction Profiling, Migration Planning).*

Inventory (Phase 1):

- The offeror will utilize industry best practices to conduct an inventory of DoD/DISA IT assets to provide DoD/DISA with a comprehensive view of DoD/DISA applications, infrastructure and security.
- The offeror will produce thorough analysis resulting in a comprehensive report on DoD/DISA IT users and stakeholders that would be impacted by cloud migration. For example, stakeholder groups could include Executive Sponsor, Legal and Contracts Management, Business Units, Application, Infrastructure, Security, and End User stakeholders.
- The offeror will identify and develop an approach and methodology for identifying the business processes and governance processes that are associated with current inventory (both applications and infrastructure).

Application Mapping / Transaction Profiling and Assessment (Phase 2):

- The offeror will provide work products for application mapping and transaction profiling that result in DoD's/DISA's understanding of the benefits and implications of moving individual applications or groups of applications to the cloud. The offeror will also complete application profiling.
- The offeror will utilize existing frameworks and data fields as prescribed by the FDCCI or DoD/DISA data center consolidation efforts.
- The offeror will produce a "quick win" analysis of applications that are well-suited based on desired outcome for accelerated deployment to the cloud, and provide recommendations for executing this migration.

Migration Planning (Phase 3):

- The offeror will develop a roadmap for DoD/DISA to effectively plan for cloud migration that maximizes cost reduction and identifies constraints and inhibitors to cloud migration. Considerations for this roadmap include:
- An approach to developing a business case for migration to include comparison of current expenditures to proposed expenditures (ranging from facility, hardware, middleware and database, infrastructure, operational costs, personnel, etc.), demonstrating ROI of proposed solution.
- A migration plan describing recommendations for the appropriate service models (SaaS, PaaS, or IaaS), and choice of deployment model (private, public, hybrid, etc.) of all services to be migrated, as well as selection rationale. Applications that fall under different categories of service models should be narrowed down to one model based on

the components of the application - whether it involves multiple systems or different service components (i.e., app logic, middleware pieces, data, etc.).

- Recommendations for cloud migration based on applications' development lifecycle, business relevance, security impacts, organizational roles, financial aspects of cloud service delivery, and other migration considerations. The platform should be based on the responsibilities the agency wants to maintain or devolve to the CSP, which is inextricably linked to the deployment model is desired.
- The sourcing model that will be authorized to control where applications will be hosted based on security, performance, disaster recovery, and service level requirements.
- Recommendations for incorporating government-wide and DoD/DISA-specific security controls into the target design and migration plan.
- An approach to identify and manage communication, change management, and training needs for migration planning.
- A plan that will have the IT management environment encompassing the management of conventional hosting, private and public clouds.
- An approach to ensure that procedures and documentation are developed for migration execution.
- Cloud governance for post-implementation. This should include a pricing, billing, and budget structure that enables "pay as you go", if not the ability to prepay for services for consumption over the life of the service agreement.

Technical Objectives

- The offeror will provide all technical advisory services necessary to fully develop and deliver services for the appropriate phases (Inventory, Application Mapping / Transaction Profiling, Migration Planning).
- The offeror will provide cloud migration planning services that account for the systems lifecycle, ranging from development, testing, and production. Provide services that include considerations for maintaining cloud services post-deployment. This may include staff with development capabilities and the necessary skills to support a cloud environment and to facilitate integration.

Inventory (Phase 1):

- The offeror will produce a baseline of DoD/DISA's technical environment including inventory of both infrastructure and applications, to include development/testing environments]. This should include an assessment of current applications and dependencies including auto-discovery tools.

- The offeror will document considerations for inventorying the infrastructure such as hardware, application, middleware and databases, networks, as well as any other relevant factors or components of the infrastructure. They should include how any changes to

- the applications or their deployment will affect interfaces with enterprise services, (e.g. authentication and authorization.)
- The offeror will deliver a methodology for utilization of auto-discovery tools to complete the inventory tasks. In addition to auto-discovery tools, it is important to have tools that monitor the application in real time to build operational models to aid in assessing what will be required by the cloud service offering. For example, the model should show resources required, which data components are used or accessed in the application to ensure the right amount of cloud computing resources (e.g., CPU type and size, memory, storage, and network) are allocated to efficiently host it.

Application Mapping/ Transaction Profiling and Assessment (Phase 2):

- The offeror will provide technical services for **application mapping** (Real-time discovery and visualization of all the interactions an application has with its underlying app infrastructure) and **transaction profiling** (Distinguishing unique transactions - i.e., "Login" vs. "Checkout" - and tracking the unique flow and code execution of a single business transaction across the underlying distributed application infrastructure over a period of time). Latency along each hop must be captured and compared against a baseline and displayed to troubleshoot bottlenecks) including illuminating interdependencies such as application dependencies and affinities to servers, server configuration etc.
- The offeror will identify and document critical dependencies between applications and data.
- The offeror will describe an approach to developing application evaluation criteria, application transaction profiling, and application dependency mapping, to include:
  - The mapping of multi-purpose applications.
  - A methodology for analyzing applications/infrastructure across a range of lifecycle stages (e.g. development, testing, and production).
- The offeror will describe an approach for decomposition of applications and identification of common functions and services that can potentially be migrated to the cloud, and identification of potential shared services.

Cloud Migration (Phase 3):

- The offeror will deliver a technical architecture including both the cloud and the broader enterprise architecture, shown together, capturing the "to-be" cloud migration state

that is consistent with adopted federal enterprise architecture frameworks[3] and consistent with specific DoD/DISA architecture standards.

- The offeror will include considerations in the migration planning solution for the target design such as capacity, schedules, migration priority, cost, etc.
- The offeror will describe an approach in the SOW to providing technical advice to cloud migration that will enable DoD/DISA to implement metering to migrated cloud services including provisioning capabilities, accounting capabilities, billing capabilities, etc.]
- The offeror will describe approach to testing for migration planning.
- The offeror will produce a plan that will support co-existing non-cloud and cloud architectures during and after migration.

Security Objectives

- The offeror will provide a comprehensive analysis of current applications and infrastructure that incorporates considerations for security such as data sensitivity, legal or other regulatory issues, disaster recovery, currently deployed remote access or internal security considerations, etc.

- As previously stated, the offeror will provide support and services in compliance and in alignment with Federal Risk and Authorization Management Program (FedRAMP) standardized security assessment, authorization, and continuous monitoring policies in migration planning services, as required by the scope of the project.

- The offeror will provide technical services regarding security and privacy in the migration planning services that are consistent with the NIST Special Publication 800-144 – "Guidelines on Security and Privacy in Public Cloud Computing", or other applicable standards and guidelines.

- The offeror will describe a framework and approach to incorporating both federal and DoD/DISA security requirements into migration planning recommendations.

- The offeror will describe how the cloud solution complies with additional security and privacy standards, such as NIST Special Publication 800-171 "Protecting Controlled Unclassified Information in a Nonfederal Information Systems and Organizations" as well as the DoD Cloud Computing Security Requirements Guide (SRG), DoD Concept of Operations for Cloud Computer Network Defense (CONOPS for CND), and any other guidance (including best practices) available at http://iase.disa.mil/cloud_security/Pages/index.aspx with particular regard to:
  - Properly securing the connections between formerly collocated systems, including systems not migrated for business or other reasons.

[3] For example, Federal Enterprise Architecture Framework http://www.cio.gov/documents/fedarch1.pdf

- Implementing Trusted Internet Connections, secure Cloud Access Points, secure nodes, and similar mandates.

Management Objectives

- The Government will allow the contractor maximum flexibility to innovatively manage program cost, schedule, performance, risks, warranties, contracts and subcontracts, offerors, and data required to deliver effective inventory services.
- The offeror will ensure clear government visibility into program cost, schedule, technical performance, and risk, including periodic reporting.
- The offeror will provide meaningful reporting and analytics that provide DoD/DISA with up-to-date and comprehensive information regarding technical and management performance.

Administrative Objectives

- The offeror will utilize relevant tools and analysis techniques for analyzing, evaluating and presenting information gathered throughout the cloud migration planning phases. The offeror will describe an approach and examples of relevant tools and analysis techniques for all cloud migration and data center consolidation phases of the project.
- The offeror will provide DoD/DISA decision making support in the form of relevant artifacts and work products.
- The offeror will describe in the proposal methods of compliance with requirements for the business, management and security objectives, proposing service level agreements (SLAs), associated terms and conditions, and enforcement methodology. At a minimum the SLA shall cover the following points:
  - Metrics for the services and descriptions of the expressions, parameters, and rules not to be less than that proposed within the acquisition vehicle, including definitions.
  - Metric Time Objectives for tasks
  - Methodology for ensuring that the Service Level Agreement is met.
  - Communications Management plan and what the government should expect as far as the frequency and degree of communication with the integrator.

Constraints

[Provide any subsections as appropriate such as:]

Access Control

- The offeror will describe a methodology for providing access control to migrated applications and virtualized legacy servers in the cloud to appropriate users. The offeror will explain in the

proposal how it will meet access control requirements described in the DoD Security Requirements Guide and in the NIST cloud computing special publications.

Authentication

- The offeror will provide users of DoD Information Systems a cost-effective and secure authentication mechanism or identity management solution to access cloud-residing IT resources.

Personnel Security Clearances

- The offeror will employ only personnel holding current security clearances at the TS/SCI level, or a level appropriate to the classification of data residing in the applications and systems to be migrated, or whatever clearance is deemed required by the Defense Security Service if the aggregate classification of all of the data in the system(s) requires an elevated clearance level.

Non-disclosure Agreements

- The offeror's personnel working with DoD systems and data will be required to sign non-disclosure agreements (NDAs) for the protection of classified or controlled unclassified information.

Accessibility

- All unclassified DoD applications and systems must be accessible to users from wherever allowed by the Security Requirements Guide.
- All applications must be accessible to users within the metrics prescribed by the service level agreement (SLA). DoD requires an availability uptime percentage of x%. Anything less will result in a service credit from the offeror to be determined by the SLA.

Sensitive and Embargoed Data, etc.

- Per the above NDAs, the offeror will be held responsible and liable for the protection of sensitive and embargoed data. Any sensitive data leak, breach, or network intrusion by unauthorized parties must be reported in accordance with the DoD SRG.

Requirements Cross-Reference

If necessary, use the table below to map the SOO objectives to additional requirements that appear in the contract vehicle being leveraged, if applicable.

Table 1: SOO to *[Acquisition Vehicle]* Cross-reference

SOO Requirement Reference	Acquisition Vehicle Requirement Cross-reference