General Services Administration

Statement of Objectives

For
Enterprise E-Mail and Collaboration Services

RFP #OCIO-14558

Source Selection Information
(See FAR 3.104)

June 2010

TABLE OF CONTENTS

SOO STATEMENT OF OBJECTIVES

SOO.1 Purpose

The General Service Administration (GSA) Office of Chief Information Officer (OCIO) is pursuing the acquisition of e-mail and collaboration services as Software as a Service (SaaS) from a commercial provider of Cloud Computing services and software. The intent is to replace the current GSA enterprise on-premise e-mail and collaboration support to a primarily web-based, SaaS services and support contract that provides a highly innovative, creative, cost-effective, and evolving environment. The ideal solution would be an integrated tool set through which the government monitors performance metrics and that allows the government to manage through roles and business rules rather than physical control of assets and direct software licensing. The government believes that traditional outsourcing and system integration support is insufficiently adaptive and costly and should be replaced by commodity services with a SaaS Cloud Computing offering.

This Statement of Objectives (SOO) describes the goals that GSA expects to achieve with regard to the

1. modernization of its e-mail system;
2. provision of an effective collaborative working environment;
3. reduction of the government's in-house system maintenance burden by providing related business, technical, and management functions; and
4. application of appropriate security and privacy safeguards.

Ultimately, the new e-mail and collaboration system will meet industry performance standards, offer the necessary redundancy and contingency features to meet GSA's needs, and provide state-of-the-art technology enhancements to improve user experience and minimize service disruption. The ideal solution will involve no software development work and minimal integration effort past implementation. The cost of operation will also be significantly reduced.

SSO.2 Background

The 2010 federal budget released by the administration and published on May 11, 2009 calls for improving innovation, efficiency and effectiveness in federal information technology (IT). The White House recommends that agencies adopt innovations and implement projects that increase efficiencies by optimizing common services and solutions across the enterprise and utilizing market innovations such as Cloud Computing services. GSA has historically sought new ideas in technology that would increase customer focus and service to the public. The current possibilities and value in sorting, sharing, and networking collective information can be enhanced by commercially available services.

The existing e-mail and collaboration infrastructures at the GSA are not adequate for the future.

They consist of aging, site specific servers, with limited redundancy, and inconsistent archiving capability. In addition, the current e-mail infrastructure makes it difficult to manage and retrieve e-mails associated with legal matters. In-house upgrading, replacement, and deployment of new servers and infrastructure will be both expensive and disruptive to GSA operations. Therefore, in an effort to improve performance, enhance redundancy, facilitate legal compliance and federal guidance, and manage cost, the GSA OCIO conducted market research to evaluate the viability and cost of various options, and is now pursuing this acquisition. This approach is expected to realize savings in cost and resources while providing the services needed to make GSA more efficient and effective.

The current e-mail and collaboration software infrastructure supporting the GSA in multiple domain names is based on:

IBM Lotus Notes® (version 7.0.3) for e-mail support and uses,
IBM Lotus Domino® (version 7.0.4, 8.0.1) for database support,
IBM Lotus Domino® (version 8.02),
IBM Lotus Connections® (version 2.5),
IBM Lotus Sametime® (version 8.02),
IBM Lotus Sametime Gateway® (version 8.02)
IBM Lotus Quickr® (version 8.2) in the collaborative environment, and
IBM DB2 CommonStore for Lotus Domino (CSLD) ® (version 8.3) for the litigation hold archiving (under 1 TB currently, growing at 2GB/day).
Blackberry Enterprise Server (version 4.1.7), and
PGP Encryption (version 9.10) for desktop client encryption.

GSA currently has 363 Quickr sites with approximately 6200 users (individual and groups) in the catalog.

The current Voice over Internet Protocol (VoIP) software infrastructure currently utilizes
Cisco Unified Connection 7.1.3.

In addition, GSA has the option to utilize the following capabilities:

Cisco MeetingPlace 7.0
Cisco Unified Presence Server 7.0.6
Cicso IP Communicator 7.0.3
Cisco Unified Personal Communicator 7.0.2
Cisco Unified Communications Manager 7.1.3
Cisco Unified Mobile Communicator Blackberry Client

A list of standard software approved for use within GSA is provided as Attachment 4 GSA Approved Standard Software.

The hardware infrastructure of e-mail servers is aging (5+ years) and requires purchase and deployment of new servers. The current e-mail infrastructure is site specific. For example, each of the seventeen locations (in the contiguous United States, Alaska, Hawaii, Belgium, Germany, Italy, Japan, and Korea) has its own set of e-mail and Blackberry servers. Further, if a regional location has power issues or becomes unusable, access to e-mail is lost for users at that location.

E-mail archiving is currently implemented inconsistently, is difficult to use, and does not meet information retrieval (e-discovery) requirements. Additionally, the storage associated with e-mail archiving continues to grow and is costly to manage. Recent regulations for handling e-mail litigation hold and discovery demand that GSA implement a more effective and expedient process.

The current hardware and software infrastructure supports approximately 15,500 individual accounts and about 3,000 additional (shared or resource) accounts; the government anticipates a possible growth up to 30,000 accounts in total. Approximately 9,300 accounts are also accessed via Blackberry phones.

Electronic messaging has evolved over the years into an integrated messaging and collaborative environment. GSA's current environment lacks the level of integrated features that is commercially available. GSA requires a greater use of these integrated messaging and collaborative tools to support its mission and critical position within the federal government. Additionally, GSA is seeking a solution that will reduce the government's in-house system maintenance burden and provide GSA users with more timely implementations of new versions and features.

GSA will maintain customer (user) support to receive Tier 1 trouble calls or requests for assistance and interface with the appropriate technical support. No direct customer support is required from this solicitation. Only technical and system administration staff will interface directly with the Offeror.

SOO.3 Scope

The scope of the resulting contract will include all Cloud Computing and support services required to transition, deploy, operate, maintain, and safeguard an enterprise-wide e-mail and collaboration environment.

SOO.3.1 Period of Performance

The base period of performance is for one year from contract award with four, one-year options.

SOO.4 Objectives

SOO.4.1 Business Objectives

SOO.4.1.1 Replace the current e-mail and collaboration environment with Cloud e-mail and collaboration services that are integrated as seamlessly as possible via a single sign-on and that improve business performance by providing GSA users with expanded and new capabilities that reflect industry standards:

1. Provide enhanced and state-of the-art e-mail functionality in a multiple domain environment.
2. Provide expanded access to state-of-the-art collaborative tools and capabilities (such as instant messaging, soft phone integration, on-line meetings, shared workspace, social media, groupware, workgroup support systems, etc.) that will enhance GSA's ability to conduct business.

3. Provide improved archiving capability with unlimited storage for e-mail and the ability to mark and retain data to support litigation requirements (litigation hold).
4. Provide frequent technology updates and/or enhancements that give GSA users access to the most current, commercially available service offerings.
5. Provide robust and rapid search (full text) capability to enable forensics and e-discovery across archived and active files.

SOO.4.1.2 Conduct a seamless and expedited transition from the current e-mail and collaboration environment to the Cloud e-mail and collaboration services with minimal disruption to business operations while insuring data integrity:

6. Plan and conduct an expedited transition from the current environment to the new environment and develop an executable exit strategy that would allow transition to another solution should this become necessary in the future.
7. Establish an efficient and executable data migration plan that will migrate litigation hold data (now in CommonStore) and a strategy for existing e-mail and archived content so that, if migration beyond litigation hold data is deemed essential, a seamless transfer of data and archived e-mail is achieved.
8. Improve workforce efficiency and effectiveness and reduce costs through enterprise-wide standardization of business operating procedures and near 100% user adoption of expanded functions and new capabilities.

SOO.4.2 Technical Objectives

SOO.4.2.1 Procure a Cloud e-mail and collaboration service with a high degree of reliability and availability:

9. Procure a service that maintains a redundant e-mail and collaboration infrastructure that will ensure access for all GSA users in the event of failure at any one provider location.
10. Procure a service that includes effective contingency planning (including back-up and disaster recovery capabilities).
11. Provide 24x7 trouble shooting service for inquiries, outages, issue resolutions, etc.
12. Provide e-mail and collaboration services that are dependable and provide response rates that are consistent with industry standards.

SOO.4.2.2 Procure a Cloud e-mail and collaboration service with the Security and Privacy levels and controls that are required by regulations and consistent with best professional practices:

13. Provide security controls that are confirmed to meet the security standards for Moderate Impact systems as described in NIST SP 800-53 with an accepted Certification and Accreditation (C&A).
14. Adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

15. Provide a security management environment that meets the requirements of GSA's CIO IT Security Procedural Guide CIO-IT Security-09-48, Security Language for IT Acquisition Efforts, including:
    - Required Policies and Regulations for GSA Contracts
    - GSA Security Compliance Requirements
    - Certification and Accreditation (C&A) Activities
    - Reporting and Continuous Monitoring
    - Additional Stipulations (as applicable)

    Within 45 days after contract award, the contractor shall be required to provide a draft System Security Plan (SSP).
    Within 90 days of award the Contractor shall provide a draft completed assessment package as prescribed in GSA CIO-IT-06-30 (Managing Enterprise Risk Guide).
    The draft completed assessment package will be reviewed by the government within 10 work days.
    The completed assessment package will be reviewed by the government within 10 work days.
    All final deliverables related to the assessment shall be required from the Contractor within 10 additional work days from the government's response.

    The deliverables are required by CIO-IT Security-09-48 to support system certification. Specific requirements for evidence of security controls to be submitted with offeror proposals are detailed in Instructions to Offerors and in Attachment 9.

SOO.4.2.3 Procure a Cloud e-mail and collaboration service that is customizable and extendable:

16. Procure a customizable and extendable e-mail and collaboration capability based on open-standards APIs that enable integration with third party applications.
17. Procure a capability that is compatible with commercially available office automation suites.

SOO.4.3 Management Objectives

SOO.4.3.1 Procure a Cloud e-mail and collaboration services provider that provides outstanding management and customer support:

18. Reduce the government's burden related to the management of e-mail and collaboration capabilities.
19. Provide GSA Systems Administrators with 24x7 visibility into the managed Cloud services through a real-time, web-based "dashboard" capability that enables them to access the status of the services, i.e. to monitor, in real or near real time, the key performance indicators of the system against the established SLAs and promised operational parameters.
20. Procure Cloud services from a provider offering comprehensive, meaningful, timely and self-explanatory invoices for managed services.

21. Procure Cloud services from a provider offering meaningful and timely reporting and analytics that provide GSA with current and comprehensive information regarding technical and management performance (summarizing projected vs. actual measures), pricing and other related issues.

SOO.5 Constraints

This section lists laws, rules, regulations, standards, technology limitations and other constraints that the service and/or service provider must adhere to or work under.

SOO.5.1 Access Control

User access to the e-mail and collaboration system must be integrated with GSA's Active Directory, to support single sign-on capability for users, to ensure that every user mailbox in the e-mail system is tied to an Active Directory account, and to ensure that if a user is disabled or deleted in Active Directory, the e-mail system will prevent user access to that e-mail account.

SOO.5.2 Authentication

The e-mail system shall support authentication using the GSA's Entrust® PKI. It is envisioned that in the future all users will authenticate with the Entrust® PKI and use the Identity, Credentials, and Access Management (ICAM) access card; for the present some users will continue to be authenticated by user name and password, and this method must also be supported. Furthermore e-mail encryption and signing shall use the existing GSA Entrust® PKI.

SOO.5.3 HSPD-12 Personnel Security Clearances

Acquired services shall comply with the following regulations and requirements:

Homeland Security Presidential Directive-12 requires that all federal entities ensure that all contractors have current and approved security background investigations that are equivalent to investigations performed on federal employees.

The Contractor shall comply with GSA order 2100.1 – IT Security Policy, GSA Order ADM 9732.1C – Suitability and Personnel Security, and GSA Order CIO P 2181 – HSPD-12 Personal Identity Verification and Credentialing Handbook. GSA separates the risk levels for personnel working on federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk. Criteria for determining which risk level a particular contract employee falls into are shown in Figure A-1 of GSA ADM 9732.1C. The Contractor shall ensure that only appropriately cleared personnel are assigned to positions that meet these criteria.

Those contract personnel determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) or equivalent investigation.

Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.

Those Applicants determined to be in a High Risk position will require a Background Investigation

(BI).

The Contracting Officer, through the Contracting Officer's Technical Representative or Program Manager will ensure that a completed Contractor Information Worksheet (CIW) for each Applicant is forwarded to the Federal Protective Service (FPS) in accordance with the GSA/FPS Contractor Suitability and Adjudication Program Implementation Plan dated 20 February 2007. FPS will then contact each Applicant with instructions for completing required forms and releases for the particular type of personnel investigation requested.

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been no break in service, and the position is identified at the same or lower risk level.

After the required background investigations have been initiated, the Contractor may request authorization for employees whose investigations are pending to access systems supporting GSA e-mail and collaboration applications. The GSA Chief Information Officer may grant this authorization based on determination of risk to the government and operational need for the support of these applications.

SOO.5.3 Non-Disclosure Agreements

Standard non-disclosure statements shall be provided as required for system administration personnel who may have access to government data in the course of their duties.

SOO.5.4 Accessibility

Requirements for accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) are determined to be relevant. Information about the Section 508 Electronic and Information Technology (EIT) Accessibility Standards may be obtained via the Web at the following URL: www.Section508.gov . The Government Product/Service Accessibility Template (GPAT) is found in Attachment 7 of this solicitation. Generally accepted inspection and test methods corresponding to the identified Section 508 standards are reflected in the EIT Acceptance Guide found at Attachment 8.

SOO.5.5 Data

All data (e-mail traffic, contact information, calendar contents, etc) is and shall remain the property of the government. The Contractor shall ensure that the government retains access and download capability of all data for research, investigation, transfer, or migration to other systems.

SOO.5.6 Confidentiality, Security, and Privacy

In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, the Contractor shall be responsible for the following privacy and security safeguards:

(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards used by the Contractor under the resulting contract or otherwise provided by or for the government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public government data collected and stored by the Contractor, the Contractor shall afford the government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(d) The Offeror's solution must comply with the GSA CIO IT Security Procedural Guide CIO-IT Security-09-48, Security Language for IT Acquisition Efforts (see Attachment 2) as required for a Moderate Impact system.

(e) Work on this project may require or allow contractor personnel access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

(f) All data at rest will reside within the contiguous United States, the District of Columbia, and Alaska (CONUS) with a minimum of two data center facilities at two different and distant geographic locations