General Services Administration

Statement of Work

For
Hosted Resume Intake, Workflow, and Storage Service

RFP #

September 2012

TABLE OF CONTENTS

SOW STATEMENT OF WORK

SOW.1 Purpose

The General Service Administration (GSA) is pursuing the acquisition for a hosted resume intake, workflow, and storage service as Software as a Service (SaaS) from a commercial provider of Cloud Computing services and software. The intent is to provide GSA with a complete replica (excluding data) of the existing White House system with all of the same features and functionality.

This Statement of Work (SOW) describes the goals that GSA expects to achieve with regard to:

1. Provision a fully operational system stood up by October 7, 2012
2. Training provided via hosted and in-person hands on between October 8, 2012 and November 1, 2012
3. Optional go-live in production with .gov (GSA provided) domain on November 7, 2012
4. Optional transition of data into existing White House system post inauguration

Ultimately, this newly hosted site 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 limited software development work and minimal integration effort.

SOW.2 Background

The Pre-Election Presidential Transition Act of 2010 (Public Law 111 283, 11th Congress) requests the GSA to provide certain transition services prior to an election. To be fully prepared for a transition, a tool for receiving and processing resumes for Presidential Appointees must be in place prior to the election and ready for immediate use if a transition occurs. Since the current sitting administration has a fully operational tool in production, it makes sense to use a copy of the existing system to limit development and build-out of a new system, ultimately limiting resources and substantially reducing costs.

SOW.3 Scope

The scope of the resulting contract will include all Cloud Computing and support services required to implement and train a fully hosted environment. An optional scope for operation and maintenance (O&M) and transition into the current production system is also required if a presidential transition does occur.

SOW.3.1 Period of Performance

The base period of performance is from contract award through November 7, 2012. Options will be provided for O&M with possible minor modifications and a transition plan into the existing system

post inauguration.

SOW.4 Objectives

SOW.4.1 Business Objectives

SOW.4.1.1 To mirror the existing White House Resume Intake system with an external facing hosting site to collect resumes. The site will support intake of a minimum of 400 resumes per hour with the ability to throttle higher if necessary. Branding information will be provided in standard formats and will need to be incorporated into external facing site.

SOW.4.1.2 To mirror the existing White House back-end system to store resumes and provides detail workflow and reporting.

SOW.4.1.3 To provide in-depth training on all functionality of the system. Training shall be provided via webinar, on-site (hands on), and possibly other offered pre-approved methods.

SOW.4.2 Options (Only if a transition occurs)

SOW.4.2.1 Provide full operation and maintenance with minor modifications to a fully operational production system. Create a transition plan to migrate all data to the current White House platform post inauguration.

1. Operation and maintenance will encompass high system availability, backups, and customer support between the hours from 8:00 AM to 6:00 PM Eastern. Minimal workflow modifications maybe required.
2. Establish an efficient and executable data migration plan to migrate data from the current system into the legacy system. This will include following contract tasks set by the current administration, but at a minimum, the legacy system should be clean of all data before a migration can begin.

SOW.4.3 Technical Objectives

SOW.4.3.1 Procure resume intake, workflow, and storage service with a high degree of reliability and availability:

3. Procure a service that maintains a redundant infrastructure that will ensure a high degree of availability.
4. Procure a service that includes effective contingency planning (including back-up and disaster recovery capabilities).
5. Provide 24x7 trouble shooting service for outages and on call support for issue resolutions between the hours from 8:00 AM to 6:00 PM Eastern Monday through Friday.

SOW.4.3.2 Procure a solution with the Security and Privacy levels and controls that are required by regulations and consistent with best professional practices:

6. 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).

7. Adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

8. 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)

   The contractor shall be required to provide a draft System Security Plan (SSP).

   If a transition occurs, the Contractor shall provide a draft completed assessment package as prescribed in GSA CIO-IT-06-30 (Managing Enterprise Risk Guide).

SOW.4.4 Management Objectives

SOW.4.4.1 Procure a resume intake, workflow, and storage service provider that provides outstanding management and customer support:

9. Procure services from a provider offering comprehensive, meaningful, timely and self-explanatory invoices for managed services.

SOW.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.

SOW.5.1 Access Control

User access to the resume intake, workflow, and storage system must be secured to allow only specified IP addresses/ranges access. In addition, require stringent password authentication based on the Security Procedures Guide provided.

SOW.5.2 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.

SOW.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.

SOW.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.

SOW.5.5 Data

All data 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.

SOW.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).