Attachment D

STATEMENT OF WORK
CHS III
CHS II Transition

A-4.1 Day One Task Order: *CHS II Transition*

The response to this Task Order is expected to be issued at contract award. The Offeror shall provide efficient and innovative technical support for the USGS Cloud vision to routinely migrate current cloud applications from the current AWS environment to the offer platform choice. Integration of these applications support local, regional, nationwide, and global science use cases and in all cases provide support to natural resource managers and in some cases support health and safety for our nation. Many decisions makers rely on these USGS systems to monitor natural hazards and time critical decisions.

The response should consider:

- A task plan for this task order to included (at a minimum) approach, scope, schedule, staffing (using titles from the skill matrix) by month and the basis-of-estimate. It is requested that a schedule primarily focused on major milestones and key deliverables be provided in soft copy using Microsoft Project (exported to PDF).
- A representative sample Monthly Status Report as described in Task Order Objectives, which includes performance metrics.
- This task order is labor hours.

Summary

The USGS Cloud Hosting Solutions (CHS) program is responsible for formulating an overarching strategic vision for the Bureau's usage of Cloud-based services, subject to confirmation of the Office of the Associate Chief Information Officer (ACIO) and senior Bureau leadership. It is also the primary team responsible for implementing and supporting the Virtual Data Center (VDC) and its range of services aligned with the strategic plan. CHS enables and accelerates cloud adoption by providing a common framework for procuring, securing, and operating cloud workloads.

Current CHS Environment

CHS is responsible for providing a secure and available network between CHS AWS Custom Accounts and the Department of Interior (DOI) internal network. CHS is responsible for providing a secure connection from on-premises resources to the CHS environment. To facilitate the service, CHS provides Core Services including Core Amazon Route 53 and Virtual Private Clouds (VPCs) to allow the CHS customers to secure access on-premises and in cloud resources. Core services include:

- AWS Direct Connect
- Virtual Private Clouds, routed through Transit VPC
- Amazon Route 53
- Security
    - Amazon Guard Duty
    - AWS Athena
    - AWS CloudTrail
    - AWS Config
    - AWS Systems Manager Explorer

CHS is responsible for securely provisioning CHS AWS Custom Accounts based on the CHS baseline. CHS maintains and monitors the configuration of these projects. CHS ensures that accounts are provisioned and adhere to their defined baseline.

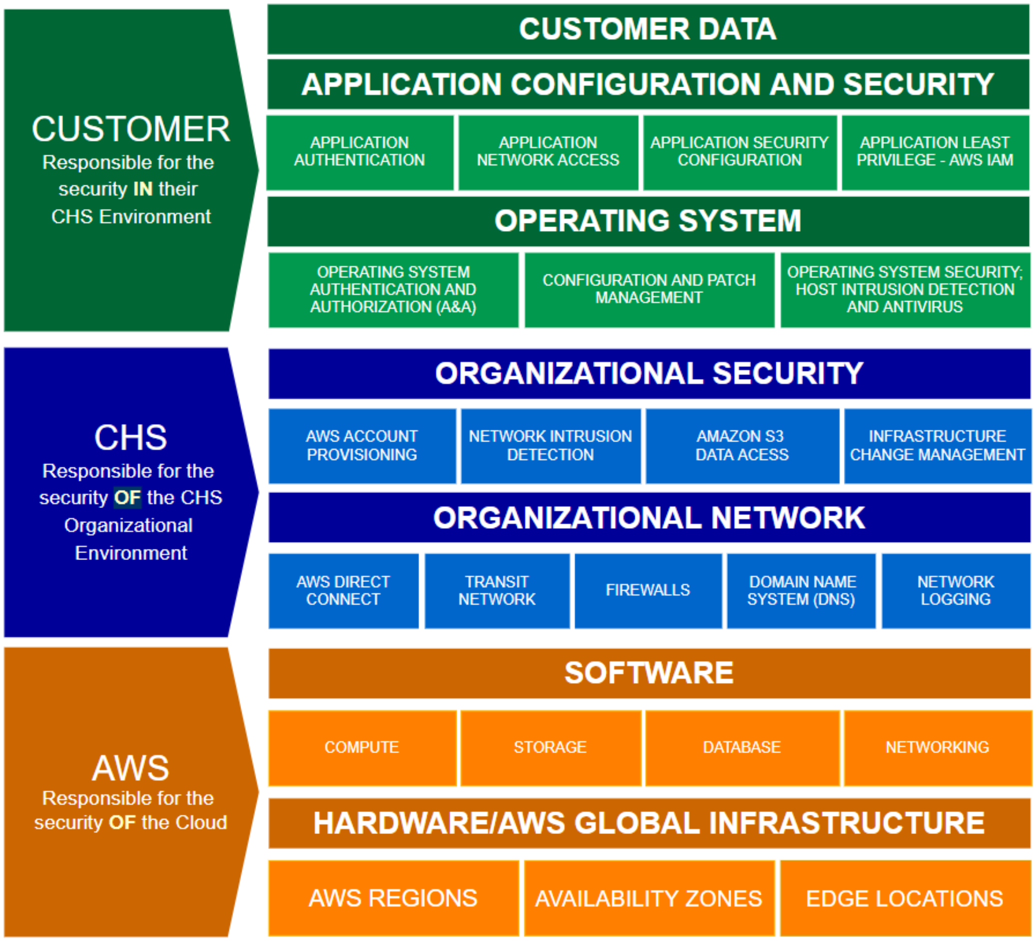
CHS is responsible for ensuring that AWS services are secure and available to CHS customers. CHS reviews every AWS service to ensure that they meet the security baseline before granting access to those services to customers. Once an AWS service is approved for use, the allowed and denied actions will be added to the csr-Developer-Permissions-Boundary AWS IAM Policy which is deployed to all CHS AWS customer accounts.

CHS implements AWS tools across the environment to log all network activity within the VPCs and detect network vulnerabilities. Customers within CHS inherit a zero-trust network architecture that can be implemented within the customer's environment, provided the customer adheres to CHS and AWS guidelines.

Service Control Policies (SCPs) are permissions policies that apply at the account or organizational unit (OU) level to govern all principals in the account(s). SCPs are ideal for macro-level controls such as controlling the AWS regions allowed in an account. CHS uses SCPs along with OUs to ensure that only authorized services and regions can be used.

Custom environments allow user groups to develop and deploy architecturally unique applications using Amazon Web Services (AWS) services and supporting tools. A Custom Environment is made available by request to an organization that requires flexibility, minimal oversight, and the space to scale.

The CHS Cloud Shared Responsibility Model (CSRM) builds off and further defines the security roles for the CHS and the CHS customer. The purpose of the CSRM is to clarify the roles and responsibilities of each entity in providing a secure operating environment in the Cloud. Security and compliance is a shared responsibility between Amazon Web Services (AWS), CHS, and the CHS customer.


CUSTOMER
Responsible for the security IN their CHS Environment
CUSTOMER DATA
APPLICATION CONFIGURATION AND SECURITY
APPLICATION AUTHENTICATION
APPLICATION NETWORK ACCESS
APPLICATION SECURITY CONFIGURATION
APPLICATION LEAST PRIVILEGE - AWS IAM
OPERATING SYSTEM
OPERATING SYSTEM AUTHENTICATION AND AUTHORIZATION (A&A)
CONFIGURATION AND PATCH MANAGEMENT
OPERATING SYSTEM SECURITY; HOST INTRUSION DETECTION AND ANTIVIRUS
CHS
Responsible for the security OF the CHS Organizational Environment
ORGANIZATIONAL SECURITY
AWS ACCOUNT PROVISIONING
NETWORK INTRUSION DETECTION
AMAZON S3 DATA ACESS
INFRASTRUCTURE CHANGE MANAGEMENT
ORGANIZATIONAL NETWORK
AWS DIRECT CONNECT
TRANSIT NETWORK
FIREWALLS
DOMAIN NAME SYSTEM (DNS)
NETWORK LOGGING
AWS
Responsible for the security OF the Cloud
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
AWS REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Change Management within CHS is defined as controlling the change to products developed and provided by CHS in a responsible and concise manner. The purpose of change management is to implement approved, coordinated, and scheduled changes into a project or product with minimum disruption. The CHS Change Management (CM) system, Request For Change (RFC) process, and subsequent Change Request (CRQ) database are utilized to receive, analyze, track, and either approve or deny changes to CHS products and/or services.

The following table provides CHS cloud service usage (USGS only) over the past four fiscal years.

Service Usage by Fiscal Year

	FY18	**FY19**	**FY20**	**FY21 (up to 8/1)**
Custom Environment (# of new Centers)	2	13	7	6
Custom Environment (# of new accounts)	5	25	21	33
Cloud Backup (# of new projects)	13	7	4	5
Cloud Sensor Processing	0	3	4	1

Framework (# of new projects)				
Desktop-as-a-Service (# of new accounts)	0	0	15	5
Desktop-as-a-Service (# of users)	0	0	56	62
Pangeo (# of new users)	0	0	50	79
Tableau (# of new users)	0	57	209	88
Rescale (# of new users)	0	0	7	12

Services Released by Fiscal Year

	FY18	**FY19**	**FY20**	**FY21**
Number of New Services	10	19	27	16

NOTE: Reference case studies in Reading Room.

Scope of Work

The purpose of this effort is to acquire cloud computing services to replace existing aging infrastructure currently managed by the U.S. Department of the Interior (DOI) and Bureaus, allowing for growth and innovation of existing and new projects. There is an existing Virtual Data Center (VDC) currently residing in Amazon Web Services (AWS) under a previous USGS-issued NITAAC (https://nitaac.nih.gov/) task order.

Requirements and Capabilities

The cloud computing services solution shall provide the best value to Government while allowing DOI the flexibility to meet future requirements. The contractor shall provide cost effective cloud computing services that utilize industry standards and best practices that meet or exceed the following criteria.

1. The Contractor shall provide transition support from the current AWS cloud Enterprise Architecture (EA).
2. The Contractor shall provide the current list of cloud services and capabilities to ensure a smooth transition and avoid any service gaps that support mission critical applications.
3. The Contractor shall:
    a. Provide the ability to procure ‘third party’ services from vendors that provide services that are designed to enhance or complement the CSP environment associated with the award.
    b. Provide, at the Government’s option, access to elevated levels of support from the CSP, in a tiered level with accompanying payment levels that are clearly defined.
    c. Provide, at the Government’s option, consulting and other Cloud-related support services on an agreed-upon labor schedule. The USGS currently supports a Virtual Data Center (VDC) and associated support services with a combined government/contractor model. In general, contractors are used to provide architecture guidance, technical services, and knowledge transfer. It is anticipated that the DOI will continue to utilize contractors in

that mode going forward, as well as grow/shrink contracted services in proportion to DOI and Bureau needs.

4. The Contractor shall provide a hosting environment that has the following general capabilities:
    a. The Contractor shall offer Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) as stand-alone services, without the requirement to bundle them with managed hosting, application development, application maintenance or other outsourcing.
    b. Provide Software as a Service (SaaS) solutions with third-party vendors at the Government's option.
    c. Provide multiple physical hosting facilities in different geographic locations, at least 50 miles apart, to allow for hardware fault tolerance and disaster recovery. There needs to be at least three hosting centers located in the United States, including at least one in the proximity of the east and west coasts, to ensure the DOI can locate systems that will be resilient to a regional outage event.
    d. The DOI must be able to maintain control over what region a particular application or data set is located in.
5. The Contractor shall provide service management and provisioning capabilities, including:
    a. Rapid self-provisioning and de-provisioning of services via access to the CSP or third-party partner's commercially supplied interfaces.
    b. Secure web-based self-service portal for establishing, maintaining, and controlling services using technologies such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH).
    c. Support the terms of service requirement of terminating the service at any time (on demand).
    d. Provide automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc., via a service dashboard.
6. The contractor shall provide the following pricing and payment capabilities:
    a. Provide cloud services on a "pay-as-you-go" pricing model.
    b. Ability for the customer to identify and categorize services by sub-accounts, which can be rolled up into one master account for billing purposes.
    c. Cloud-related support services will generally be billed by fixed-price tasks, although time and materials (T&M) tasks based on contractually established professional labor categories may be used for some tasks.