DEPARTMENT OF VETERANS AFFAIRS

Office of Information and Technology (OIT)

Technology Acquisition Center (TAC)

REQUEST FOR INFORMATION (RFI)

VA Enterprise Cloud Brokerage Service

Federal Acquisition Package

RFI Number: 36C10B26Q0492

NAICS Code: 518210 - Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services

PSC Code: D399 - IT and Telecom - Other IT and Telecommunications

Set-Aside: Full and Open Competition (Market Research Phase)

Date Issued: June 2, 2026

Response Due: June 22, 2026

Classification: Controlled Unclassified Information (CUI)

DISCLAIMER / NOTICE

This document is issued for information and planning purposes only and does not constitute a solicitation or a commitment by the Government to issue a solicitation or award a contract. The Department of Veterans Affairs (VA) will not reimburse respondents for any costs associated with the preparation or submission of responses to this Request for Information (RFI). This RFI is issued pursuant to Federal Acquisition Regulation (FAR) 15.201, Exchanges with Industry Before Receipt of Proposals. The Government reserves the right to cancel this RFI at any time without obligation or notice.

TABLE OF CONTENTS

SECTION 1: STATEMENT OF OBJECTIVES (SOO)

1.1 Purpose

1.2 Background

1.3 Scope

1.4 Objectives

1.5 Explicitly Out of Scope

1.6 Period of Performance

1.7 Place of Performance

1.8 Applicable Standards and Regulations

SECTION 2: PERFORMANCE WORK STATEMENT (PWS)

2.1 General

2.2 Definitions

2.3 Task Areas

Task Area 1: Cloud Brokerage Platform Operations

Task Area 2: Credit Procurement and Financial Management

Task Area 3: Intake-to-Provisioning Automation

Task Area 4: Governance and Compliance

Task Area 5: Security and Risk Management

Task Area 6: Operational Handoff and Transition

2.4 Government-Furnished Property/Information

2.5 Contractor-Furnished Property

2.6 Security Requirements

2.7 Section 508 Compliance

2.8 Deliverables

SECTION 3: QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

3.1 Purpose

3.2 Performance Standards

3.3 Surveillance Methods

3.4 Procedures

3.5 Remediation Process

SECTION 4: INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

4.1 General Instructions

4.2 RFI Response Format

4.3 RFI Response Content Structure

4.4 Submission Instructions

4.5 Points of Contact

4.6 Important Notices

SECTION 5: MARKET RESEARCH QUESTIONS

Category A: Cloud Brokerage Platform Capabilities

Category B: Security and Compliance

Category C: Pricing and Commercial Models

Category D: Transition and Operations

Category E: Innovation and Future State

SECTION 6: ATTACHMENTS AND EXHIBITS

Attachment 6-1: Acronym and Definition List

Attachment 6-2: Service Level Agreement (SLA) Matrix

Attachment 6-3: Labor Category Descriptions

Attachment 6-4: Deliverables Schedule

Attachment 6-5: Government-Furnished Equipment/Information List

Attachment 6-6: Security Requirements Checklist

SECTION 1: STATEMENT OF OBJECTIVES (SOO)

1.1 Purpose

The Department of Veterans Affairs (VA), Office of Information and Technology (OIT), through the Technology Acquisition Center (TAC), issues this Request for Information (RFI) pursuant to Federal Acquisition Regulation (FAR) 15.201, *Exchanges with Industry Before Receipt of Proposals*, to seek industry feedback and capability demonstrations for a Cloud Brokerage Service. The intended

Cloud Brokerage Service shall consolidate, optimize, and govern multi-cloud operations across the VA Enterprise Cloud (VAEC) environment.

Several ongoing FinOps pilots and governance programs are developing cost-visibility, optimization, and reporting capabilities. To avoid duplication, this RFI is not seeking solutions that recreate or replace existing FinOps dashboards, cost-optimization tooling, tagging frameworks, or multi-cloud visibility services. This RFI is focused specifically on identifying partners who can help streamline and modernize how VA procures, allocates, and charges back CSP credits, consistent with ongoing Infrastructure Operations (IO) FinOps guidance.

This RFI is issued solely for market research and information-gathering purposes. It does not constitute a solicitation, a Request for Proposal (RFP), or a Request for Quotation (RFQ), and it shall not be construed as a commitment by the Government to issue a solicitation or ultimately award a contract. The Government will not reimburse respondents for any costs incurred in preparing or submitting responses to this RFI. Responses will not be evaluated for contract award. Information received may be used to shape requirements for a potential future acquisition.

1.2 Background

The VA Enterprise Cloud (VAEC) serves as the Department's primary cloud computing environment, currently hosting approximately 757 applications across three Federal Risk and Authorization Management Program (FedRAMP) High-certified Cloud Service Providers (CSPs): Amazon Web Services (AWS) and Microsoft Azure. The VAEC supports mission-critical operations for the three VA administrations - the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA) - as well as OIT and VA Central Office (VACO) staff offices.

The Enterprise Cloud Solutions Office (ECSO), operating within OIT, manages the VAEC environment and serves as the central governing body for cloud strategy, operations, and policy enforcement across the Department. ECSO is responsible for ensuring that all cloud-hosted workloads comply with federal security requirements, VA-specific directives, and applicable regulatory standards. While VA faces challenges in Cloud Credit procurement and chargeback consistency, FinOps pilots are actively addressing cost-management challenges such as optimization, multi-cloud visibility, and standardized tagging. This RFI limits its scope to procurement and financial-allocation challenges, not optimization or FinOps tooling duplication.

As the VAEC continues to mature and expand, the VA faces several operational challenges that this acquisition seeks to address:

- **Manual Credit Procurement:** Cloud credit procurement processes are largely manual, creating delays in provisioning and inefficient use of appropriated funds across fiscal year boundaries for customer chargeback purposes.
- **CSP Credit Procurement & Chargeback Complexity:** Current processes for purchasing, allocating, and financially reconciling cloud service provider (CSP) credits are inconsistent and labor intensive. This RFI focuses specifically on improving the efficiency, transparency, and automation of *how VA buys, allocates, and charges back CSP credits*, distinct from other efforts that address cost optimization, tagging, engineering, or FinOps operational capabilities.
- **Inconsistent Governance:** Governance policies, including tagging standards, naming conventions, access controls, and approved service configurations, are implemented differently across CSP environments, leading to compliance gaps and audit findings.
- **Manual Intake and Provisioning Workflows:** Cloud resource requests are processed through semi-manual workflows, resulting in extended fulfillment timelines and inconsistent configurations.
- **Limited Chargeback Granularity:** The current chargeback model lacks the granularity needed to accurately allocate costs to individual programs, offices, and cost centers, limiting financial accountability across VA business lines.
- **CSP Expansion Requirements:** The VA is exploring expansion to additional FedRAMP High-authorized CSPs beyond its current AWS and Azure footprint to support workload portability, avoid vendor lock-in, and leverage best-of-breed services, further complicating multi-cloud management.

1.3 Scope

The Cloud Brokerage Service shall provide comprehensive, end-to-end lifecycle management across multiple FedRAMP High-authorized Cloud Service Providers. The scope of services encompasses the following functional areas:

1. **Multi-CSP Credit and Commitment Procurement and Management.** The Contractor shall procure, allocate, track, and reconcile cloud credits, reservations, and financial commitments across all managed CSP environments on behalf of the VA.

2. **Enterprise Discount and Savings Plan Optimization.** The Contractor shall continuously analyze consumption patterns and execute strategies leveraging Reserved Instances, Savings Plans, Committed Use Discounts, and Enterprise Discount Programs to maximize cost savings.
3. **Financial Management with Chargeback/Showback.** The Contractor shall implement granular financial management capabilities, including chargeback and showback reporting to VA business lines, programs, and organizational cost centers with monthly reconciliation.
4. **Automated Intake-to-Provisioning Pipeline with Approval Workflows.** The Contractor shall provide a self-service intake portal with configurable, multi-tier approval workflows and automated provisioning of approved cloud resources using Infrastructure-as-Code (IaC) methodologies. The response shall include workflow automations that can be derived from requestor inputs.
5. **Cloud Governance and Policy Enforcement.** The Contractor shall implement and enforce governance policies encompassing tagging standards, naming conventions, regional restrictions, approved service catalogs, and security guardrails using policy-as-code frameworks across all managed CSP environments.
6. **Enhanced Tiered Reporting.** The Contractor shall implement a tiered reporting dashboard for Executives, Product Line Management, & Customer Journey management teams to include monitoring of Operational KPIs.
7. **Security and Compliance Monitoring.** The Contractor shall integrate security and compliance monitoring with VA Security Operations Center (SOC) capabilities, Enterprise Security Architecture, and Continuous Diagnostics and Mitigation (CDM) programs.
8. **Operational Handoff, Transition Management, and Knowledge Transfer.** The Contractor shall execute structured transition-in and transition-out activities, maintain comprehensive operational documentation, and conduct periodic knowledge transfer sessions with VA staff.
9. **AI/ML Cost Optimization and Workload Placement Recommendations.** The Contractor shall leverage artificial intelligence and machine learning capabilities to provide intelligent cost optimization recommendations, workload placement analysis, and predictive analytics for capacity planning and spend forecasting.

Where Cloud Broker activities intersect with FinOps, the Broker's role is limited to:

- Providing data inputs necessary for CSP credit procurement decisions
- Supporting RI/SP rate analysis only where it informs procurement strategy
- Executing allocation or chargeback workflows once defined by VA FinOps

1.4 Objectives

The VA seeks to achieve the following specific, measurable objectives through the Cloud Brokerage Service:

Establish a unified Cloud Brokerage Platform supporting a minimum of two (2) FedRAMP High-authorized CSPs (AWS and Microsoft Azure) with capacity to onboard additional CSPs. The Contractor shall ensure the platform for AWS and Microsoft Azure is operational within 6 months of contract start and additional CSPs are onboarded and operational within 12 months.

Obj. #	Objective	Success Metric
O-1	Reduce cloud credit procurement cycle time by forty percent (40%) or greater from current baseline.	Measured quarterly against baseline established during transition-in.
O-2	Achieve ninety-eight percent (98%) or greater chargeback accuracy to VA organizational cost centers.	Monthly reconciliation audit; variance ≤ 2%.
O-3	Automate eighty percent (80%) or greater of standard cloud resource provisioning requests through self-service workflows.	Measured monthly; ratio of automated to total standard requests.
O-4	Maintain continuous Authority to Operate (ATO) compliance across all managed CSP environments.	Zero lapses in ATO status; continuous compliance monitoring dashboard.
O-5	Deliver monthly FinOps dashboards with cost anomaly detection, trend analysis, and optimization recommendations.	Dashboard delivered by the 10th business day of each month; anomaly detection latency ≤ 24 hours.
O-6	Provide real-time reporting dashboards with Customer Journey mapping and integrate with VA's intake system.	Real-time reporting of current Customer Journey lifecycle with remaining exit criteria
O-7	Provide real-time governance policy enforcement with automated remediation for non-compliant resources.	Policy violation detection ≤ 15 minutes; automated remediation for 90%+ of standard violations.

Obj. #	Objective	Success Metric
O-8	Enable workload portability assessments and migration planning across CSPs to support strategic workload placement.	Portability assessment reports for 100% of Tier 1 applications within 18 months. Portability assessment reports for 100% of newly added Tier 1 applications within 12 months.
O-9	Integrate with VA's existing enterprise platforms, including ITSM (ServiceNow), Identity (SailPoint/Okta), and monitoring (Splunk).	Bi-directional integration operational within 6 months of contract start for AWS and Azure and within 12 months of contract start for new CSPs.
O-10	Achieve System and Organization Controls (SOC) 2 Type II and FedRAMP High operational compliance for the Cloud Brokerage Platform itself.	SOC 2 Type II attestation and FedRAMP High authorization maintained throughout period of performance.
O-11	Provide Monthly KPI reporting for Customer Journey analytics.	Report shall include Journey entry and exit criteria for process mapping, FinOps services, project reengagements, and modernization opportunities
O-12	Provide FinOps Backlog Tracking Metrics	Monthly reporting for FinOps programming, to include optimizations, rightsizing, unattached resources, & Discount and Savings Optimization efforts.

1.5 Explicitly Out of Scope

The below tasks are ongoing efforts within VA and would not be a desired objective of this effort.

- Introducing new cost-visibility dashboards or multi-cloud reporting functions already under the FinOps program
- Duplicating optimization engines, RI/SP analytics, or savings-plan governance
- Adding policy-as-code or cloud governance layers that overlap with existing VA governance tools
- Re-creating ATO-in-a-box, onboarding accelerators, or architecture templates managed under IO Architecture and Security. These activities are already in execution under FinOps, Governance, or Architecture programs and should not be proposed as Cloud Broker capabilities.

- The Broker shall not create or operate any hosted application facing FinOps dashboards, governance tooling, optimization algorithms, or reporting systems that duplicate current VA FinOps efforts.

1.6 Period of Performance

The anticipated period of performance for the resulting contract shall be structured as follows:

Period	Duration	Description
Base Year	12 Months	Knowledge transfer, system integration, parallel operations, baseline establishment. Full transition of AWS and Azure within the first six (6) months Full transition of additional CSPs within twelve (12) months
Option Year 1	12 Months	Full operational capability for all task areas.
Option Year 2	12 Months	Continued operations with performance-based enhancements.
Option Year 3	12 Months	Continued operations with performance-based enhancements.
Option Year 4	12 Months	Continued operations with performance-based enhancements.
Option Year 5	12 Months	Continued operations with performance-based enhancements.
Transition-Out	6 Months (two 3-month optional Tasks)	Optional Task 1: Knowledge transfer, documentation handoff, 90-day post-transition support. Optional Task 2: Knowledge transfer, documentation handoff, 90-day post-transition support.

The total potential period of performance, including transition periods, is six (6) years and six (6) months. The Government may exercise option years at its sole discretion in accordance with FAR 52.217-9, *Option to Extend the Term of the Contract*.

1.7 Place of Performance

Primary Place of Performance: VA Office of Information and Technology, Washington, DC metropolitan area. The Contractor's primary facility supporting this effort must be located within the Continental United States (CONUS).

Remote Work: The primary place of performance is at the Contractor’s facility or remote performance. All remote work locations must meet VA security requirements for handling Controlled Unclassified Information (CUI) and be within CONUS.

Travel: The Contractor shall anticipate periodic travel to VA facilities nationwide, including but not limited to VA data center locations and regional offices, not to exceed an estimated four (4) trips per year for 2 resources per trip. Travel shall be reimbursed in accordance with the Federal Travel Regulation (FTR) and requires prior COR approval Travel cost shall be included as a Firm-Fixed Price amount built into the Contract Line Item price.

1.8 Applicable Standards and Regulations

The Contractor shall comply with the following standards, regulations, directives, and executive orders throughout the period of performance:

Standard / Regulation	Description / Applicability
FedRAMP High Baseline	All managed CSP environments and the brokerage platform itself shall maintain FedRAMP High authorization.
NIST SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations. Applicable control baselines per system categorization.
NIST SP 800-171 Rev. 2	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
VA Directive 6500	VA Information Security Program. Governs all VA information and information systems.
VA Handbook 6500	Risk Management Framework for VA Information Systems. Defines ATO process and ongoing authorization requirements.
Federal Information Security Modernization Act (FISMA)	Requires federal agencies to implement information security programs. Annual assessment and reporting requirements.
Federal Information Technology Acquisition Reform Act (FITARA)	CIO authority over IT investments and acquisitions. ECSO governance alignment required.
OMB Circular A-130	Managing Information as a Strategic Resource. Governs federal information resources management.
FAR Part 39	Acquisition of Information Technology. Governs IT procurement policies and procedures.
VAAR Part 839	VA Acquisition Regulation - Acquisition of Information Technology. VA-specific IT procurement requirements.
Section 508, Rehabilitation Act	All electronic and information technology deliverables must be accessible to individuals with disabilities.
Executive Order 14028	Improving the Nation's Cybersecurity. Zero trust architecture, software supply chain security, incident reporting requirements.

Standard / Regulation	Description / Applicability
NIST SP 800-161 Rev. 1	Cybersecurity Supply Chain Risk Management Practices. Supply chain risk management program requirements.

SECTION 2: PERFORMANCE WORK STATEMENT (PWS)

2.1 General

This Performance Work Statement (PWS) describes the performance-based requirements for the VA Enterprise Cloud Brokerage Service as outlined in the Statement of Objectives (SOO), Section 1 of this document. This acquisition is structured as a performance-based acquisition in accordance with FAR Subpart 37.6, *Performance-Based Acquisition*, and OMB Circular A-76, *Performance of Commercial Activities*. The Contractor shall provide all personnel, management, supervision, equipment, tools, materials, and facilities necessary to perform the tasks described herein, except as specified in Section 2.4 (Government-Furnished Property/Information).

The Contractor shall perform all work in accordance with the quality standards defined in the Quality Assurance Surveillance Plan (QASP), Section 3 of this document. Performance shall be measured against the objectives, standards, and acceptable quality levels defined therein. The Contractor is expected to exercise professional judgment and apply industry best practices, including FinOps Foundation principles, Cloud Security Alliance (CSA) guidance, and IT Infrastructure Library (ITIL) frameworks, in the execution of all task areas.

2.2 Definitions

The following terms and definitions apply throughout this document:

Term	Definition
Cloud Brokerage Platform	An integrated technology platform that serves as an intermediary between the VA and multiple Cloud Service Providers, providing unified management of

Term	Definition
	procurement, provisioning, governance, financial management, security, and operations across heterogeneous cloud environments.
Cloud Service Provider (CSP)	A third-party company that provides cloud computing services, including infrastructure, platforms, and software delivered over the internet. In this context, CSPs must hold FedRAMP High authorization.
Chargeback	A financial management practice in which actual cloud consumption costs are billed back to the consuming organizational unit, program, or cost center based on measured usage.
Customer Journey	The end-to-end path an internal customer follows during the cloud intake process, from initial Intake request submission through assessment, approvals, provisioning, and Deployment. Continuance into Sustainment and Operations Management are NOT within the scope of this PWS.
Showback	A financial reporting practice that displays cloud consumption costs attributable to an organizational unit without formal billing, used for awareness and accountability.
FinOps	Financial Operations - a collaborative practice combining systems, best practices, and culture to increase an organization's ability to understand and manage cloud costs and make business tradeoffs.
FinOps Capabilities	FinOps Capabilities (Existing VA Program): A set of ongoing VA initiatives that include: • Multi-cloud cost visibility • Tagging standards • Optimization analytics (RI/SP, usage, commitment) • Spend management policy and dashboards
Authority to Operate (ATO)	A formal authorization granted by an Authorizing Official that permits a system to operate at an accepted level of risk based on the implementation of an approved set of security and privacy controls.
Continuous ATO (cATO)	An approach to authorization that replaces periodic re-authorization with continuous monitoring, automated evidence collection, and real-time risk assessment to maintain ongoing operational authorization.
Landing Zone	A pre-configured, security-hardened cloud environment with baseline networking, identity, security, and governance configurations that serves as the foundation for deploying workloads.
Guardrail	An automated policy mechanism that prevents or detects cloud resource configurations that violate organizational standards for security, compliance, cost, or operational best practices.
Intake Request	A formal request submitted by a VA stakeholder for cloud resources, services, or changes, processed through the brokerage platform's intake portal and approval workflow.
Provisioning	The process of allocating, configuring, and deploying cloud resources (compute, storage, networking, services) to a requestor's environment using approved templates and automation.

Term	Definition
Workload	A distinct application, service, or set of computing tasks running on cloud infrastructure that can be identified, managed, and measured as a unit.
Tenant	A logical organizational unit within the cloud brokerage platform, typically corresponding to a VA program, administration, or office, with isolated resources, access controls, and cost tracking.
Cost Center	A VA organizational or programmatic unit to which cloud costs are allocated for financial tracking, budgeting, and accountability purposes.
Enterprise Discount Program (EDP)	A negotiated pricing arrangement between an enterprise customer and a CSP that provides volume-based discounts on cloud services in exchange for spend commitments.
Savings Plan	A CSP pricing model (e.g., AWS Savings Plans) that offers reduced rates in exchange for a commitment to a consistent amount of usage (measured in $/hour) for a one- or three-year term.
Reserved Instance	A CSP pricing model that provides a significant discount compared to on-demand pricing in exchange for a commitment to use a specific instance type in a specific region for a one- or three-year term.
Spot Instance	A CSP pricing model that allows customers to use spare cloud capacity at steep discounts, with the understanding that instances may be reclaimed by the CSP with short notice.

2.3 Task Areas

2.3.1 Task Area 1: Cloud Brokerage Platform Operations

2.3.1.1 Platform Deployment and Configuration

The Contractor shall deploy, configure, and maintain the Cloud Brokerage Platform in a FedRAMP High-authorized environment. The platform shall provide:

- Multi-tenant architecture with logical isolation between VA organizational units.
- Role-based access control (RBAC) with integration to VA's enterprise identity management systems.
- Comprehensive Application Programming Interface (API) framework for integration with VA enterprise tools, including ServiceNow, Splunk, SailPoint, and Okta.
- Web-based management console compliant with Section 508 accessibility requirements.

- Automated backup, disaster recovery, and business continuity capabilities with a Recovery Time Objective (RTO) of four (4) hours and a Recovery Point Objective (RPO) of one (1) hour.
- Release management processes with documented change control, testing, and rollback procedures.

2.3.1.2 Multi-CSP Account and Subscription Management

The Contractor shall manage organizational structures across all supported CSP environments, including but not limited to:

- AWS Organizations - management of organizational units (OUs), accounts, and service control policies (SCPs).
- Azure Management Groups - management of management group hierarchies, subscriptions, and Azure Policy assignments.
- Google Cloud Platform (GCP) Folders - management of organization, folder, and project hierarchies (if applicable).
- Oracle Cloud Infrastructure (OCI) Compartments - management of tenancy structure, compartment hierarchies, and OCI Identity and Access Management (IAM) policy assignments.
- Account lifecycle management including creation, configuration, monitoring, decommissioning, and archive of CSP accounts/subscriptions.
- Consolidated billing management and cost allocation tag propagation across account hierarchies.

2.3.1.3 Service Catalog Management

The Contractor shall develop and maintain an approved service catalog of pre-vetted, FedRAMP High-compliant cloud services. The service catalog shall include:

- Categorized listing of approved cloud services by CSP, with security classification levels and approved use cases.
- Automated provisioning templates (IaC) for each cataloged service.
- Service descriptions, pricing information, compliance implications, and usage guidelines.

- Monthly review cycle to evaluate new CSP service offerings for inclusion and retire deprecated services.
- Exception request process for services not currently in the approved catalog.
- Maintain Standard Image Baselines with repository management and version controls

2.3.1.4 Platform Availability

The Contractor shall maintain ninety-nine point nine percent (99.9%) platform uptime, calculated monthly, excluding planned maintenance windows. Planned maintenance shall be scheduled during non-peak hours (10:00 PM – 6:00 AM Eastern Time, weekends, and federal holidays) and communicated to stakeholders a minimum of seventy-two (72) hours in advance. Emergency maintenance may be performed with two (2) hours advance notice with VA PM and COR notification.

2.3.2 Task Area 2: Credit Procurement and Financial Management

2.3.2.1 Multi-CSP Credit Procurement

The Contractor shall procure, allocate, and track cloud credits and financial commitments across all managed CSPs on behalf of the VA. Responsibilities include:

- Executing credit purchases and commitment agreements in accordance with VA-approved procurement authorities and appropriation constraints.
- Tracking credit balances, expiration dates, and utilization rates across all CSP accounts.
- Providing advance notification (minimum 60 days) of credit expiration to enable timely action.
- Providing forecast estimation per CSP to include; date of current funds expiration per CSP, a forecasted consumption need per CSP for the next future credit purchase, a forecasted total lifecycle date of projected consumption and date of forecasted expiration per CSP. All forecasts shall provide transparent mathematical logic behind all forecasts.
- Managing credit transfers and reallocations between VA organizational units as directed by the COR.
- Ensuring alignment of credit procurement with federal fiscal year boundaries and appropriation requirements (31 U.S.C. § 1502, Bona Fide Needs Rule).

2.3.2.2 Discount and Savings Optimization

The Contractor shall continuously analyze cloud usage patterns and recommend and/or execute cost optimization strategies, including:

- Reserved Instance (RI) purchasing recommendations and lifecycle management, including modification, exchange, and marketplace resale where applicable.
- Savings Plan coverage analysis and commitment recommendations.
- Committed Use Discount (CUD) strategy for GCP environments.
- Oracle Cloud Infrastructure (OCI) Universal Credits and Annual Flex pricing analysis and commitment management.
- Enterprise Discount Program (EDP) negotiation support and compliance monitoring.
- Right-sizing recommendations for underutilized or idle resources.
- Spot/Preemptible instance strategy for fault-tolerant workloads.
- Monthly savings realization report quantifying actual savings achieved against on-demand baseline pricing.

2.3.2.4 Chargeback and Showback

The Contractor shall implement and operate a granular chargeback and showback system that provides:

- Cost allocation to VA organizational units, programs, projects, and cost centers based on actual consumption.
- Allocation of shared costs (e.g., landing zone infrastructure, shared services, platform fees) using configurable allocation methodologies approved by the COR.
- Monthly chargeback reports delivered by the tenth (10th) business day of each month for the prior month's consumption.
- Self-service showback dashboards accessible to VA cost center managers with real-time or near-real-time data (latency ≤ 24 hours).
- Monthly reconciliation process with documented variance analysis for discrepancies exceeding two percent (2%).
- Integration with VA financial systems for automated chargeback data feeds.

2.3.2.5 Budget Forecasting and Anomaly Detection

The Contractor shall provide AI-driven budget forecasting and automated anomaly detection capabilities, including:

- Monthly and quarterly spend forecasts with configurable confidence intervals, using a minimum of twelve (12) months of historical data.
- Automated anomaly alerts triggered when consumption deviates beyond configurable thresholds. The default threshold shall be fifteen percent (15%) above projected spend, adjustable per product line or products.
- Root cause analysis support for cost anomalies within four (4) business hours of alert generation.
- Annual budget planning support with scenario modeling capabilities (best case, expected, worst case).
- Trending analysis identifying cost drivers, growth trajectories, and optimization opportunities.

2.3.2.6 Invoice Reconciliation

The Contractor shall reconcile CSP invoices against internal consumption tracking on a monthly basis. Responsibilities include:

- Line-item reconciliation of CSP invoices against brokerage platform consumption records.
- Identification, documentation, and resolution of discrepancies within ten (10) business days.
- Maintenance of auditable financial records for a minimum of seven (7) years in compliance with federal records retention requirements.
- Support for audits from Government agencies such as VA Office of Inspector General (OIG) and Government Accountability Office (GAO) audits related to this Contract.

2.3.3 Task Area 3: Provisioning Automation known as the Customer Journey Management Process

2.3.3.2 Automated Provisioning

The Contractor shall automate provisioning of approved cloud resources using Infrastructure-as-Code (IaC) templates and methodologies, including:

- Terraform modules for multi-CSP resource provisioning.
- AWS CloudFormation templates for AWS-specific resources.
- Azure Bicep/ARM templates for Azure-specific resources.
- OCI Resource Manager (Terraform-based) stacks for Oracle Cloud Infrastructure-specific resources.
- Version-controlled IaC repositories with code review and approval processes.
- Automated triage to evaluate Provisioning supportability using a structured gate-check process.
- Automated testing (linting, security scanning, compliance validation) of IaC templates prior to deployment.
- Idempotent, repeatable deployments with documented rollback procedures.

2.3.3.3 Landing Zone Deployment

The Contractor shall deploy and maintain standardized, security-hardened landing zones for each managed CSP environment. Landing zones shall incorporate:

- Network segmentation with micro-segmentation capabilities aligned to VA security architecture.
- Centralized logging and monitoring integration with VA Splunk and Security Operations Center (SOC).
- Identity federation with VA enterprise Active Directory and identity governance platforms.
- Baseline security controls pre-implemented per NIST SP 800-53 Rev. 5 High baseline.
- Automated compliance scanning and drift detection upon deployment.

- Documented landing zone architecture with regular review and update cycle (minimum quarterly).
- Coordination and approval through a Government-Controlled Change Management Process.

2.3.3.4 Approval Workflow Engine

The Contractor shall configure and operate multi-tier approval workflows with the following capabilities:

- Configurable approval tiers: Technical Review, Security Review, Financial Review, and Executive Approval.
- Automated routing based on request type, cost threshold, security classification, and organizational unit.
- SLA-based escalation: automatic escalation to next-level approver if approval is not completed within defined SLA (default: 24 business hours per tier).
- Delegation of authority capabilities for approver absences.
- Audit trail of all approval actions with timestamp, approver identity, and decision rationale.

2.3.3.5 Customer Satisfaction & Feedback

The Contractor shall implement a customer satisfaction program that incorporates both human and AI-enabled feedback capabilities where possible.

- Conduct customer satisfaction surveys and post-interaction surveys to measure service quality for the intake through provisioning Customer Journey points.
- Use AI-assisted analysis (e.g., sentiment analysis, pattern detection, trend identification) to automatically assess feedback and identify recurring issues or improvement opportunities.
- Maintain a closed-loop feedback process to review results, perform root-cause analysis on negative trends, and implement corrective actions.
- Report customer satisfaction metrics, AI-generated insights, and documented improvement actions during monthly and quarterly service reviews.

2.3.3.6 Request Fulfillment SLAs

The Contractor shall fulfill cloud resource requests within the following service level targets:

Request Category	Definition	Fulfillment SLA	AQL
Standard Request	Pre-approved, catalog-based requests requiring no additional security review (e.g., standard VM, storage, database from approved templates).	4 business hours from final approval	95% compliance
Complex Request	Requests requiring custom configuration, security review, or multi-service orchestration.	3 business days from final approval	90% compliance
Emergency Request	Urgent requests approved by COR or designee to support critical mission operations.	2 business hours from final approval	95% compliance
Customer Satisfaction	Metrics that showcase customer satisfaction results at the Customer Journey checkpoints	Monthly & Quarterly	100% Compliance

2.3.4 Task Area 4: Governance and Compliance

2.3.4.1 Policy-as-Code

The Contractor shall implement and enforce governance policies across all managed CSP environments using policy-as-code frameworks, including but not limited to:

- Open Policy Agent (OPA) / Rego for cross-CSP policy evaluation.
- AWS Service Control Policies (SCPs) and AWS Config Rules for AWS environments.
- Azure Policy and Azure Blueprints for Azure environments.
- Sentinel (HashiCorp) for Terraform-integrated policy enforcement.
- OCI Policies and OCI Cloud Guard for Oracle Cloud Infrastructure governance and threat detection.
- Policies shall enforce VA-Approved: tagging standards, naming conventions, allowed regions (US-only for VA data), approved instance types and sizes, required encryption configurations, network access controls, and prohibited service usage.
- All policies shall be version-controlled, peer-reviewed, and tested in non-production environments prior to enforcement.

2.3.4.2 Tagging Enforcement

The Contractor shall enforce a mandatory VA-Approved tagging taxonomy for all cloud resources across all managed CSP environments. The tagging taxonomy shall include, at minimum:

Tag Key	Purpose	Example Values	Required
va:cost-center	Cost allocation to VA organizational unit	VHA-EHRM, VBA-CLAIMS, NCA-OPS	Yes
va:application-id	Application identification and portfolio tracking	APP-00752, APP-01234	Yes
va:environment	Environment classification	production, staging, development, sandbox	Yes
va:data-classification	Data sensitivity level	CUI, PHI, PII, Public	Yes
va:owner	Resource ownership and accountability	team-email or individual-id	Yes
va:compliance-scope	Applicable compliance framework	FedRAMP-High, HIPAA, PCI	Yes
va:expiration-date	Resource lifecycle management	2027-03-31	Conditional

The Contractor shall identify non-compliant resources, including: automated tagging of resources with default values where determinable, notification to resource owners for resources missing required tags, and automated quarantine or deletion of untagged resources after a configurable grace period (default: 14 calendar days) with COR approval.

2.3.4.3 Compliance Monitoring

The Contractor shall perform continuous compliance monitoring against NIST SP 800-53 Rev. 5, FedRAMP High Baseline, and VA Directive 6500 controls. Monitoring shall include:

- Automated evidence collection for applicable technical controls with mapping to NIST control families.
- Continuous compliance scoring dashboards accessible to VA security personnel and ECSO leadership.
- Automated generation of Plan of Action and Milestones (POA&M) entries for identified deficiencies.
- Integration with VA's GRC (Governance, Risk, and Compliance) platform for centralized compliance tracking.
- Support for Third-Party Assessment Organization (3PAO) audits, including evidence package preparation and audit facilitation.

2.3.4.4 Drift Detection

The Contractor shall identify infrastructure configuration drift detection and remediation capabilities, including:

- Continuous comparison of deployed resource configurations against approved IaC baselines.
- Automated alerting within fifteen (15) minutes of drift detection for security-relevant configurations.
- Automated remediation (self-healing) for pre-approved drift categories (e.g., security group modifications, encryption settings).
- Semi-automated remediation with human approval for complex drift scenarios.
- Weekly drift summary reports with trend analysis and root cause categorization.

2.3.4.5 Reporting

The Contractor shall generate and deliver VAEC-Approved Governance and Compliance Reports on the following schedule:

- **Monthly:** Governance compliance reports detailing policy compliance rates, tagging compliance, drift incidents, remediation actions, and exception requests.
- **Quarterly:** Executive briefings summarizing governance posture, trends, risks, and recommendations for VAEC leadership.
- **Annually:** Comprehensive governance maturity assessment benchmarked against industry standards (e.g., FinOps Foundation maturity model, CSA Cloud Controls Matrix).
- **Ad hoc:** Custom reports as requested by the COR or Contracting Officer with a seven (7) business day turnaround.

2.3.5 Task Area 5: Security and Risk Management

2.3.5.1 Security Integration

The Contractor shall integrate the Cloud Brokerage Platform and all managed cloud environments with VA's security operations infrastructure, including:

- Obtain and retain an Authorization To Operate (ATO) - following VA Governance, Risk, and Compliance (GRC) policies and procedures.

- VA Cybersecurity Operations Center (VA CSOC) - security event forwarding, alert correlation, incident coordination, and forensic support..
- Continuous Diagnostics and Mitigation (CDM) program - asset discovery, vulnerability data, and configuration data feeds.
- VA Enterprise Security Architecture - alignment with zero trust architecture principles per Executive Order 14028 and OMB Memorandum M-22-09.
- Enterprise SIEM - log aggregation, correlation rules, and alerting for cloud-specific security events.

2.3.5.2 Vulnerability Management

The Contractor shall monitor VA vulnerability scanning results, support Application Owners with remediation tracking, and POA&M management for all brokerage-managed infrastructure. Responsibilities include:

- Review monthly automated vulnerability scanning of all managed cloud resources using VA-approved scanning tools.
- Support Critical/High/Moderate vulnerability remediation per VA Security Policy.
- Provide POA&M support, tracking, and remediations for all identified vulnerabilities with milestones and responsible parties.

2.3.5.3 Identity and Access Management

The Contractor shall integrate the Cloud Brokerage Platform with the Department of Veterans Affairs (VA) enterprise Identity and Access Management (IAM) infrastructure to ensure secure, standardized, and compliant access to all brokerage and Cloud Service Provider (CSP) environments. At a minimum, the Contractor shall support the following capabilities:

- Federated Authentication using VA Active Directory through Security Assertion Markup Language (SAML) 2.0 or OpenID Connect (OIDC) to provide single sign-on (SSO) and centralized identity validation.
- Integration with Microsoft Entra ID (Azure Active Directory) to support modern authentication using OAuth 2.0 and OIDC, aligned with VA Zero Trust and Conditional Access requirements.

    - Directory synchronization and lifecycle management for user, service, and group objects utilized by the Cloud Brokerage Platform.
    - Enforcement of VA-approved Multi-Factor Authentication (MFA) policies through Conditional Access and authentication strength requirements.
    - Role-Based Access Control (RBAC) alignment between Entra ID security groups and platform roles to ensure least-privilege access.
    - Monitoring and logging of identity events through Entra ID Identity Protection, including risk-based sign-in detection, anomaly reporting, and integration with VA security operations.
- Integration with SailPoint IdentityNow for identity governance, including automated provisioning/de-provisioning, access certifications, separation-of-duties checks, and role management.
- Integration with Okta for enforcement of Multi-Factor Authentication (MFA) per VA MFA policy where Okta is designated as the authoritative MFA provider.
- Privileged Access Management (PAM) for administrative access to cloud environments, including just-in-time (JIT) access capabilities, session recording, credential vaulting, and audit-ready reporting.
- Quarterly Access Reviews and re-certification of all user accounts with access to the Cloud Brokerage Platform, underlying CSP environments, or related administrative interfaces, in accordance with VA security and governance requirements.

2.3.5.4 Data Protection

The Contractor shall enforce data protection controls across all managed cloud environments, including:

- Encryption at rest using Advanced Encryption Standard (AES)-256 (or equivalent) for all data stored in managed CSP environments, utilizing CSP-managed or customer-managed encryption keys as directed by the COR.
- Encryption in transit using Transport Layer Security (TLS) 1.2 or higher for all data communications.
- Key management using Federal Information Processing Standards (FIPS) 140-2 Level 3 validated Hardware Security Modules (HSMs) or equivalent.

- Data Loss Prevention (DLP) monitoring for sensitive data categories, including Protected Health Information (PHI), Personally Identifiable Information (PII), and CUI.
- Data residency enforcement ensuring all VA data remains within authorized US geographic regions.

2.3.5.5 Incident Response

The Contractor shall support VA CSOC incident response procedures and maintain the following capabilities:

- **Initial Response SLA:** The Contractor shall acknowledge, triage, and initiate response within the current VA Policy timeframes.
- Forensic data collection and preservation capabilities, including log retention, memory captures, and disk snapshots per VA forensic procedures.
- Coordination with VA CSOC, US-CERT, and law enforcement as directed by the VA Chief Information Security Officer (CISO).
- Post-incident root cause analysis and lessons learned reports delivered within five (5) business days of incident closure.
- Annual incident response tabletop exercises with VA security personnel.
- Maintained and tested incident response playbooks specific to cloud security scenarios (e.g., compromised credentials, data exfiltration, cryptomining, unauthorized resource deployment).

2.3.6 Task Area 6: Operational Handoff and Transition

2.3.6.1 Transition-In Plan

The Contractor shall develop and execute a phased transition-in plan over a six (6) month period. The transition-in plan shall include:

- **Phase 1 - Discovery and Planning (Months 1-2):** Requirements validation, environment assessment, baseline establishment, integration planning, and transition schedule development.

- **Phase 2 - Build and Integrate (Months 2-4):** Platform deployment, integration with VA enterprise systems, IaC template development, policy configuration, and user acceptance testing.
- **Phase 3 - Pilot and Validate (Months 4-5):** Pilot deployment with selected VA applications, parallel operations with existing management processes, performance baselining, and issue resolution.
- **Phase 4 - Full Operations (Months 5-6):** Complete migration of management functions, decommission of replaced tools/processes, transition to steady-state operations, and formal acceptance by the COR.

2.3.6.2 Operational Documentation

The Contractor shall develop and maintain comprehensive operational documentation, including:

- Standard Operating Procedures (SOPs) for all recurring operational activities.
- Runbooks for incident response, escalation, and emergency procedures.
- Architecture diagrams (logical, physical, network, security) for the brokerage platform and all managed environments.
- Configuration documentation for all platform settings, policies, integrations, and IaC templates.
- All documentation shall be updated within five (5) business days of any operational change and maintained in a VA-accessible repository.

2.3.6.3 Knowledge Transfer

The Contractor shall conduct structured knowledge transfer sessions with VA staff on a quarterly basis. Knowledge transfer shall include:

- Platform administration training for designated VA technical staff.
- FinOps practices and cost management training for VA cost center managers.
- Governance policy management and exception handling training.
- Recorded training sessions with materials maintained in a VA-accessible learning management system.

- Cross-training to ensure VA staff can assume critical functions in the event of contract transition.

2.3.6.4 Transition-Out

The Contractor shall develop and execute a transition-out plan to be initiated no later than six (6) months prior to contract conclusion. The transition-out plan shall ensure:

- Zero data loss during transition of management responsibilities to the successor contractor or Government personnel.
- Complete documentation handoff, including all SOPs, runbooks, architecture diagrams, IaC repositories, policy configurations, and operational records.
- Ninety (90) calendar days of post-transition support, including subject matter expert availability (minimum 20 hours/week) for the successor entity.
- Orderly transfer of all credentials, access rights, and administrative privileges.
- Removal of all Contractor proprietary tools and data from VA environments within thirty (30) calendar days of contract conclusion.

2.3.6.5 Staffing

The Contractor shall provide qualified personnel in the labor categories described in Attachment J-3 (Labor Category Descriptions). The Contractor shall:

- Identify Key Personnel (Program Manager, Cloud Solutions Architect, FinOps Lead, Cloud Security Engineer) who shall not be removed or replaced without prior written COR approval.
- Maintain a maximum fifteen percent (15%) annual turnover rate for Key Personnel positions.
- Provide replacement personnel of equal or greater qualifications within thirty (30) calendar days of any vacancy.
- Ensure all personnel possess required certifications as specified in Attachment J-3 prior to performing work under this contract.

2.4 Government-Furnished Property/Information

The Government shall provide the following property, equipment, and information to support the Contractor's performance:

GFP #	Item	Description
GFP-1	VAEC Environment Access	Access to VA Enterprise Cloud environments in AWS and Azure, including management plane access for brokerage operations.
GFP-2	VA Network Connectivity (TIC 3.0)	Trusted Internet Connections (TIC 3.0) compliant network connectivity between Contractor facilities and VA environments.
GFP-3	ServiceNow Instance Access	Access to VA's ServiceNow ITSM instance for integration, ticket management, and workflow configuration.
GFP-4	VA Enterprise Security Tools	Access to VA-licensed security tools including Splunk, vulnerability scanners, and CDM tools as needed for integration.
GFP-5	System Documentation	Relevant system architecture documentation, security plans, ATO packages, and configuration baselines for VAEC environments.
GFP-6	Government Workspace	On-site workspace at VA facilities for Contractor personnel when required for on-site work. Subject to space availability.
GFP-7	VA Active Directory Integration	Integration access to VA Active Directory for federated authentication and identity management.
GFP-8	PIV Infrastructure	Access to VA's Personal Identity Verification (PIV) credentialing infrastructure for Contractor personnel.
GFP-9	VA-issued Laptops	Issuance of up to ten (10) laptops per CSP and not exceed forty (40) laptops for the total contract. All GFE shall be returned within seven (7) calendar days of separation of the resource.
GFP-10	VA-issued Smart/cellular Phones	Issuance of phones shall require pre-approval from the COR and not exceed six (6) phones for the total contract, inclusive of all CSPs. All GFE shall be returned within seven (7) calendar days of separation of the resource.

2.5 Contractor-Furnished Property

The Contractor shall furnish all equipment, software licenses, tools, materials, and facilities necessary to perform the work described in this PWS, unless specifically identified as Government-Furnished Property in Section 2.4. Contractor-furnished items shall include, but are not limited to:

- Cloud Brokerage Platform software licenses and hosting infrastructure.
- Development, testing, and staging environments for platform releases.

- Project management, collaboration, and documentation tools.
- Employee workstations, communication equipment, and office facilities.
- All third-party software licenses and tools required for service delivery.
- Training environments and materials for VA staff knowledge transfer.

2.6 Security Requirements

All Contractor personnel performing work under this contract shall comply with the following security requirements:

1. **Background Investigations:** All Contractor personnel shall undergo and pass a background investigation at Tier 2 (moderate risk) level, or higher as determined by VA position sensitivity designation, prior to accessing VA systems or data. Investigations shall be coordinated through the COR with the Personnel Security Adjudication Center (PSAC) and investigated by the Defense Counterintelligence and Security Agency (DCSA).
2. **PIV Credentials:** All Contractor personnel requiring access to VA facilities or information systems shall obtain and maintain Personal Identity Verification (PIV) credentials in accordance with Homeland Security Presidential Directive 12 (HSPD-12).
3. **Security Training:** All Contractor personnel shall complete VA Privacy and Information Security Awareness training and Health Insurance Portability and Accountability Act (HIPAA) training upon onboarding and annually thereafter. Role-based security training shall be completed as required by position.
4. **Contractor Rules of Behavior:** All Contractor personnel shall sign and comply with VA Handbook 6500.6, *Contract Security*, Appendix C, *Contractor Rules of Behavior*, prior to accessing VA systems.
5. **Incident Reporting:** The Contractor shall report all actual or suspected security incidents to the VA Network Security Operations Center (NSOC) within one (1) hour of discovery per VA Handbook 6500.2.
6. **Data Handling:** The Contractor shall handle, store, transmit, and dispose of VA data in accordance with VA Directive 6500 and applicable data classification requirements. All VA data shall be encrypted at rest and in transit.

2.7 Section 508 Compliance

All deliverables, platforms, portals, dashboards, reports, and tools provided under this contract shall comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794d), and conform to the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA success criteria. The Contractor shall:

- Conduct accessibility testing using automated and manual methods, including assistive technology testing (screen readers, keyboard navigation).
- Provide a Voluntary Product Accessibility Template (VPAT) based on the ITI VPAT 2.4 format for the Cloud Brokerage Platform.
- Remediate accessibility deficiencies identified during testing within thirty (30) calendar days.
- Include accessibility requirements in the platform's software development lifecycle (SDLC).

2.8 Deliverables

The Contractor shall provide the following Contract Data Requirements List (CDRL) deliverables throughout the period of performance:

CDRL #	Deliverable Title	Description	Format	Frequency	Due Date
001	Monthly Status Report	Comprehensive report covering task area progress, risks, issues, staffing, and upcoming milestones.	PDF/DOCX	Monthly	10th business day of each month
002	Monthly FinOps Dashboard	Cloud spend analysis, cost trends, optimization recommendations, anomaly alerts, and savings realization.	Web/PDF	Monthly	10th business day of each month
003	Quarterly Governance Report	Policy compliance rates, tagging compliance, drift incidents, remediation actions, and	PDF/DOCX	Quarterly	15th business day after quarter end

CDRL #	Deliverable Title	Description	Format	Frequency	Due Date
		governance posture assessment.			
004	Annual Security Assessment	Comprehensive security posture review, vulnerability assessment summary, compliance status, and risk assessment.	PDF/DOCX	Annually	90 days before ATO renewal
005	Transition-In Plan	Detailed plan with phases, milestones, resource requirements, risk mitigation, and acceptance criteria.	PDF/DOCX	One-time	15 calendar days after contract start
006	Transition-Out Plan	Comprehensive plan for knowledge transfer, documentation handoff, and post-transition support.	PDF/DOCX	One-time	180 days before contract end
007	Incident Reports	Security and operational incident reports with root cause analysis and corrective actions.	PDF/DOCX	As needed	5 business days after incident closure
008	Change Management Log	Log of all changes to managed environments including change description, risk, approval, and outcome.	Excel/CSV	Weekly	Every Monday by 12:00 PM ET
009	Service Catalog Updates	Updated service catalog with additions, retirements, pricing changes, and compliance notes.	Web/PDF	Monthly	Last business day of each month
010	SOPs/Runbooks	Standard operating procedures and runbooks for all operational processes. Updated as changes occur.	PDF/DOCX	As updated	5 business days after operational change

CDRL #	Deliverable Title	Description	Format	Frequency	Due Date
011	Training Materials	Training curricula, presentations, lab guides, and recorded sessions for VA staff knowledge transfer.	PPTX/PDF/Video	Quarterly	1 week prior to quarterly KT session
012	Executive Briefings	Quarterly briefings for ECSO leadership and VA CIO covering performance, trends, and strategic recommendations.	PPTX/PDF	Quarterly	10th business day after quarter end
013	Cost Optimization Recommendations	Monthly actionable recommendations for cost savings with projected impact and implementation plan.	PDF/DOCX	Monthly	15th business day of each month
014	Compliance Evidence Packages	Compiled evidence packages for ATO assessments, including control implementation evidence and test results.	PDF/Excel	Per ATO cycle	30 days before 3PAO assessment
015	Platform Release Notes	Documentation of platform updates, new features, bug fixes, and known issues for each release.	PDF/Web	Per release	48 hours prior to deployment

SECTION 3: QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

3.1 Purpose

This Quality Assurance Surveillance Plan (QASP) provides a systematic method for evaluating the Contractor's performance under the VA Enterprise Cloud Brokerage Service contract. This QASP is developed in accordance with FAR Subpart 46.4, *Government Contract Quality Assurance*, and VAAR Part 846, *Quality Assurance*. The QASP defines performance objectives, standards, acceptable quality levels (AQLs), surveillance methods, and incentive/disincentive mechanisms. The COR shall

use this QASP as the primary tool for monitoring and documenting Contractor performance throughout the period of performance.

This QASP is a living document and may be revised by the Contracting Officer in consultation with the COR as mission requirements evolve. Any revisions shall be documented in writing and provided to the Contractor.

3.2 Performance Standards

#	Performance Objective	Performance Standard	AQL	Surveillance Method	Incentive / Disincentive
1	Platform Availability	99.9% uptime, calculated monthly, excluding scheduled maintenance.	99.9%	Monthly system logs review; automated uptime monitoring.	Below 99.9%: service credit of 2% of monthly invoice per 0.1% below threshold. Below 99.5%: Corrective Action Request (CAR).
2	Standard Provisioning SLA	Standard requests fulfilled within 4 business hours of final approval.	95%	Random sampling of 20% of tickets monthly.	Below 95%: written improvement plan required. Below 90%: CAR issued. Sustained performance above 98%: positive CPARS notation.
3	Complex Provisioning SLA	Complex requests fulfilled within 3 business days of final approval.	90%	Random sampling of 20% of tickets monthly.	Below 90%: written improvement plan. Below 85%: CAR issued.
4	Chargeback Accuracy	Cost allocation accuracy to VA organizational cost centers.	98%	Monthly reconciliation audit comparing chargeback reports to CSP invoices.	Below 98%: root cause analysis and remediation within 10 business days. Below 95%: CAR issued and chargeback process review.
5	Credit Procurement Cycle Time	40% reduction from baseline established during transition-in.	40% reduction	Quarterly cycle time analysis comparing	Below 30% reduction: improvement plan. Exceeding 50%

#	Performance Objective	Performance Standard	AQL	Surveillance Method	Incentive / Disincentive
				current vs. baseline.	reduction: positive CPARS notation.
6	Security Incident Response	Initial response within 15 minutes for Priority 1 security events.	100%	Incident log review; automated timestamp verification.	Any missed P1 SLA: immediate CAR. Pattern of missed SLAs: escalation to Contracting Officer for potential cure notice.
7	Governance Policy Compliance	Resources in compliance with governance policies across all managed CSP environments.	95%	Automated scanning reports; monthly compliance dashboard review.	Below 95%: remediation plan within 5 business days. Below 90%: CAR issued.
8	Tagging Compliance	Resources tagged per approved taxonomy across all managed environments.	98%	Automated tagging compliance reports; monthly audit.	Below 98%: improvement plan with 30-day remediation target. Below 95%: CAR issued.
9	Cost Optimization Savings	Annual cloud spend reduction through optimization activities (RI/SP/rightsizing/waste elimination).	15% annually	Annual cost analysis comparing actual spend vs. on-demand baseline.	Below 10%: improvement plan with quarterly milestones. Exceeding 20%: positive CPARS notation.
10	Deliverable Timeliness	All CDRL deliverables submitted on or before the due date.	95%	Deliverable tracking log maintained by COR.	Below 95%: written explanation required. Below 90%: CAR issued. Pattern of late deliverables: negative CPARS entry.
11	Transition Milestones	All transition milestones completed per approved schedule.	100%	Milestone tracking against approved transition plan.	Missed milestone: CAR with 10-business-day remediation timeline. Multiple missed milestones: escalation to CO.

#	Performance Objective	Performance Standard	AQL	Surveillance Method	Incentive / Disincentive
12	Customer Satisfaction	Satisfaction rating from VA stakeholders on service quality, responsiveness, and professionalism.	4.0 / 5.0	Quarterly survey of VA cost center managers and ECSO stakeholders.	Below 3.5: improvement plan with COR review. Below 3.0: CAR issued. Above 4.5: positive CPARS notation.

3.3 Surveillance Methods

The COR shall employ the following surveillance methods to assess Contractor performance:

1. **Direct Observation:** COR or designee directly observes Contractor operations, processes, and service delivery during site visits and operational reviews.
2. **Periodic Inspection:** Scheduled and unscheduled reviews of deliverables, reports, dashboards, and operational outputs against quality standards.
3. **Validated User/Customer Complaints:** Documented complaints from VA users, validated by the COR, regarding service quality, timeliness, or professionalism.
4. **Automated Monitoring:** Continuous automated monitoring of platform availability, policy compliance, tagging compliance, and SLA adherence through platform-generated metrics and dashboards.
5. **Management Information Systems:** Review of Contractor-provided management reports, metrics, and dashboards for trend analysis and performance tracking.
6. **Third-Party Audit:** Independent assessments conducted by 3PAOs, VA OIG, or other authorized auditors to validate Contractor performance, security compliance, and financial accuracy.

3.4 Procedures

Performance surveillance shall follow the cadence outlined below:

Cadence	Activity	Participants
Monthly	COR reviews Monthly Status Report and FinOps Dashboard. Validates SLA compliance for provisioning, availability, and deliverables. Documents findings in COR performance file. Conducts monthly performance review meeting with Contractor Program Manager.	COR, Contractor PM
Quarterly	COR conducts comprehensive quarterly performance assessment. Reviews governance reports, customer satisfaction surveys, and cost optimization progress. Conducts quarterly executive briefing with ECSO leadership. Documents performance in interim CPARS assessment (if applicable).	COR, CO, ECSO Leadership, Contractor PM
Annually	CO and COR complete formal Contractor Performance Assessment Report in CPARS. Annual security assessment review. Cost optimization savings analysis against annual target. Contract option year exercise recommendation based on performance.	CO, COR, ECSO Director, Contractor PM

All performance assessments shall be documented and maintained in the official contract file. The Contractor shall be afforded the opportunity to respond to any performance deficiency findings in accordance with FAR 42.15 and CPARS procedures.

3.5 Remediation Process

When performance falls below AQL thresholds, the following escalation and remediation process shall be followed:

1. **Verbal Notification:** COR provides initial verbal notification to Contractor Program Manager identifying the performance deficiency and requesting immediate corrective action.
2. **Corrective Action Request (CAR):** For sustained or significant deficiencies, the COR issues a formal written CAR. The Contractor shall respond within ten (10) business days with a root cause analysis and corrective action plan, including milestones and completion dates.
3. **COR Escalation to CO:** If the Contractor fails to adequately address the CAR, or if deficiencies persist, the COR escalates the issue to the Contracting Officer with supporting documentation and a recommendation for further action.
4. **Cure Notice:** The CO may issue a Cure Notice per FAR 52.249-8, giving the Contractor ten (10) calendar days to cure the deficiency. The cure notice shall specify the exact nature of the failure and the actions required.

5. **Show Cause:** If the deficiency is not cured, the CO may issue a Show Cause Notice requiring the Contractor to demonstrate why the contract should not be terminated for default. The Contractor shall respond within ten (10) calendar days.
6. **Termination for Default:** The CO retains the right to terminate the contract for default in accordance with FAR 52.249-8 if the Contractor fails to perform at acceptable quality levels and remediation efforts are unsuccessful.

SECTION 4: INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

4.1 General Instructions

This Request for Information (RFI) is issued pursuant to FAR 15.201, *Exchanges with Industry Before Receipt of Proposals*, for market research purposes only. Interested parties are invited to submit written responses providing information on their capabilities, experience, and recommendations related to the VA Enterprise Cloud Brokerage Service described in this document.

Responses to this RFI are entirely voluntary. Responses will not be evaluated for contract award, and no contract, agreement, or obligation will result from this RFI or any response thereto. No solicitation exists at this time, and the Government makes no commitment to issue a solicitation based on this RFI.

Proprietary information included in responses shall be protected in accordance with FAR 15.207, *Handling Proposals and Information*. Respondents should clearly mark any proprietary, confidential, or trade secret information with the appropriate restrictive legend on each page containing such information. Unmarked information will be treated as non-proprietary and may be used by the Government without restriction.

4.2 RFI Response Format

Respondents shall adhere to the following formatting requirements:

Requirement	Specification
Maximum Page Count	40 pages (excluding cover page, table of contents, resumes, and past performance reference forms).
Font	Times New Roman, 12-point. Charts, tables, and figures may use 10-point font minimum.
Margins	1-inch margins on all sides.
Spacing	Single-spaced.
Page Numbering	All pages sequentially numbered in the footer (Page X of Y).
File Format	Adobe Portable Document Format (PDF). Microsoft Office attachments (Word, Excel, PowerPoint) are acceptable as supplementary materials only.
Maximum File Size	25 MB per submission. If the total submission exceeds 25 MB, respondents may submit multiple emails clearly labeled (e.g., "Part 1 of 2").
Paper Size	8.5 x 11 inches (US Letter).

4.3 RFI Response Content Structure

Respondents shall organize their submissions into the following volumes:

Volume I: Technical Capability (Maximum 20 pages)

- Describe the proposed Cloud Brokerage Platform architecture, including technology stack, deployment model, and multi-tenant capabilities.
- Detail the multi-CSP management approach, including supported CSPs and integration methodology.
- Describe automation capabilities for intake-to-provisioning workflows, automated requestor workflow automations, IaC frameworks and approval engine.
- Outline the governance framework, including policy-as-code approach, tagging enforcement, and drift detection.
- Describe the security approach, including FedRAMP authorization status, compliance monitoring, and incident response.
- Detail integration methodology with enterprise platforms (ServiceNow, SailPoint/Okta, Splunk, Active Directory).

- Describe FinOps capabilities, including chargeback/showback, anomaly detection, and optimization analytics.

Volume II: Management Approach (Maximum 10 pages)

- Describe the organizational structure, including key personnel roles, qualifications, and reporting relationships.
- Detail the transition approach, including phasing, risk mitigation, and parallel operations methodology.
- Describe the quality management methodology and continuous improvement framework.
- Outline the staffing plan, including recruitment, retention, and personnel development strategies.
- Describe the risk management approach for identifying, assessing, and mitigating project and operational risks.

Volume III: Past Performance (Maximum 5 pages)

- Describe up to three (3) relevant past performance references involving cloud brokerage, multi-CSP management, or federal cloud services of similar scope and complexity within the past five (5) years.
- For each reference, provide: contract number, contracting agency, period of performance, contract value, brief description of work performed, relevance to this requirement, and customer point of contact (name, title, email, phone).
- If available, include CPARS ratings or customer letters of commendation.

Volume IV: Market Research Questionnaire (Maximum 5 pages)

- Complete responses to all market research questions presented in Section 5 of this document.
- Responses should be concise and directly address each question with specific, factual information.

4.4 Submission Instructions

Item	Detail
Submission Method	Email to: Lauren Sankar@va.gov and John.Fields3@va.gov
Subject Line Format	"RFI 36C10B26Q0492 - [Company Name] - VA Cloud Brokerage Service"
Response Due Date	June 22, 2026
Questions Due Date	June 10, 2026 9 AM EST. All questions regarding this RFI must be submitted in writing via email to the Contract Specialist and Contracting Officer.
Oral Presentations	The Government may request oral presentations and/or capability demonstrations from selected respondents following initial review of written responses. Oral presentations, if requested, shall not exceed 90 minutes, including a question-and-answer period.
Teaming Arrangements	Respondents planning to team or subcontract for significant portions of the work should identify team members and their respective roles in the response.

4.5 Points of Contact

Role	Name	Email
Contracting Officer	John Fields	John.Fields3@va.gov
Contract Specialist	Lauren Sankar	Lauren.Sankar@va.gov

All communications regarding this RFI shall be directed to the Contracting Officer and Contract Specialist. Direct communication with the COR, technical evaluation team members, or program office personnel regarding this RFI is prohibited and may result in the respondent's submission being excluded from consideration.

4.6 Important Notices

1. **No Cost Reimbursement:** This RFI does not commit the Government to pay any costs incurred in the preparation or submission of responses. All costs associated with responding to this RFI shall be borne solely by the respondent.

2. **Cancellation Rights:** The Government reserves the right to cancel this RFI at any time without prior notice and without obligation to any respondent.
3. **Use of Information:** Information provided in response to this RFI may be used by the Government to develop requirements, refine acquisition strategies, and inform future solicitation documents. By submitting a response, respondents consent to such use, subject to proprietary markings.
4. **No Notification of Results:** Respondents will not be notified of the results of the Government's evaluation of RFI responses. The Government is under no obligation to provide debriefs or feedback on submissions.
5. **No Solicitation:** This RFI does not constitute a solicitation, Invitation for Bid (IFB), Request for Proposal (RFP), or Request for Quotation (RFQ). No contract award will result from this RFI.
6. **No Obligation:** The Government is not obligated to issue a solicitation, award a contract, or take any other procurement action as a result of this RFI.
7. **Future Solicitation:** If a future solicitation is issued, a notice will be published under the solicitation number and NAICS code identified on the cover page of this RFI, or an updated number as appropriate
8. **Small Business Participation:** The Government encourages responses from small businesses, including service-disabled veteran-owned small businesses (SDVOSB), veteran-owned small businesses (VOSB), women-owned small businesses (WOSB), HUBZone small businesses, and 8(a) firms. Respondents should indicate their applicable socioeconomic status.
9. **RFI – Loopback.** After responses to the posted RFI have been reviewed, a notice will be posted on the same platform as the original RFI to inform potential vendors of the intended outcome/strategy.

SECTION 5: MARKET RESEARCH QUESTIONS

Respondents are requested to address all questions below. Responses should be specific, concise, and based on existing or demonstrated capabilities. Where questions reference quantitative data, respondents should provide measurable evidence wherever possible. Please provide the following information by 9 AM EST on June 22, 2026 via email to Lauren Sankar, Contract Specialist, at lauren.sankar@va.gov and John Fields, Contracting Officer, at john.fields3@va.gov.

Please provide the following in your response:

- Vendor name and POC information
- SAM Unique Entity ID
- Business size standard under NAICS Code 518210 (Large, Small, SDVOSB, WOSB, etc.)
- List any federal contracts in which you are a prime contract holder, and this effort is withinscope of, for example: GSA, NASA SEWP, ETC.

Category A: Cloud Brokerage Platform Capabilities

Question 1. Describe your Cloud Brokerage Platform's architecture, including multi-tenant capabilities, underlying technology stack, API framework, and the list of Cloud Service Providers currently supported. Identify whether the platform is proprietary, commercial off-the-shelf (COTS), or a hybrid of COTS and custom components.

Question 2. How does your platform handle credit procurement and commitment management across multiple CSPs simultaneously? Describe the workflow for procuring, allocating, tracking, and reconciling cloud credits across AWS, Azure, OCI, and other CSPs within a single management plane.

Question 3. Describe your platform's chargeback and showback capabilities, including the granularity of cost allocation (e.g., account, resource, tag, custom dimension), integration with enterprise financial systems (e.g., SAP, Oracle Financials), and the methodology for allocating shared costs.

Question 4. What automation capabilities does your platform provide for intake-to-provisioning workflows? What percentage of standard cloud resource requests can be fully automated (zero-touch) from submission through provisioning? Describe the IaC frameworks supported and the approval workflow engine.

Question 5. How does your platform enforce governance policies (tagging standards, guardrails, approved services, regional restrictions) across heterogeneous CSP environments? Describe the

policy-as-code frameworks supported and the mechanism for automated remediation of non-compliant resources.

Question 6. Describe your platform's FinOps capabilities, including cost optimization recommendations (RI/SP/rightsizing/waste elimination), anomaly detection methodology, and forecasting accuracy. What measurable cost savings have you achieved for customers of comparable scale (500+ applications)?

Would a broker be subject to the same constraints as VA when we initiate RIs and Savings Plans? Example - CSPs offer "No Upfront" payment terms for Reserved Instances? Does a broker have the ability to purchase the different types of RI's and Savings Plans (1yr / 3yr / All up front / Pay as you go) or what constraints would a broker have?

Question 7. What integration capabilities exist for ITSM platforms (ServiceNow), IAM solutions (SailPoint/Okta), and SIEM platforms (Splunk)? Describe the integration methodology (API, connector, custom), data flow, and any limitations.

Question 8. Does your platform support workload portability analysis and migration planning between CSPs? Describe the methodology for assessing application portability, estimating migration effort, and recommending optimal CSP placement based on cost, performance, and compliance factors.

Category B: Security and Compliance

Question 9. What is your platform's current FedRAMP authorization status? If the platform holds a FedRAMP authorization, identify the authorization level (Low, Moderate, High), the authorizing agency, and the authorization date. If not yet FedRAMP High authorized, provide a detailed timeline to achieve FedRAMP High authorization, including current progress against the authorization process.

Question 10. Describe how your platform supports continuous ATO (cATO) processes, including automated evidence collection for NIST SP 800-53 Rev. 5 controls, continuous compliance monitoring, and integration with GRC platforms. How many NIST 800-53 controls can your platform automatically assess?

Question 11. How do you ensure data sovereignty and VA data protection requirements across multiple CSP environments? Describe controls for data residency enforcement, encryption key management, data classification, and data loss prevention.

Question 12. Describe your security incident response capabilities and integration with federal SOC operations. Include response time SLAs, forensic capabilities, escalation procedures, and experience coordinating with US-CERT and federal law enforcement.

Question 13. How does your platform address supply chain risk management per NIST SP 800-161? Describe your software bill of materials (SBOM) practices, third-party component vetting, and secure software development lifecycle.

Category C: Pricing and Commercial Models

Question 14. Describe your pricing model for Cloud Brokerage Services (e.g., subscription-based, consumption-based, percentage of managed spend, hybrid). How do you ensure cost transparency, and what is the typical total cost of brokerage services as a percentage of managed cloud spend?

Question 15. What enterprise discount programs, volume commitments, or strategic pricing arrangements can you facilitate across CSPs? Describe your negotiating leverage with major CSPs and any existing strategic partner agreements.

Question 16. How do you handle appropriation alignment and fiscal year boundary management for cloud credits and commitments? Describe your approach to ensuring compliance with the Bona Fide Needs Rule (31 U.S.C. § 1502) and Anti-Deficiency Act requirements in a cloud consumption model.

Question 17. What is your approach to cost optimization, and what measurable savings have you achieved for customers of similar scale (700+ applications, $50M+ annual cloud spend)? Provide specific metrics and case studies where possible.

Question 18. How do you handle CSP marketplace procurement limitations and ensure compliance with federal acquisition regulations (FAR/DFARS) when procuring cloud services and third-party marketplace offerings?

Category D: Transition and Operations

Question 19. Describe your approach to transitioning an enterprise of 700+ applications from existing cloud management processes to your brokerage platform. What is your methodology for minimizing disruption to ongoing operations during transition?

Question 20. What is your recommended timeline for achieving full operational capability? Describe your phasing approach, key milestones, critical path items, and dependencies on Government actions or third-party integrations.

Question 21. Describe your staffing model, including key personnel roles, clearance requirements, and your approach to personnel retention. What is your historical annual turnover rate for cloud brokerage engagements of similar scope?

Question 22. How do you handle knowledge transfer to ensure the Government retains institutional knowledge throughout the contract and is positioned for successful transition at contract conclusion? Describe your approach to building organic Government capability.

Question 23. What SLAs do you propose for platform availability, incident response (by priority level), and service request fulfillment? How do these SLAs compare to industry benchmarks for federal cloud brokerage services?

Category E: Innovation and Future State

Question 24. How does your platform incorporate artificial intelligence and machine learning for cost optimization, workload placement, predictive analytics, and autonomous remediation? Describe specific AI/ML use cases currently in production versus on your roadmap.

Question 25. How do you accommodate emerging CSPs and new cloud services (e.g., IBM Cloud, additional sovereign cloud providers) without requiring major contract modifications or significant platform re-engineering?

Question 26. Describe your platform's technology roadmap for the next three to five years, particularly regarding multi-cloud governance maturity, FinOps capabilities, AI-driven automation, and alignment with evolving federal mandates (e.g., zero trust, software supply chain security).

Question 27. What recommendations do you have for structuring a long-term cloud brokerage contract (5+ years) to maintain competitiveness, encourage innovation, and ensure the Government benefits from market evolution and emerging capabilities? Consider contract type, incentive structures, and technology refresh mechanisms.

SECTION 6: ATTACHMENTS AND EXHIBITS

Attachment 6-1: Acronym and Definition List

Acronym	Definition
3PAO	Third-Party Assessment Organization
AES	Advanced Encryption Standard
API	Application Programming Interface
ARM	Azure Resource Manager
ATO	Authority to Operate
AWS	Amazon Web Services
Azure	Microsoft Azure Cloud Computing Platform
CAR	Corrective Action Request
cATO	Continuous Authority to Operate
CDM	Continuous Diagnostics and Mitigation
CDRL	Contract Data Requirements List
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CO	Contracting Officer
CONUS	Continental United States
COR	Contracting Officer's Representative
CPARS	Contractor Performance Assessment Reporting System
CSA	Cloud Security Alliance
CSOC	Cybersecurity Operations Center
CSP	Cloud Service Provider
CUD	Committed Use Discount
CUI	Controlled Unclassified Information
DCSA	Defense Counterintelligence and Security Agency
DLP	Data Loss Prevention
ECSO	Enterprise Cloud Solutions Office
EDP	Enterprise Discount Program
EO	Executive Order

Acronym	Definition
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FinOps	Financial Operations (Cloud Financial Management)
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
FTR	Federal Travel Regulation
GAO	Government Accountability Office
GCP	Google Cloud Platform
GFE	Government-Furnished Equipment
GFI	Government-Furnished Information
GFP	Government-Furnished Property
GRC	Governance, Risk, and Compliance
HIPAA	Health Insurance Portability and Accountability Act
HSM	Hardware Security Module
HSPD	Homeland Security Presidential Directive
IaC	Infrastructure as Code
IAM	Identity and Access Management
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
MFA	Multi-Factor Authentication
NAICS	North American Industry Classification System
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
NSOC	Network Security Operations Center
OCI	Oracle Cloud Infrastructure
OIDC	OpenID Connect
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OPA	Open Policy Agent
ORM	Oracle Resource Manager
OSLE	Office of Security and Law Enforcement

Acronym	Definition
OU	Organizational Unit
PAM	Privileged Access Management
PHI	Protected Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
PSAC	Personnel Security Adjudication Center
PSC	Product and Service Code
QASP	Quality Assurance Surveillance Plan
RBAC	Role-Based Access Control
RFI	Request for Information
RFP	Request for Proposal
RFQ	Request for Quotation
RI	Reserved Instance
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SBOM	Software Bill of Materials
SCP	Service Control Policy
SDLC	Software Development Lifecycle
SDVOSB	Service-Disabled Veteran-Owned Small Business
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center / System and Organization Controls
SOO	Statement of Objectives
SOP	Standard Operating Procedure
SP	Savings Plan
TAC	Technology Acquisition Center
TIC	Trusted Internet Connections
TLS	Transport Layer Security
US-CERT	United States Computer Emergency Readiness Team
VA	Department of Veterans Affairs
VAAR	VA Acquisition Regulation

Acronym	Definition
VACO	VA Central Office
VAEC	VA Enterprise Cloud
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VOSB	Veteran-Owned Small Business
VPAT	Voluntary Product Accessibility Template
WCAG	Web Content Accessibility Guidelines
WOSB	Women-Owned Small Business

Attachment 6-2: Service Level Agreement (SLA) Matrix

SLA Category	Metric	Target	Measurement Method	Reporting Frequency	Consequence for Non-Compliance
Platform Uptime	Monthly availability percentage	99.9%	Automated monitoring tools; monthly logs	Monthly	Service credit: 2% of monthly invoice per 0.1% below threshold. Below 99.5%: CAR issued.
Standard Provisioning	Time from final approval to resource availability	≤ 4 business hours	Ticket timestamps in ServiceNow	Monthly	Below 95% compliance: improvement plan. Below 90%: CAR issued.
Complex Provisioning	Time from final approval to resource availability	≤ 3 business days	Ticket timestamps in ServiceNow	Monthly	Below 90% compliance: improvement plan. Below 85%: CAR issued.
Incident Response - P1 (Critical)	Time to initial acknowledgement and triage	≤ 15 minutes	Incident management system timestamps	Per incident	Any missed P1 SLA: immediate CAR. Pattern: escalation to CO.
Incident Response - P2 (High)	Time to initial acknowledgement and triage	≤ 30 minutes	Incident management system timestamps	Per incident	Below 95% compliance: CAR issued.
Incident Response -	Time to initial acknowledgement	≤ 2 business hours	Incident management	Monthly	Below 90% compliance:

SLA Category	Metric	Target	Measurement Method	Reporting Frequency	Consequence for Non-Compliance
P3 (Medium)			system timestamps		improvement plan required.
Incident Response - P4 (Low)	Time to initial acknowledgement	≤ 1 business day	Incident management system timestamps	Monthly	Below 90% compliance: improvement plan required.
Chargeback Report Delivery	Monthly chargeback report delivery date	By 10th business day	Report submission timestamp	Monthly	Late delivery: written explanation. Pattern: CAR issued.
Change Request Processing	Time to evaluate and schedule standard changes	≤ 2 business days	Change management system timestamps	Monthly	Below 90% compliance: improvement plan required.
Security Scan Completion	Weekly vulnerability scan execution across all managed environments	100% coverage weekly	Scan reports and coverage metrics	Weekly	Missed scan: immediate remediation and root cause report within 24 hours.
Monthly Report Delivery	All recurring monthly deliverables on time	95% on-time	Deliverable tracking log	Monthly	Below 95%: written explanation. Below 90%: CAR issued.
Tagging Compliance	Percentage of resources with all mandatory tags	98%	Automated tagging compliance reports	Monthly	Below 98%: 30-day remediation target. Below 95%: CAR issued.

Attachment 6-3: Labor Category Descriptions

1. Program Manager

Attribute	Requirement
Minimum Education	Master's degree in Business Administration, Information Technology, Computer Science, or related field.
Minimum Experience	Ten (10) years of progressive IT program management experience, including a minimum of five (5) years managing cloud services contracts of $20M+ annual value.
Key Responsibilities	Overall contract performance accountability. Client relationship management with ECSO leadership and COR. Resource allocation, risk management, and strategic planning. Financial management and reporting. Quality assurance and CPARS performance oversight.

Attribute	Requirement
Required Certifications	Project Management Professional (PMP). ITIL v4 Foundation or higher.
Key Personnel	Yes

2. Cloud Solutions Architect

At least two (2) of the following: AWS Solutions Architect Professional, Azure Solutions Architect Expert, Oracle Cloud Infrastructure Architect Professional, Google Cloud Professional Cloud Architect.

Attribute	Requirement
Minimum Education	Bachelor's degree in Computer Science, Information Technology, Engineering, or related field.
Minimum Experience	Eight (8) years of cloud architecture experience, including a minimum of three (3) years in multi-CSP enterprise environments (500+ applications).
Key Responsibilities	Enterprise cloud architecture design and optimization. Multi-CSP integration strategy and technical roadmap. Landing zone architecture and IaC framework design. Technical leadership for platform deployment and evolution. Workload portability and migration architecture.
Required Certifications	
Key Personnel	Yes

3. FinOps Lead

Attribute	Requirement
Minimum Education	Bachelor's degree in Finance, Business, Information Technology, or related field.
Minimum Experience	Seven (7) years of IT financial management experience, including a minimum of four (4) years in cloud financial operations (FinOps) managing $30M+ annual cloud spend.
Key Responsibilities	Cloud financial management strategy and execution. Chargeback/showback implementation and reporting. Cost optimization program management

Attribute	Requirement
	(RI/SP/rightsizing). Budget forecasting, anomaly detection, and spend trend analysis. FinOps maturity advancement and stakeholder education.
Required Certifications	FinOps Certified Practitioner (FOCP). Cloud cost management certification from at least one CSP (e.g., AWS Cloud Financial Management).
Key Personnel	Yes

4. Cloud Security Engineer

Attribute	Requirement
Minimum Education	Bachelor's degree in Cybersecurity, Computer Science, Information Technology, or related field.
Minimum Experience	Six (6) years of cybersecurity experience, including a minimum of three (3) years in cloud security engineering within FedRAMP High or equivalent environments.
Key Responsibilities	Cloud security architecture and controls implementation. FedRAMP compliance and ATO maintenance. Security integration with VA SOC, CDM, and enterprise security tools. Vulnerability management, incident response coordination, and forensic support. Security policy-as-code development and enforcement.
Required Certifications	CISSP (Certified Information Systems Security Professional) or CCSP (Certified Cloud Security Professional). At least one CSP-specific security certification (e.g., AWS Security Specialty, Azure Security Engineer Associate).
Key Personnel	Yes

5. Cloud Governance Analyst

Attribute	Requirement
Minimum Education	Bachelor's degree in Information Technology, Business, or related field.
Minimum Experience	Five (5) years of IT governance experience, including a minimum of two (2) years in cloud governance, policy management, and compliance monitoring.
Key Responsibilities	Cloud governance policy development and enforcement. Tagging taxonomy management and compliance monitoring. Compliance reporting and audit support. Drift detection management and remediation tracking. Governance documentation and process improvement.
Required Certifications	At least one cloud certification (AWS Certified Cloud Practitioner, Azure Fundamentals, or equivalent). ITIL v4 Foundation.
Key Personnel	No

6. DevOps/Automation Engineer

Attribute	Requirement
Minimum Education	Bachelor's degree in Computer Science, Software Engineering, or related field.
Minimum Experience	Five (5) years of DevOps and automation experience, including a minimum of three (3) years working with IaC tools and CI/CD pipelines in cloud environments.
Key Responsibilities	IaC template development and management (Terraform, CloudFormation, Bicep). CI/CD pipeline design and automation. Automated provisioning workflow development. Platform integration development (API, webhooks, connectors). Automated testing and quality assurance for IaC templates.
Required Certifications	HashiCorp Certified: Terraform Associate (or higher). At least one CSP DevOps/Developer certification (e.g., AWS DevOps Engineer Professional, Azure DevOps Engineer Expert).
Key Personnel	No

7. ServiceNow Integration Specialist

Attribute	Requirement
Minimum Education	Bachelor's degree in Information Technology, Computer Science, or related field.
Minimum Experience	Four (4) years of ServiceNow administration and development experience, including a minimum of two (2) years integrating ServiceNow with cloud management platforms.
Key Responsibilities	ServiceNow ITSM integration design and implementation. Workflow automation and catalog item development. Service portal customization and maintenance. Reporting and dashboard development within ServiceNow. Integration troubleshooting and performance optimization.
Required Certifications	ServiceNow Certified System Administrator. ServiceNow Certified Application Developer (preferred).
Key Personnel	No

8. Cloud Financial Analyst

Attribute	Requirement
Minimum Education	Bachelor's degree in Finance, Accounting, Business Administration, or related field.
Minimum Experience	Four (4) years of financial analysis experience, including a minimum of two (2) years in cloud cost analysis, chargeback/showback, or IT financial management.
Key Responsibilities	Monthly chargeback/showback report generation and reconciliation. Invoice reconciliation and discrepancy resolution. Budget forecasting and spend

Attribute	Requirement
	analysis. Cost optimization analysis and savings tracking. Financial data quality assurance and audit support.
Required Certifications	FinOps Certified Practitioner (preferred). Advanced proficiency in data analytics tools (Excel, Power BI, Tableau).
Key Personnel	No

9. Transition Manager

Attribute	Requirement
Minimum Education	Bachelor's degree in Information Technology, Business, Project Management, or related field.
Minimum Experience	Eight (8) years of IT project/program management experience, including a minimum of three (3) years managing large-scale IT service transitions in federal or enterprise environments.
Key Responsibilities	Transition-in and transition-out planning and execution. Risk management and mitigation during transition periods. Milestone tracking, dependency management, and stakeholder communication. Knowledge transfer program design and delivery. Parallel operations coordination and cutover management.
Required Certifications	PMP (Project Management Professional) or ITIL Expert / Managing Professional.
Key Personnel	No

10. Help Desk / Service Desk Analyst

Attribute	Requirement
Minimum Education	Associate's degree in Information Technology or related field, or equivalent combination of education and experience.
Minimum Experience	Two (2) years of IT service desk or help desk experience, including familiarity with cloud computing concepts and ITSM processes.
Key Responsibilities	Tier 1 support for cloud brokerage platform users. Intake request triage, categorization, and routing. Service request status communication and customer follow-up. Knowledge base article creation and maintenance. Ticket escalation per defined procedures and SLAs.
Required Certifications	CompTIA A+ or Cloud+ (preferred). ITIL v4 Foundation (preferred).
Key Personnel	No

Attachment 6-4: Deliverables Schedule

CDRL #	Title	Description	Initial Due Date	Frequency	Distribution	Format	Approval Authority
001	Monthly Status Report	Task area progress, risks, issues, staffing, milestones.	T+30 days	Monthly	COR, CO	PDF	COR
002	Monthly FinOps Dashboard	Spend analysis, trends, optimization recs, anomalies.	T+30 days	Monthly	COR, ECSO	Web/PDF	COR
003	Quarterly Governance Report	Compliance rates, drift, remediation, governance posture.	T+90 days	Quarterly	COR, ECSO, CISO	PDF	COR
004	Annual Security Assessment	Security posture, vulnerability summary, risk assessment.	T+365 days	Annually	COR, CISO, AO	PDF	CISO
005	Transition-In Plan	Phases, milestones, resources, risks, acceptance criteria.	T+15 days	One-time	COR, CO, ECSO	PDF	COR/CO
006	Transition-Out Plan	KT plan, documentation handoff, post-transition support.	T-180 days (from contract end)	One-time	COR, CO, ECSO	PDF	COR/CO
007	Incident Reports	Root cause analysis, impact, corrective actions.	As needed	As needed	COR, CSOC	PDF	COR
008	Change Management Log	All changes: description, risk, approval, outcome.	T+7 days	Weekly	COR	Excel	COR

CDRL #	Title	Description	Initial Due Date	Frequency	Distribution	Format	Approval Authority
009	Service Catalog Updates	Additions, retirements, pricing, compliance notes.	T+30 days	Monthly	COR, ECSO	Web/PDF	COR
010	SOPs/Runbooks	Operating procedures for all recurring activities.	T+60 days	As updated	COR, VA ops staff	PDF	COR
011	Training Materials	Curricula, guides, recorded sessions for KT.	T+90 days	Quarterly	COR, VA staff	PPTX/PDF	COR
012	Executive Briefings	Performance, trends, strategic recs for leadership.	T+90, 180, & 270 days (3 per year)	Quarterly	ECSO Director, CIO	PPTX	ECSO Director
013	Cost Optimization Recommendations	Actionable recs with projected impact and plan.	T+45 days	Monthly	COR, ECSO, CFO	PDF	COR
014	Compliance Evidence Packages	Control evidence, test results for ATO assessments.	Per ATO cycle	Per ATO cycle	COR, CISO, 3PAO	PDF/Excel	CISO
015	Platform Release Notes	Updates, features, fixes, known issues per release.	Per release	Per release	COR, VA ops staff	PDF	COR

Note: "T" refers to contract start date. "T-" refers to days before contract end date.

Attachment 6-5: Government-Furnished Equipment/Information List

GFE/GFI #	Item	Description	Provided By	Delivery Timeline
GFE-01	VA TIC 3.0 Network Access	Trusted Internet Connections 3.0 compliant network connectivity between Contractor facilities and VA enterprise network, including VPN credentials and TIC-compliant routing.	VA OIT Network Operations	T+30 days
GFE-02	VAEC Environment Access - AWS	Administrative access to VA Enterprise Cloud AWS environment, including management account access, organization-level permissions, and billing console access.	ECSO Cloud Operations	T+15 days
GFE-03	VAEC Environment Access - Azure	Administrative access to VA Enterprise Cloud Azure environment, including management group access, subscription permissions, and Azure AD integration.	ECSO Cloud Operations	T+15 days
GFI-04	ServiceNow Instance Access	Developer/Administrator access to VA's ServiceNow ITSM instance for integration development, workflow configuration, and catalog management.	VA OIT Service Management	T+30 days
GFI-05	VA Active Directory Integration	Service account credentials and integration endpoints for VA Active Directory federation, including SAML/OIDC configuration specifications.	VA OIT Identity Services	T+30 days
GFE-06	VA PIV Infrastructure	Access to VA's PIV credentialing process and infrastructure for Contractor personnel requiring facility and system access.	VA COR through USAccess	T+45 days
GFI-07	VA Directive and Handbook Library	Access to current versions of all applicable VA Directives, Handbooks, and policy documents governing IT operations and security.	VA OIT Policy Office	T+5 days
GFI-08	System Architecture Documentation	Current VAEC architecture diagrams, security plans, ATO packages, network diagrams, and configuration baselines for managed environments.	ECSO Architecture Team	T+15 days
GFE-9	VA Enterprise Security Tools	Access to VA-licensed Splunk instance, vulnerability scanning	VA CSOC / CDM PMO	T+30 days

GFE/GFI #	Item	Description	Provided By	Delivery Timeline
		tools, and CDM platform connectors for integration purposes.		
GFE-10	Account Provisioning / Deprovisioning System (APDS)	Onboarding access to APDS as a Contractor Lead role. For Prime Contractor's single point of contact for onboarding.	VA COR	T+15 days

Attachment 6-6: Security Requirements Checklist

Req. #	Security Requirement	Applicable Standard	Contractor Responsibility	VA Responsibility	Verification Method
SR-01	Background Investigations	HSPD-12; VA Handbook 0710; 5 CFR 731	Submit personnel for Tier 2 background investigation. Provide required documentation and fingerprints.	Adjudicate investigations through DCSA. Provide interim access determinations as appropriate.	DCSA investigation records; personnel security files.
SR-02	PIV Credentialing	HSPD-12; FIPS 201-3	Ensure all personnel complete PIV enrollment process. Report lost/stolen PIV cards within 24 hours.	Issue and manage PIV credentials through VA credentialing office.	PIV issuance records; active credential verification.
SR-03	Security Awareness Training	VA Handbook 6500; FISMA	Ensure all personnel complete VA Privacy and Information Security Awareness training within 30 days and annually. Track and report completion.	Provide access to VA TMS (Talent Management System) for training completion.	TMS training completion records; quarterly compliance reports.
SR-04	ATO Maintenance	NIST SP 800-37; VA Handbook 6500; FedRAMP	Maintain brokerage platform ATO. Support cATO processes. Collect and submit evidence per assessment schedule.	Provide Authorizing Official. Conduct security assessments through designated 3PAO.	ATO documentation; continuous monitoring dashboards; 3PAO assessment reports.

Req. #	Security Requirement	Applicable Standard	Contractor Responsibility	VA Responsibility	Verification Method
SR-05	Vulnerability Scanning	VA Handbook 6500; NIST SP 800-53 (RA-5); BOD 22-01	Conduct weekly vulnerability scans. Remediate Critical/High within 30 days, Moderate within 90 days. Report results monthly.	Provide VA-approved scanning tools and scan policies. Review and validate scan results.	Weekly scan reports; POA&M tracking; remediation evidence.
SR-06	Encryption Standards	NIST SP 800-53 (SC-13, SC-28); FIPS 140-2	Implement AES-256 encryption at rest, TLS 1.2+ in transit. Use FIPS 140-2 Level 3 validated HSMs for key management.	Provide encryption policy guidance. Validate compliance during security assessments.	Configuration audit; encryption compliance scans; HSM certification records.
SR-07	Incident Reporting	VA Handbook 6500.2; US-CERT Federal Incident Notification Guidelines; EO 14028	Report all actual/suspected security incidents to VA NSOC within 1 hour. Provide forensic support and root cause analysis.	Operate NSOC/CSOC. Coordinate with US-CERT and law enforcement. Issue incident response directives.	Incident tickets; response timeline verification; post-incident reports.
SR-08	Audit Logging	NIST SP 800-53 (AU family); VA Handbook 6500	Enable comprehensive audit logging for all managed environments. Forward logs to VA Splunk. Retain logs per VA retention policy (minimum 1 year online, 3 years archived).	Provide Splunk infrastructure and log ingestion endpoints. Define log retention requirements.	Log aggregation verification; Splunk dashboard review; retention compliance audit.
SR-09	Access Control	NIST SP 800-53 (AC family); VA Handbook 6500	Implement RBAC with least-privilege principles. Conduct quarterly access reviews. Deprovision terminated personnel within 24 hours.	Provide IAM integration endpoints. Approve access roles and permissions. Participate in access reviews.	Access control audit; quarterly review records; deprovisioning evidence.
SR-10	Data Handling and Destruction	VA Directive 6300; NIST SP 800-88 Rev. 1; 36	Handle VA data per classification requirements. Sanitize/destroy data using NIST 800-88	Provide data classification guidance. Verify data destruction	Data handling audit; destruction certificates; media

Req. #	Security Requirement	Applicable Standard	Contractor Responsibility	VA Responsibility	Verification Method
		CFR Part 1236	methods upon contract conclusion. Certify data destruction in writing.	certifications. Audit data handling practices.	sanitization records.
SR-11	Contractor Rules of Behavior	VA Handbook 6500.6, Appendix C	Ensure all personnel sign Contractor Rules of Behavior prior to system access. Maintain signed copies. Report violations immediately.	Provide current Rules of Behavior document. Enforce consequences for violations.	Signed Rules of Behavior on file; annual re-signing confirmation.
SR-12	Supply Chain Risk Management	NIST SP 800-161; EO 14028; FAR 52.204-25	Maintain SBOM for brokerage platform. Vet third-party components. Report supply chain risks. Comply with prohibited vendor restrictions.	Provide supply chain risk guidance. Review SBOMs and risk assessments.	SBOM review; supply chain risk assessment reports; component vetting records.

- END OF DOCUMENT -