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” provider). The platform includes access to this infrastructure while removing the complexity of managing it from the developer experience.

The 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

The General Services Administration (GSA) intends to purchase professional services in order for the vendor 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 Tasks

cloud.gov is seeking **to contract a team of dedicated, skilled and knowledgeable resources with a capacity to commit up to 5,760 annual labor hours (equivalent of three people full-time)** to assist with the operations, maintenance, and improvement of the cloud.gov platform. (cloud.gov may ask for an increase in hours over time.)

Team members are 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 employees and contractors during core hours.

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

3.1 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.

3.2 Task 2: Assist with troubleshooting unexpected behavior

cloud.gov has an internal goal of at least 99.99% customer application availability and routinely exceeds it. To identify potential problems, cloud.gov uses automated monitoring and customer reports. The contractor shall assist in troubleshooting problems in the platform's operations (including availability issues) reported by the cloud.gov team or cloud.gov 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 incident is reported/alerted, etc.

3.3 Task 3: Increase automation and maintainability

In collaboration with the cloud.gov team, the contractor will reduce the manual overhead and costs 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.

3.4 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. All scripts, including those from Task 3, must be stored in source control and regularly tested to ensure that a completely new working environment can be created using automation.

Examples: migration to Kubo, deployment of BOSH Backup and Restore and/or SHIELD, etc.

3.5 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 contribute to security impact analyses for potential technical changes, to help determine whether a change meets the FedRAMP definition of “significant”. When the contractor does substantial work on a significant change, they will help create documentation of that change 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.

3.6 Task 6: Contribute to government-tailored DevSecOps automation.

The contractor shall advise and assist with the creation of standardized, repeatable, and customizable DevSecOps processes, tools, and pipelines which reduce the burden of government compliance for the cloud.gov platform operators and cloud.gov customers.

3.7 Task 7 (Optional): Assist and advise with new capabilities

The contractor shall assist and advise the cloud.gov team on building and deploying features based on new capabilities and projects in the wider Cloud Foundry and Cloud Native Computing Foundation (CNCF) ecosystems.

Example: implementing features based on stratos-metrics, blacksmith, service fabrik, abacus, fissile, kibosh, eirini, prometheus, falco, etc.

3.8 Task 8 (Optional): 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 use additional and higher-security IaaS deployments using Cloud Foundry standard technologies, such as alternative Cloud Provider Interfaces (CPIs), isolation segments, or Open Service Broker API (OSBAPI) brokers.

Examples: AWS GovCloud East, Azure Government, Google Cloud Platform.

3.9 Task 9 (Optional): Expand support for Windows apps

cloud.gov currently hosts applications targeting the Linux kernel Application Binary Interface (ABI). The contractor may be asked to assist with expanding cloud.gov services to include support for Windows OS in order to support .NET Framework and applications targeting the Windows kernel ABI.

3.10 Task 10 (Optional): Facilitate onboarding activity

The contractor may be called on to assist in the onboarding of end users onto the cloud.gov platform in an effort to drive consumption of the platform. This may include the development of informational and educational materials as well as conducting training and workshops. This also may include the development of additional automation tools to aid in the self-service onboarding of new users, projects and agencies.

3.11 Task 11 (Optional): Support customer migration

The contractor may be called on to assist with the migration of customer applications, services, and data into the target cloud.gov environment.

3.12 Task 12 (Optional): Outreach and guidance

Facilitate outreach to the Federal IT community regarding cloud.gov services and provide high-level guidance for vendor projects targeting cloud.gov.

3.13 Task 13 (Optional): Business operations support

The contractor may be called for support with business operations including account management, financial modeling, and running the customer billing cycle. This is currently run manually by the cloud.gov team using spreadsheets. Contractor support could include help with the manual process and automation to reduce the manual effort and potential for error involved.

4.0 Program Assumptions and Constraints

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

5.0 Qualifications

Continuity, technical expertise, and institutional knowledge are important for the success of this requirement. The existing cloud.gov team applies the following skills in day-to-day development, operations, and continuous monitoring of the cloud.gov system.

To perform all requirements specified in this document the contractor should provide qualified personnel who also possess these skills (based in their professional and personal experience) so they will supplement our capacity to operate and improve the system.

For each person:

- 3+ years of experience designing and developing business applications or other software
- Experience working in a team environment applying XP methods (such as pairing and test-driven development) and agile practices (such as Scrum or Kanban)

- Strong experience with deployment and operation of Cloud Foundry, with hands-on experience applying related tools including Concourse, BOSH, and Terraform
- Experience using git (and preferably GitHub) to manage code and infrastructure configuration

Between the full-time personnel:

- Experience logging and monitoring distributed systems (using tools such as ELK or Prometheus)
- Ability to work with Golang, Python, and Java code
- Hands-on experience applying containerization tools (such as Docker) and container orchestration tools (such as Kubernetes)
- Experience providing common managed services using the Open Service Broker API (such as Elasticsearch, S3, or RDBMSes)
- Knowledge of best practices and recommendations for cloud governance and cost minimization
- Experience in operating distributed and cloud-native architectures
- Experience operating common AWS services (such as EC2, VPC, S3, ELB, Security Groups, IAM, CloudWatch, and CloudTrail) and preferably other public clouds such as Google Cloud Platform, Azure, OpenStack, etc.
- Operating system administration and security – Ubuntu Linux and preferably also Windows Server
- Experienced with DevOps processes/tools and have an understanding of secure coding, testing, and deployment practices (i.e. DevSecOps)
- Experience operating a service requiring at least 99.99% availability.

The Contractor shall provide people who are comfortable working with a geographically distributed team and who can leverage the existing tools used by the program, or new tools as become available and are approved for use by GSA. The Government will choose from the tools above (or Contractor-proposed equivalent or superior) based on its needs at the time of award.

6.0 Deliverables

The contractor will provide a monthly report at the end of each month detailing the task(s) completed as stated above. The monthly report should link to the QASP specifying what was accomplished.

The monthly report should detail all applicable task(s) elements with a description of the objectives and milestones reached to date as well as those planned to be attained 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.