General Services Administration
Federal Acquisition Service
Technology Transformation Services
1800 F St NW | Washington, DC | 20405

cloud.gov Professional Support Services

Performance Work Statement

1.0 Background

The General Services Administration (GSA) is dedicated to procuring goods and services on behalf of the US federal government. As an integral part of GSA, the Federal Acquisition Service (FAS) helps agencies procure innovative solutions and services in a wide range of areas including technology.

Within FAS, the Technology Transformation Services (TTS) organization applies modern methodologies and technologies to improve the public's experience with government by helping agencies make their services more accessible, efficient, and effective, and by itself providing services that exemplify these values. TTS builds, provides, and shares technology applications, platforms, processes, personnel, and software solutions to federal agencies in an effort to help them better serve the public.

cloud.gov is a shared service operated by TTS. cloud.gov is a Platform-as-a-Service (PaaS) built specifically for teams delivering federal government applications. Customers of cloud.gov are responsible for building their own applications, while the cloud.gov platform handles the security and maintenance of everything underneath. cloud.gov maintains a FedRAMP Joint Authorization Board (JAB) Moderate Provisional Authority to Operate (P-ATO), which enables federal agencies to host applications meeting federal security compliance requirements.

cloud.gov runs on top of industry-provided infrastructure. Amazon Web Services

GovCloud is the initial Infrastructure-as-a-Service (IaaS) provider. cloud.gov PaaS is built using open source technologies, with Cloud Foundry being the foundational component. Cloud Foundry is a multi-cloud technology that supports the full application development lifecycle. cloud.gov uses additional open source software as part of this Cloud Foundry deployment including Prometheus, Elasticsearch, and Kubernetes.

Statistics

- **Customers:** cloud.gov currently hosts 41 customer "organizations" (systems) across more than a dozen federal agencies. Customer systems hosted on cloud.gov include fdic.gov and fec.gov.
    - cloud.gov also hosts Federalist (https://federalist.18f.gov/), a companion shared service for hosting static websites. Federalist hosts more than 100 websites for many agencies, including high profile informational sites such as vote.gov, cio.gov, and opioids.gov.
- **Support:** cloud.gov handles an average of 30 customer email support requests a month.
- **Security posture:** cloud.gov deploys updates several times a month. cloud.gov routinely carries fewer than five open FedRAMP POAM (Plan of Actions and Milestones) items a month.
- **Infrastructure:** cloud.gov has 270+ virtual machines with individual components of the system.
- **Availability:** cloud.gov has an internal goal of at least 99.99% customer application availability and routinely exceeds it. We publicly report outages and any reduced availability here: https://cloudgov.statuspage.io/
- **Team:** The cloud.gov federal employee team ranges from 8-15 people. Our team is fully responsible for cloud.gov, including features, operations, support, compliance, and business development.

2.0 Objectives

TTS intends to procure professional services in order for the contractor to perform operations and maintenance for the cloud.gov technical system, specifically the Cloud Foundry-based platform and supporting services and web applications.

The primary objectives are:

- Operate, maintain, monitor, and update a Cloud Foundry deployment and the supporting services underlying cloud.gov.

- Provide consultation for the cloud.gov team to support adoption of Cloud Foundry best practices and solutions to provide new capabilities.
- Automate operation processes and increase the resilience of the system.
- Maintain Secure Configuration Management practices and assist the security team in developing threat assessment and incident response processes at the organizational and system level.

3.0 Project Scope

cloud.gov is seeking **to contract a team of dedicated, skilled and knowledgeable resources with a capacity to commit up to 6,000 annual labor hours (equivalent of three people full-time)** to assist with the operations, maintenance, and improvement of the cloud.gov platform.

The contractor is expected to follow the cloud.gov Configuration Management plan. In summary: The work to be performed will combine system administration and code development, using DevSecOps practices and Infrastructure as Code principles: Team members commit all changes to source control (git) and test and deploy them using continuous integration and deployment tools (Concourse) and orchestration tools (BOSH). Team members manage IaaS environments and configuration using infrastructure as code techniques (using Terraform).

We work in a collaborative, remote-first environment, including chat and video conferencing collaboration on changes before, during, and after development, with frequent use of pairing between government employees and contractors during the core hours, 12:00pm - 6:00pm EST.

3.1 Core Tasks

The following core tasks are required to support cloud.gov's operation and maintenance:

Task 1: Meet vulnerability management objectives

The cloud.gov system consists of many components from Cloud Foundry and the broader open source ecosystem. cloud.gov components must be kept up to date as new versions and fixes appear in order to maintain our security posture and FedRAMP Authorization. The contractor shall keep the system up to date on an ongoing basis. The contractor will also be expected to scan cloud.gov platform components monthly

using OWASP ZAP and Nessus (provided by cloud.gov). The contractor will be expected to assist with evaluating findings, identifying when findings are false positives or operational requirements, and resolving findings. Any findings must be addressed within a 30-, 60-, or 180-day period depending on severity. The contractor may offer assistance in reducing the labor required for this process, such as using automation, scripting, and increased monitoring.

Task 2: Assist with troubleshooting unexpected behavior
The contractor shall assist in troubleshooting problems in the platform's operations reported by the cloud.gov team or cloud.gov's customers during normal business hours. The contractor should be able to help assess whether unexpected system behavior is explainable as a routine operational incident or a potential indicator of compromise. In the latter case, the contractor will be expected to help gather evidence.

Examples: a customer is unable to bind services, a brokered service becomes unavailable, a security incidents are reported/alerted, etc.

Task 3: Increase automation and maintainability
The contractor shall take an active role to reduce the manual overhead necessary for operating the platform, rotating secrets, performing updates, etc.

Examples: scripts that automate common tasks, automated CI/CD pipelines in Concourse, increased use of CredHub, Terraform, etc.

Task 4: Improve resilience and recoverability
The contractor shall assist in improving the resilience of the cloud.gov platform and increase likelihood of complete, full recovery in case of a major contingency event. Examples: migration to Kubo, deployment of BOSH Backup and Restore and/or SHIELD, etc.

Task 5: Assist with documentation of significant changes
As a FedRAMP-authorized provider, cloud.gov must submit Significant Changes (major changes to security or risk or architecture) to assessment by a FedRAMP Third Party Assessment Organization (3PAO). The contractor will be expected to describe the technical changes to cloud.gov team members in enough detail that they can create documents for compliance review processes. The contractor will also be expected to

help produce artifacts as evidence that the system works as described during compliance reviews.

3.2 Additional Tasks

The following specific tasks may be required to support expansion of cloud.gov's capabilities as need arises.

Task 6: Assist and advise with new capabilities
The contractor shall assist and advise the cloud.gov team on building and deploying new capabilities based on projects in the wider Cloud Foundry ecosystem. Example: incorporating technologies based on stratos metrics, blacksmith, service fabrik, abacus, fissile, kibosh, eirini, etc.

Task 7: Expand services to other IaaS providers
cloud.gov currently uses AWS GovCloud as its IaaS provider. The contractor may be called upon to assist with expanding cloud.gov services to include additional and higher-security IaaS deployments through judicious application of alternative CPIs, isolation segments, or OSBAPI brokers.

Task 8: Expand support for Windows apps
The contractor may be required to assist with expanding cloud.gov services to include support for Windows cells and .NET Framework apps.

Task 9: Business operations support
The contractor may be called for support with business operations including account management, financial modeling, and running the government's billing cycle.

4.0 Technical Direction

As necessary, technical direction or clarification concerning the details of specific tasks set above will be given. The contractor may be asked to plan and perform other procedures that arise from the results of the tasks included within the scope of this PWS. This technical direction will be communicated to the contractor by the Contracting Officer's Representative (COR) and/or the Alternate COR.

The responsibilities and limitations of the COR are as follows:

(1) The COR is responsible for the technical aspects of the project and serves as technical liaison with the contractor. The COR is also responsible for the final inspection and acceptance of all reports, and such other responsibilities as may be specified in the contract.
(2) The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes, which affect the Contract price, terms or conditions. Any contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the expressed prior authorization of the Contracting Officer. The COR may designate alternate COR(s) to act for the COR by naming such alternate(s) in writing and transmitting a copy of such designation through the Contracting Officer to the contractor.

5.0 Program Assumptions and Constraints

The contractor will be responsible for all training for work to be performed under this requirement. The contractor shall maintain any necessary competencies, certifications, licensure, and apply industry standards in support of their efforts. The contractor must ensure that personnel working on this requirement stay current on all requirements and processes both in the federal government and in industry standards.

6.0 Deliverables

Please refer to the QASP for detailed information. Some of the deliverables include the following:

- The contractor will document all dependencies (all licenses and dependencies). The dependencies will be listed and all major functions documented. System diagram is provided as appropriate to the release. The contractor will also assist with the documentation of significant changes. They will contribute to documents for compliance review processes; they will also assist with producing evidence that the system works as described during compliance reviews.

- The contractor will provide a monthly report containing the level of effort expended in support of the various task elements during the previous month, the amount to date, and the annual amount remaining.

- The contractor will provide a monthly report projecting the distribution of hours remaining during the contract period by task element with a description of the objectives and milestones reached to date as well as those planned to be obtained within the contract period. The Government will review this report to ensure value is consistently added by the team and ensure resources and priority remains in alignment with Government strategic objectives.