Logo

Description automatically generated

U.S. Department of State

Evolve

Draft Sample Task Order

Cloud Services

Solicitation 19AQMM22R0029

Task Order Number: [XXXXXXXXX]

Date: OCT 2022

Table of Contents

[1. General 5](#_Toc116643460)

[1.1. Background and Purpose 5](#_Toc116643461)

[1.2. Objective 6](#_Toc116643462)

[1.3. Scope of Work 6](#_Toc116643463)

[1.4. Current State 6](#_Toc116643464)

[1.4.1. Multiple Environments 6](#_Toc116643465)

[1.4.2. Cloud Coverage, Facilities and Locations 7](#_Toc116643466)

[1.4.3. Personnel 7](#_Toc116643467)

[1.4.4. Policies and Procedures 7](#_Toc116643468)

[1.4.5. Agreements and Licenses 7](#_Toc116643469)

[1.4.6. Required Languages 7](#_Toc116643470)

[1.4.7. Tools 7](#_Toc116643471)

[1.5. Contract Type 8](#_Toc116643472)

[2. Requirements 8](#_Toc116643473)

[2.1. Cloud Engineering 8](#_Toc116643474)

[2.2. Cloud Operations 10](#_Toc116643475)

[2.3. Cloud Business Function Support 11](#_Toc116643476)

[2.4. Business Analysis & Process Management Support 12](#_Toc116643477)

[2.5. Cybersecurity and Information Assurance 12](#_Toc116643478)

[2.5.1. Compliance 13](#_Toc116643479)

[2.5.2. Cloud Security 13](#_Toc116643480)

[2.5.3. Risk Management 14](#_Toc116643481)

[2.5.4. Information Assurance 14](#_Toc116643482)

[2.5.5. Identity Management 15](#_Toc116643483)

[2.6. Cross-Functional Requirements 15](#_Toc116643484)

[2.6.1. IT Compliance 16](#_Toc116643485)

[2.6.1.1. 508 Compliance 17](#_Toc116643486)

[2.6.2. Security 17](#_Toc116643487)

[2.6.2.1. Information Technology Security Plan 17](#_Toc116643488)

[2.6.2.2. Cybersecurity 17](#_Toc116643489)

[2.6.3. Disaster Recovery 20](#_Toc116643490)

[2.6.4. IaaS and PaaS True On-Demand Commercial Cloud Services 20](#_Toc116643491)

[2.6.5. IT Service Management 22](#_Toc116643492)

[2.6.6. Product and Project Management 23](#_Toc116643493)

[2.6.7. Innovation, Ideation, and Modernization 23](#_Toc116643494)

[2.6.8. Product and Project Management 24](#_Toc116643495)

[3. Special Requirements / Instructions 25](#_Toc116643496)

[3.1. Standards (e.g., 5 FAM 600) 25](#_Toc116643497)

[3.2. Government-Furnished Equipment / Information (if applicable) 25](#_Toc116643498)

[3.3. Place of Performance 25](#_Toc116643499)

[3.4. Standard Work Hours 25](#_Toc116643500)

[3.5. Period of Performance 25](#_Toc116643501)

[3.6. Security Clearance Requirements 26](#_Toc116643502)

[3.7. Non-Disclosure Agreement 26](#_Toc116643503)

[3.8. Organizational Conflict of Interest (OCI) 27](#_Toc116643504)

[3.9. Associate Contractor Agreements 27](#_Toc116643505)

[3.10. Travel 29](#_Toc116643506)

[3.11. Other Direct Costs 29](#_Toc116643507)

[3.12. Funding 29](#_Toc116643508)

[3.13. Invoice Approval 29](#_Toc116643509)

[4. Task Order Management 29](#_Toc116643510)

[4.1. Key Personnel 29](#_Toc116643511)

[4.1.1. Substitution of Key Personnel 30](#_Toc116643512)

[4.2. Task Order Kick-Off Meeting 31](#_Toc116643513)

[4.3. Task Order Deliverables 32](#_Toc116643514)

[4.4. Reports, Plan, and Meetings 33](#_Toc116643515)

[4.4.1. Work Plan 33](#_Toc116643516)

[4.4.2. Monthly Status/Progress Reports 34](#_Toc116643517)

[4.4.3. Annual Program Management Plan 34](#_Toc116643518)

[4.4.4. Monthly Cost Performance Report 34](#_Toc116643519)

[4.4.5. Monthly Master Milestone Schedule 34](#_Toc116643520)

[4.4.6. Task Order Monthly Status Reports 34](#_Toc116643521)

[4.4.7. Transition-In Plan 35](#_Toc116643522)

[4.4.8. Transition-Out Plan 35](#_Toc116643523)

[4.4.9. Project Management Plan 36](#_Toc116643524)

[5. Performance Requirements 37](#_Toc116643525)

[5.1. Quality of Reports and Deliverables 37](#_Toc116643526)

[5.1.1. Acceptance Criteria and Inspection 37](#_Toc116643527)

[5.2. Quality Control and Quality Assurance 37](#_Toc116643528)

[5.2.1. Quality Control 37](#_Toc116643529)

[5.2.2. Quality Assurance 38](#_Toc116643530)

**PERFORMANCE WORK STATEMENT**

**FOR**

**EVOLVE CLOUD SERVICES**

## General

## Background and Purpose

This Performance Work Statement (or “PWS”) sets forth the roles and responsibilities of the Parties for the Cloud Services provided under the EVOLVE IDIQ as part of the Cloud & Data Center Services Functional Category. Cloud Services are the services and activities, as further detailed in this PWS, required to deliver a wide range of services on demand by Department of State (DOS) customers and/or partners for easy, affordable access to applications and resources.

The scope of cloud services to be supported includes public cloud services and hybrid solutions across DOS's environment spanning:

* Cloud service models (IaaS, PaaS, SaaS)
* Cloud Scalability, Reliability, Availability
* Security (Controlled Unclassified Information, Secret)
* IT Collaboration Support
* Analysis, Budgeting, Reporting, and Administrative Support
* Innovation and Modernization

Cloud Services include selecting enterprise cloud services, engineering them to meet DOS requirements, obtains an Authorization to Operate (ATO), and then continually developing and releasing updates to those services.

In addition, Cloud Services support provides the following user-focused services for all DOS customers:

* Manages cloud service acquisitions, contracts, and billing, ensuring that customers have visibility into their individual costs.
* Guiding new customers through the onboarding process to enable timely access to cloud services.
* Providing administration and security monitoring of the cloud platform at the enterprise level.
* Providing service desk for cloud services during regular business days/hours and operating a Change Control Board (CCB).
* Implementing and sustaining enterprise cloud systems that provide the full range of business solutions to end users and shared service providers
  + Including creating a cloud application environment that encourages and facilitates user interaction, acceptance, and leverages DOS’s investment in existing and future enterprise cloud architectures and solutions
* Managing development, delivery, and operations of new and existing cloud services
* Managing internal business functions, solution architecture services, security compliance, monitoring, and infrastructure capabilities, application-level services, and change management synchronization
* CPMO will target specific modernization efforts through this engagement and rapidly deploy MVPs to take advantage of newly available platform tools along with pre-existing tools already deployed and adopted by The State Department.

## Objective

The objective of this Cloud Services Performance work statement (PWS) is for DOS to obtain technical expertise and scalable support to assist the Cloud PMO in achievement of the DOS Cloud Strategic Goals:

1. Power Diplomacy on the Edge
2. Achieve a Fully Enabled and Orchestrated Cloud
3. Drive Data Security & Resilience
4. Cloud Talent Management

## Scope of Work

This section and the related Service Environment Appendices describes and scopes the Cloud Services environment to be supported and complied with. These Service Environment Appendices are to be maintained by Vendor, reviewed with DOS, updated by Vendor and made available to DOS on a quarterly basis.

## Current State

## Multiple Environments

The Vendor will need to support Cloud Services across DOS's multiple cloud service models (IaaS, PaaS, SaaS), deployments (Private, Public, Community, Hybrid), security domains (Controlled Unclassified Information, Secret, Top Secret), and service providers (including but not be limited to AWS, Azure, Google Cloud Platform, and ServiceNow).

1. Scalability – Each Commercial Cloud Service Providers (CCSP) shall be both horizontally and vertically scalable to two thousand virtual instances in less than 10 minutes. It shall support hundreds of petabytes of storage, a minimum of six terabytes of storage for databases, and be able to scale across two or more data centers as a selectable option in the API or web console.
2. Reliability – Each CCSP shall provide redundancy across multiple data centers, geographically dispersed from each other, to prevent natural and man-made disasters from impacting operational status. All services shall be scaled over multiple data centers and provide for real-time automatic failover without interruption to the service the systems are supporting, should a disaster occur. Launching resources in multiple data centers shall be a selectable option within the API and web console.
3. Availability – Each CCSP shall provide a minimum availability level of 99.9% for each of their services unless otherwise stated for a particular service. And each service shall meet their commercially advertised Service Level Agreements (SLA’s). Resources launched in multiple data centers shall continue to operate and be available when one of the data centers is offline for 100% uptime redundancy.
4. Direct Access to the Console and APIs – Each CCSP shall provide for direct and unfettered access to the cloud management and configuration console and APIs by Government personnel to control all the resources and configuration within the cloud.
5. Cloudcheckr (brand name) Integration – All IaaS and PaaS clouds must be integrated with the Cloudcheckr cloud reporting tool as this is how the Government manages its cloud environments for cost, configuration management, and security compliance.
6. Third Party Messaging Service – CPMO requires a three-tiered authentication mechanism to validate and verify an end user’s identity. The authentication shall be done through the (1.) username, (2.) password, and a (3.) security code transmitted to the user via text message, email, or voicemail.

## Cloud Coverage, Facilities and Locations

Vendor will provide Cloud Services to all DOS workforce, regardless of location.

## Personnel

Vendor will be responsible for providing appropriately skilled staffing to meet the Cloud Services Roles and Responsibilities and Service Level Requirements set forth in this PWS.

## Policies and Procedures

The policies and procedures with which Vendor will provide Cloud Services are provided in Enclosure G.5 – Policies, Standards and Procedures.

## Agreements and Licenses

A list of IT Service Desk-related agreements and licenses that the Vendor is required to assume, transfer or transition is provided in Enclosure G.6 — Licenses and Contracts.

## Required Languages

#### English is the current required language. Due to the nature of the work vendor personnel must be able to communicate complex ideas and technical concepts with non-technical individuals.

## Tools

DOS currently use the following tools to support it’s cloud environment: Integrate with DOS IT Service Management processes and support the management of the cloud program:

1. ServiceNow
2. BMC Remedy
3. CloudCheckr
4. JIRA
5. GitLab
6. RedHat Ansible Tower
7. Terraform
8. Nutanix Frame
9. Box
10. UiPath
11. Salesforce

This is a sampling of tools and does not limit the ability of The Department of State to leverage additional tools that are not part of this list which could require support.

## Contract Type

This is a performance-based task order that utilizes Labor Hour Contract Line Items (CLINs).

## Requirements

Contractor shall be responsible for the following Cloud Services across the DOS's cloud service models, deployments, security domains, and service providers.

## Cloud Engineering

Cloud Engineering is the implementation and support of cloud services as defined and architected by DOS and their Cloud Architecture program. The Contractor will take responsibility of existing cloud solutions within the DOS ecosystem as well as developing new cloud services and providing oversight of the execution of design solutions and transitions.

The Contractor shall perform the following tasks/subtasks:

1. Define high level cloud strategies, service requirements and policies.
2. Provide input to the Cloud Strategy (including cloud principles and reference models) and directional guidance to the Cloud PMO.
3. Provide input to the organizational strategy for how cloud computing will be leveraged within DOS and the use cases in which the organization will derive the most business value.
4. Provide input to cloud governance, strategic cloud provider selection, and application placement.
5. Provide special studies and analyses (as necessary) related to the use of cloud services and emerging technologies and practices.
6. Select and define the cloud services to be implemented and supported.
7. Design, integrate, and deliver cloud services across hosting service models to fit requirements for security, extensibility, availability, scalability, etc.
8. Design, implement and support cloud Infrastructure and Platform services and management capabilities, to include the following:
   1. A cloud management platform, potentially integrated with on and off -premises support to manage all hosting solutions, cloud-platform-native tools, and the integration between the two
   2. Self-service cloud capabilities
   3. Automation of cloud provisioning, maintenance, and reporting processes
   4. ICAM integration
   5. Network integration
   6. Database as a Service
   7. Backup and Disaster Recovery as a Service
   8. Agile and DevSecOps toolchains to support Continuous Integration/Continuous Delivery (CI/CD) pipelines
   9. Infrastructure as Code
   10. Container based solutions
9. Implement and support cloud Software services, to include the following:
   1. The FAN (G-Suite) as an IT Shared Service
   2. SaaS collaboration and productivity tools
   3. IT Service Management tools (e.g., ServiceNow)
10. Define Business Continuity & Disaster Recovery Services strategies, requirements, policies, and plans.
11. Implement required Business Continuity (BC) & Disaster Recovery (DR) services that meet requirements for recovering DOS's systems and information assets within established recovery requirement time frames after a disaster affects DOS's use of the Services. Activities include but are not limited to:
    1. Coordinate Business Continuity & Disaster Recovery efforts across all cloud service providers, including data, backups, storage management and contingency operations, and scheduled Business Continuity & Disaster Recovery testing
    2. Initiate the BC and DR plans in the event of a situation per the established policies and procedures
    3. Develop and maintain Business Continuity & Disaster Recovery Reports
12. Provide Tier 3 support to resolve cloud-related incidents including incidents escalated to Third Parties
13. Development Platforms – Each CCSP shall provide PaaS development platforms that provide for loading code and running a workload through a managed CI/CD pipeline and all infrastructure is handled by the development and infrastructure code. This service shall support, at a minimum, .Net, Java, Ruby, Node JS, and PHP development platforms.
14. Artificial Intelligence Platforms – Each CCSP shall provide a PaaS capability that supports machine learning and artificial intelligence based on algorithms that can parse data, find patterns, and learn from that data make determinations/predictions about the world based on the data, and update settings without relying on a human to change the rules-based programming.
15. Cloud Service Monitoring (CSM) – Each CCSP shall provide a monitoring service for cloud resources and the applications run in the cloud. This service shall collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in the cloud resources. This service shall monitor all forms of cloud service resources (e.g. virtual compute, storage, network, database, containerization, etc.), application logs, and provide that data via an automated interface to external logging tools such as Splunk.

## Cloud Operations

Cloud Operations provides the day-to-day service delivery management, monitoring, and reporting required to manage the provisioning, capacity, performance, and availability of the DOS cloud ecosystem while ensuring the overall quality, efficiency, and experience of cloud services.

The Contractor shall perform the following tasks/subtasks:

1. Define cloud operations requirements and policies
2. Develop and document cloud operations procedures that meet requirements and adhere to defined policies
3. Provide ongoing IT Service Management of cloud services and hybrid solutions, including event management, incident management, and problem management across multiple environments (e.g., production, development, and test, OpenNet/ClassNet)
4. Support cloud services across functional areas will ensure coverage for 24/7 cloud operations worldwide. Supported services include but are not limited to:
   1. Cloud management platform (tools)
   2. ICAM integration
   3. Network integration
   4. Database as a Service
   5. The FAN (G-Suite) as an IT Shared Service
   6. SaaS collaboration and productivity tools
   7. Backup and Disaster Recovery as a Service
   8. Agile and DevSecOps toolchains to support Continuous Integration/Continuous Delivery (CI/CD) pipelines
   9. Infrastructure as Code
5. Integrate with the DOS Tier 1 Help Desk and ITSM platform to support IT Service Management including responding to incidents, diagnosing incidents, escalating to cloud service providers or DOS partners as required, and restoring services
6. Support end-to-end Incident identification, escalation, resolution (management) and closure of cloud-related incidents including incidents escalated to Third Parties
7. Monitor unresolved cloud-related Incidents and manage tickets via ITIL-based end to end Incident Management processes
8. Troubleshoot Incidents using the DOS Known Error Database (KEDB) and Knowledge Library and/or Third-Party knowledge databases (e.g., Application Vendor knowledge databases, if applicable)
9. Take responsibility for Incidents that have been assigned by the DOS Tier 1 Help Desk and resolve in accordance with SLAs, recommend escalation to other appropriate Tier 2 or 3 resources as required,
10. Document solutions to Resolved Incidents in DOS KEDB and Knowledge Library
11. Verify that all records (e.g., inventory, asset, and Configuration Management records) are updated to reflect completed/Resolved Service Request (e.g., IMACs) or Incidents
12. Provide authorization to the process of closing service requests and incidents
13. Conduct proactive trend analysis of Incidents and Problems, and other data elements to identify recurring situations that are or may be indicative of future Problems and points of failure
14. Support Root Cause Analysis (RCA) for all Problems that meet defined criteria, including all Priority 1 and 2 Incidents, per agreed-to procedures
15. Review and approve RCAs prior to remediation efforts
16. Remediate Problems per RCAs using defined Change Management procedures within mutually agreed timeframes (or 45 business days)
17. Review and provide authorization to close remediated Problems per RCAs
18. Support monthly Problem Management proactive review sessions
19. Document Problem Management information in DOS KEDB and Knowledge Library, including Problems, Root Cause, Known Errors, Workarounds and problem resolution actions
20. Review and approve Service Request, Incident Management, and Problem Management procedures

## Cloud Business Function Support

As the Contractor supporting the day-to-day operations of cloud services and maintaining the most frequent contact with DOS cloud customers, provide input into the business, financial, marketing and program processes to help optimize the performance and delivery of cloud solutions, cost-effective cloud operations, and innovations.

The Contractor shall perform the following tasks/subtasks:

1. Perform business, financial, and program management including invoice aggregation, chargeback, and billing; support of cloud governance processes; maintenance of business relationship with cloud customers; and standard program management office support.
2. Support cloud business, financial, and program management as required, including providing current and projected cloud usage data and trends concerning customer issues, emerging requirements, and opportunities for improvements and resource optimization.
3. Build and maintain relationships with current and potential consumers of cloud services, including program offices, vendors, mission customers, CORs/GTMs, etc. Collaboratively resolve any business or technical challenges to improve the delivery and management of cloud services.
4. Support reporting to management, GTMs, CORs and other key stakeholder groups as required, including updating Cloud PMO related activities in iSchedule and iMatrix as required.
5. Develop, collect, and maintain documentation as necessary to support effective management of cloud services, as well as project/program management. 'Documentation' includes but is not limited to: Presentations, Meeting minutes, Action items, Agreements, reports/ analysis, electronic records.
6. Enterprise Governance established for Structure and Management of Cloud Adoption to include creating a Governance Guide, target use cases, roles and responsibilities
7. Operationalize enterprise cloud governance for delivering premium, prompt and tailor-made services to customers with attention to detail to operationalize Cloud which includes cloud enabled low code no code platforms
8. Deliver Marketing program material to ensure market cloud adoption
9. Identify, list, and rank in complexity of Locally Developed Applications (LDAs) which could be maintained using leveraging the cloud or cloud enabled low code no code platform tools

## Business Analysis & Process Management Support

As the vendor supporting the day-to-day operations of cloud services and maintaining the most frequent contact with DOS cloud customers, provide services to support business analysis of capabilities and desired requirements, as well as business process engineering.

Business analysis and business process management (BPM) employs various methods to design IT/OT systems/applications and discover, model, analyze, measure, improve and optimize business processes.

The Contractor shall perform the following tasks/subtasks:

1. Design processes to support the implementation of applications/systems and business processes that will coordinate the behavior of people, systems, information, and things to produce business outcomes in support of DOS' strategic objectives.
2. Support the implementation of applications/systems and business processes that will coordinate the behavior of people, systems, information and things to produce business outcomes in support of DOS' strategic objectives.
3. Monitor and understand evolving cloud capabilities, IT infrastructure modernizations and application development trends for translation into potentially new functionality to support mission needs.
4. Implement processes that are streamlined, structured and repeatable to deliver on mission objectives and promote alignment of investments to DOS' strategy, as well as a sustainable culture of continuous improvement through automation.
5. Overcome bottlenecks to drive strategic process improvement and solve organizational issues (e.g., business process reengineering, change management efforts).
6. Provide support for the development and ongoing management of business/mission use cases for prioritizing system/application development efforts and business process improvements.
7. Collaborate with key stakeholder groups across the organization to facilitate change in behavior / processes (e.g., Change Management, Communications, Automation, Governance).

## Cybersecurity and Information Assurance

Cybersecurity and Information Assurance implements and oversees a cloud information security program which includes implementing security policies, processes and standards in coordination with DOS and/or partners, vendors for establishing a secure infrastructure and systems for DOS's environment.

## Compliance

The Contractor shall perform the following tasks/subtasks:

1. Define cloud Cybersecurity and Information Assurance requirements and policies.
2. Execution and support of compliance activities related to Federal Information Technology security mandates including but not limited to: Federal Information Security Modernization Act (FISMA), Federal Information System Control Audit Manual (FISCAM), Federal Information Technology Acquisition Reform Act (FITARA), Presidential Directives (PD) 63 and 67, Public Law 100-235, Office of Management and Budget (0MB) A-123, 0MB A-127, and 0MB A-130.
3. Provide expertise and resources to assist with meeting FEDRAMP requirements and ensuring that systems/solutions are in compliance with DOS policies/directives/guidance, OMB Circular A-130, Federal Information Security Modernization Act (FISMA), FIPS Standards, National Information Assurance Certification and Accreditation Process (NIACAP), NIST guidance and other federal laws and regulations.
4. Support the semi-annual and annual account review/recertification process and continuous monitoring activities.

## Cloud Security

The Contractor shall perform the following tasks/subtasks:

1. Provide expertise and resources to support the adoption of the DOS Enterprise Cloud Security Architecture.
2. Design, develop, implement and maintain cloud solutions to support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB). IPv6 technology, in accordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html), shall be included in all cloud infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations.
3. Design, develop, implement and maintain Cloud security solutions that are aligned with Zero Trust.
4. Establish and maintain Cloud systems configuration, operation, maintenance, and disposal pursuant to DOS guidance.
5. Provide expertise and resources to assist with Cloud Native (CNAPP) technologies to take advantage of cloud delivery model.
6. Provide expertise and resources to assist with Cloud Risk Management related to processes and practices associated with service provider policies and program.
7. Provide expertise and resources to assist with Cloud Access Security Broker (CASB), Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP).
8. Implement and maintain the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) for continuous / systematic assessment of cloud implementations to proactively provide DOS guidance on which security controls /standards/policies should be implemented by which actor within the cloud supply chain in support of securing the organization's information assets and adherence DOS's security assurance and compliance requirements.
9. Closely collaborate with key stakeholder groups (e.g., ISSO, program offices, vendor(s), partner(s)) to ensure security related functions, enterprise architectural design and cloud services are performed and meet security requirements.

## Risk Management

The Contractor shall perform the following tasks/subtasks:

1. Conduct regular reviews of DOS's risk exposure, which includes without limitation: Security audit including access rights, Quality of service delivery, Delayed service delivery, Business continuity and disaster recovery, Non-performance or inability to cloud deliver Services.
2. Maintain and track Authorities to Operate (ATOs) for new and existing solutions within the cloud ecosystem following the Assessment and Authorization (A&A)/system security authorization process.
3. Support the development and implementation of Ongoing Authorization, Continuous Monitoring, and ASA guidance and processes.

## Information Assurance

The Contractor shall perform the following tasks/subtasks:

1. Review the data and documentation for cloud solutions to ensure the quality of the information, identify any deficiencies and draft recommendations to correct the deficiencies for delivery. These recommendations shall be written and submitted to key stakeholder groups (e.g., ISSO, system owner) in accordance with standard operating procedures (SOP).
2. Coordinate across all key stakeholder groups (e.g., program offices, vendor(s), partner(s)) to develop, document and maintain technical design plans, specifications, and environment configuration based on DOS Design Specifications Services standards and requirements including IT architecture, functional, performance, Availability, maintainability, security, and Disaster Recovery requirements for cloud solutions.
3. Maintain a library of supporting documentation for accreditation/authorization packages in accordance with DOS's standard operating procedures (SOP).
4. Provide technical security oversight and management for cloud security, cryptographic services, and Information Integrity for the DOS PKI/biometric and anti-virus programs.
5. Provide security-based engineering support for cloud systems/solutions. This support shall include services such as identity (ICAM), network design and analysis, data security, automation enablement, and configuration of information systems to conform to DOS security standards.
6. Provide DOS security and privacy awareness and role-based training projects in support of cloud solutions
7. Assist in the execution of Quarterly POA&M reviews and Quarterly FISMA reviews.
8. Provide support for security reviews, Budget Data Requests, and IT Security Cost data calls.
9. Assist in the completion of asset inventory for cloud assets- ITAM (Information Technology Asset Management).

## Identity Management

Identity and Access Management Service (IAMS) – Each CCSP shall provide an IAMS that is

fully configurable by customer that integrates with customer three factor authentication systems.

This service shall support the Government three factor authentication standard.

The Contractor shall perform the following tasks/subtasks:

1. Design, develop, implement, and maintain Cloud applications and systems that provide user authentication services compliant with NIST Special Publication 800-63 and DOS IAM enterprise requirements for zero- trust based authentication. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided if they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements set forth in OMB Memora+F3nda M-04-04, M-05-24, M-11-11, National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2 and supporting NIST Special Publications.

## Cross-Functional Requirements

The following table summarizes the Cross-Functional categories that all contractors are required to support across each task order.

Cross-Functional Requirements

| Requirements Category | Description |
| --- | --- |
| IT Compliance | IT Compliance resources setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. Includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery. |
| Security | IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cyber Security & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security. |
| Disaster Recovery | IT Disaster Recovery resources setting DR Policy, establishing process and means, dedicated failover facilities, performing DR testing: NOTE: DR designated equipment is included directly in its own sub-tower (e.g., extra servers for DR are included in Compute tower, etc.). |
| IaaS and PaaS | CPMO’s objectives and architectures and provide cloud diversity |
| IT Service Management | Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier 1 help desk). |
| Product and Project Management | Resources involved with managing and supporting IT related projects and/or continuous product development (e.g., Agile) across business and IT-driven initiatives. |
| Innovation, Ideation, and Modernization | The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services.  Includes enterprise architecture solutions that enhance and modernize DOS services. |

## IT Compliance

IT Compliance resources include setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. This includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery.

The Contractor shall:

1. Comply with all relevant certification and accreditation requirements and documentation specified by DOS and the U.S. Government.
2. Adhere to policies and procedures defined in the Foreign Affairs Manual (FAM) and associated Foreign Affairs Handbooks (FAHs) to include, but not limited to proactively reporting non-compliance issues and risks.
3. Participate in compliance, risk and regulatory governing bodies, processes and activities as required.
4. Measure (or provide inputs needed to support measurement of) compliance to relevant legal and compliance requirements.
5. Monitor all work performed by assigned Contractor personnel to ensure the ongoing and continuous incorporation of and adherence to all appropriate Compliance requirements.
6. Report on compliance in coordination with other DOS stakeholders and/or Contractors.
7. Support remediation of compliance discrepancies as directed.
8. Support the definition and establishment of controls to monitor compliance.

## 508 Compliance

The Contractor shall ensure the system is compliant with Section 508 throughout the implementation and integration of the work to be performed. The Contractor shall ensure the system is compliant with all appropriate 508 requirements and lead the testing and validation for every major and minor release. In the event that a user with disabilities identifies a defect with 508 compliance the Contractor must accommodate appropriately. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C.794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency.

Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

Applicable standards are 1194.211194-26.

Implementation Instructions

* <http://www.section508.gov/content/learn/laws-and-policies>
* <http://www.access-board.gov/508.htm>
* <http://www.w3.org/WAI/Resources>

## Security

IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cyber Security & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security.

The Contractor shall:

1. Provide robust security features, including integrated certificate management and SSL termination and decryption. Centrally manage SSL settings and offload CPU intensive workloads from the applications.

## Information Technology Security Plan

In accordance with Dept of State Acquisition Regulation (DOSAR) clause 652.239-71(b), the contractor shall develop, provide, implement, and maintain an IT Security Plan.

## Cybersecurity

Cybersecurity is mandatory for all task orders placed under the Evolve contract. The objective of the cybersecurity requirement is to ensure that all task orders placed under the Evolve IDIQ not only comply with DOS standards but go above and beyond those requirements to consider how to make DOS systems more resilient and secure in the face of continuously changing threats. The following are the current cybersecurity standards, frameworks and policies that will apply at the task order level as applicable. These lists are not all inclusive and are subject to change:

1. Federal Information Processing Standards Publications

| Federal Information Processing Standards Publications (FIPS Pub) | Reference |
| --- | --- |
| Security Requirements for Cryptographic Modules | FIPS Pub 140-3 |
| Standards for Security Categorization of Federal Information and Information Systems, February 2004 | FIPS Pub 199 |
| Minimum Security Requirements for Federal Information and Information Systems, March 2016 | FIPS Pub 200 |
| Personal Identity Verification of Federal Employees and Contractors,” January 24, 2022 | FIPS Pub 201-3 |

1. National Institute of Standards and Technology Publications

| National Institute of Standards and Technology (NIST) | Reference |
| --- | --- |
| Guide for Applying the Risk Management Framework to Federal Information Systems:  A Security Life Cycle Approach, June 10, 2014 | NIST SP 800-37 |
| Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015 | NIST SP 800-53 Rev. 4 |
| A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008 | NIST SP 800-116 |
| Digital Identity Guidelines, June 2017 | NIST SP 800-63-3, 800-63A, 800-63B, 800-63C |
| Guidelines for Derived PIV Credentials, December 2014 | NIST SP 800-157 |
| Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012 | NIST SP 800-164 |
| Draft National Institute of Standards and Technology Interagency Report - Mobile, PIV, and Authentication, March 2014 | NISTIR 7981 |

1. Office of Management and Budget Publications

| Office of Management and Budget (OMB) | Reference |
| --- | --- |
| Managing Federal Information as a Strategic Resource,” July 28, 2016 | OMB Circular A-130 |
| Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011 | OMB Memorandum M-11-11 |
| Transition to IPv6, September 28, 2010 | OMB Memorandum |
| Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006 | OMB Memorandum M-06-18 |
| Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005 | OMB Memorandum 05-24 |
| Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007 | OMB Memorandum M-07-16 |
| Implementation of Trusted Internet Connections (TIC), November 20, 2007 | OMB Memorandum M-08-05 |
| Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008 | OMB Memorandum M-08-23 |
| Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents August 27, 2021 | OMB Memorandum M-21-31 |
| [Identity, Credentialing, and Access Management (ICAM)](https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf), May 2019 | OMB Memorandum M-19-17 |

1. Security Policies

| Security Policies | Reference |
| --- | --- |
| "Trusted Internet Connections (TIC) Reference Architecture Document, Federal Interagency Technical Reference Architectures, Department of Homeland Security, ([https://www.doi.gov/sites/doi.gov/files/uploads/tic\_ref\_arch\_v2-0\_2013.pdf](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.doi.gov%2Fsites%2Fdoi.gov%2Ffiles%2Fuploads%2Ftic_ref_arch_v2-0_2013.pdf&data=04%7C01%7CWeakley-LugoKF%40state.gov%7C14aea13923b646e405db08d96bae63f1%7C66cf50745afe48d1a691a12b2121f44b%7C0%7C0%7C637659219012429211%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=YbP5%2FAfsntmTWA2EUBBBFCR5F8gVqSLDiifPXpmWiWs%3D&reserved=0)) " | Version 2.0, October 1, 2013\*Version 3 in draft |
| "Trusted Internet Connections (TIC) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf" | OMB M-08-05 |
| "Domain Name System Security (NSSEC) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf" | OMB M-08-23 |
| Federal Information Security Modernization Act (FISMA) of 2014 | 44 U.S.C. § ch.35 |
| Clinger-Cohen Act of 1996 also known as the Information Technology Management Reform Act of 1996 | 40 U.S.C |
| Privacy Act of 1974 | 5 U.S.C. § 552a |
| Homeland Security Presidential Directive, “Policy for a Common Identification | HSPD-12 |
| Standard for Federal Employees and Contractors, August 27, 2004 |  |
| Management of Federal Information Resources, and Appendix III, | (OMB) Circular A-130 |
| Security of Federal Automated Information Systems”, as amended | OMB Circular A-130 | |
| E-Authentication Guidance for Federal Agencies | OMB Memo M-04-04 | |
| Standards for Security Categorization of Federal Information and Information Systems | FIPS PUB 199 | |
| Minimum Security Requirements for Federal Information and Information Systems | FIPS PUB 200 | |
| Security Requirements for Cryptographic Modules | FIPS PUB 140-3 | |
| Guide for Developing Security Plans for Federal Information Systems | NIST Special Publication 800-18 Rev 1 | |
| Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems | NIST Special Publication 800-30 | |
| Contingency Planning Guide for Information Technology Systems | NIST Special Publication 800-34 | |
| Guide for the Security Certification and Accreditation of Federal Information Systems | NIST Special Publication 800-37 | |
| Security Guide for Interconnecting Information Technology Systems | NIST Special Publication 800-47 | |
| Recommended Security Controls for Federal Information Systems | NIST Special Publication 800-53 | |
| Guide for Assessing the Security Controls in Federal Information Systems | NIST Special Publication 800-53A | |
| Voice Over Internet Protocol (VoIP) Telephony | CNSSI 5000 | |
| Voice over Secure Internet Protocol (VoSIP) | CNSSI 5000 ANNEX I | |
| Softphone Security Requirements | CNSSI 5000 ANNEX J | |
| Type-Acceptance Program for Voice Over Internet Protocol (VoIP) Telephones | CNSSI 5001 | |
| Telephony Isolation Used for Unified Communications Implementations Within Physically Protected Spaces | CNSSI 5002 | |
| National Instruction for Approved Telephone Equipment | CNSSI 5006 | |
| Telephone and Security Equipment Submission and Evaluation Procedures | CNSSI 5007 | |
| Safeguarding Communications Security (COMSEC) Facilities and Materials | CNSSI 4005 | |
| Enabling Mission Delivery through Improved Identity, Credential, and Access Management | OMB Memo M19-17 | |
| Cybersecurity Strategy and implementation Plan (CSIP) | OMB Memo M16-04 | |
| Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure | E.O 13800 | |
| Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information | E.O. 13587 | |
| Instruction for National Security Systems (NSS) Public Key Infrastructure (PKI) X.509 Certificate Policy, Under CNSS Policy No. 25 | CNSSI 1300 | |

The contractor is responsible for remaining abreast of all new mandatory cybersecurity requirements at both the federal and DOS level and complying with the requirements relevant to this task order.

In addition to being able to perform in accordance to the referenced publications as required at the Task Order level for sensitive data and information technology (IT) resources, a contractor shall ensure that the contractor's information security policies, procedures, and practices applicable to all information systems it owns or operates which contain, transmit, or process information provided by or generated for the Government to support the operations and assets of a Federal agency (“Federal Information”), and which may be reasonably contemplated to be used during the performance of this contract, meet, at a minimum, the requirements of the security control baseline for Low-Impact information systems (in the most current version of NIST Special Publication 800-53), or conform to commercial standards requirements that provide a substantially equivalent or greater level of security.

## Disaster Recovery

See Reliability Specifications for Cloud environments above in section 3.3.1

## IaaS and PaaS True On-Demand Commercial Cloud Services

To support CPMO’s objective and architectures and provide cloud diversity, the contractor shall provide three or more CCSP’s for the IaaS and PaaS offerings. All offerings must be FedRAMP Authorized and FedRAMP Impact Level moderate at a minimum; additionally, at least one offering must be FedRAMP Impact Level high. Each offering shall include all the following services:

Virtual Compute Service (VCS) –Virtual compute resources shall be configurable in real-time.

In addition, VCS’s must:

* Be able to instantiate and resize on demand without the need to rebuild the virtual instance, Provide scalable, on demand sizing to support additional load or reduction in load via programmatic scripting through an API.
* Allow the automated configuration of memory, CPU, instance storage, and the boot partition size that is optimal for the Government’s choice of operating system and application.
* The VCS shall support the latest versions of operating systems such as Red Hat Linux, Ubuntu Linux, CentOS Linux, and Microsoft Windows Server 2012 or newer. These shall be updated over the life of the IDIQ as new operating system technologies emerge and are supported by each CCSP.

Scaling Automation Service (SAS) – Each CCSP shall provide a Virtual Computer scaling

service that provides for programmatic launching and shutdown of compute instances based on

load of the instances in the compute pool. Load shall be based on an increase or decrease in

processor or memory utilization of a period to trigger the launch or shutdown action.

Database Management Services (DBMS) – Each CCSP shall provide a minimum of three

database services that do not require any management or administration on the part of the

customer for the underlying DBMS. It shall provide for automatic backups that can be

configured by the user to save the data in cloud storage for data recovery purposes in the event of

a system failure. All database configuration commands and options shall be available via the

GUI or API.

Relational Database Services (RDS) – Each CCSP shall provide a highly available relational

database service for large scalable databases without USCIS having to manage the servers or

DBMS. This service must be geographically redundant over more than 500 miles. The database

creation, modification, deletion, and management on this service must be available via API’s and

scale on demand to 20000 IOPS and 6 TB. The RDS shall provide a minimum of two of the

following databases: Oracle, MySQL, PostgreSQL, and Microsoft SQL Server.

NoSQL (NSDS) – Each CCSP shall provide a fast and flexible NoSQL database service for

applications that need consistent, single-digit millisecond latency at any scale. It shall be a fully

managed cloud database that supports both document and key-value store models. It shall provide

a flexible data model, reliable performance, and automatic scaling of throughput capacity,

providing response times from milliseconds to microseconds up to millions of requests per

second.

Data Warehouse Service (DWS) – Each CCSP shall provide a fully managed, petabyte-scale

data warehouse service in the cloud, which allows for a100GB of data to stability and the ability

to scale to a petabyte or more. This service shall allow the user to run Business Intelligence tools

against the data source to use the data to acquire new insights for the business. Complex query

datasets shall be returned within minutes using SQL based tools to analyze the data.

Storage – All storage shall be highly available and replicated automatically across multiple data

centers to prevent outages or loss of data.

Scalable Block Storage (SBS) – Each CCSP shall provide persistent high speed, low latency

block storage for the virtual compute instances that remain even when the virtual compute

instance is turned off or decommissioned. The storage shall be scalable up or down within 15

minutes of an API call or administration console change.

Highly Scalable Network Storage Service (HSNSS) – Each CCSP shall provide access to

reliable, fast, and inexpensive network data storage infrastructure. It shall provide web-scale

computing by allowing storage and retrieve any amount of data, at any time, from within CCSP

or anywhere on the web. It shall store data objects redundantly on multiple devices across

multiple facilities and allows concurrent read or write access to these data objects by many

separate clients or application threads. The redundant data stored shall be usable to recover

reliably and quickly from instance or application failures. This storage shall also allow for the

storage and recovery of machine images, snapshots, and data backups programmatically. It shall

provide for programmatic recovery from these snapshots and backups in the case of a system

failure. The data stores shall be logically organized in buckets and be accessible to the systems

that are providing permission to that data. The data shall have HTTPS URL pointers that address

the data by the logical buckets in which it is stored.

Highly Scalable (Glacial) Network Storage Service (GNSS) – Each CCSP shall provide slower

speed network storage for data that is less frequently accessed. This storage has the same

redundancy requirements as the Highly Scalable Network Storage, but with higher latency disk to provide for more cost-effective storage of long term, infrequently accessed data.

Auto-Scaling File Storage (AFS) – Each CCSP shall provide for automatic scaling File Storage

that allows the expansion and contraction of the file system as data is added to and removed from

the File Store. The file store shall be mountable by the Virtual Compute Instances and provide

file storage as needed based on the storage amount that is needed.

Server Containerization Services (SCS) – Each CCSP shall provide a highly scalable, high

performance, container management service that supports a standard container format and allows applications to easily run on a CCSP managed cluster of Virtual Computer instances.

* This service shall eliminate the need to install, operate, and scale the cluster management

infrastructure.

* The service shall, via the API, be able to launch and stop container enabled applications,
* query the complete state of the cluster, and access many features like security groups,
* Virtual Load Balancing, SBS volumes, and IAM roles.
* The system teams shall be able to schedule the placement of containers across the cluster
* service based on resource needs and availability requirements.
* This service shall support third-party schedulers to meet business or application specific
* requirements.

## IT Service Management

The contractor shall provide a SaaS Service Desk Management service that supports Asset Management, customizable ticketing workflows, knowledge base management, smartphone apps for the user, web-based user portal, customizable, user role-based permissions that integrate with the Department of State Active Directory Services, and integration with the Microsoft Exchange email system.

## Product and Project Management

Resources involved with managing and supporting IT related projects and/or continuous product development (e.g., Agile) across business and IT-driven initiatives.

The Contractor shall:

1. Support the Cloud PMO’s Product Management approach for conceiving, defining, delivering, monitoring, and refining products to maximize mission results.
2. Support the Cloud PMO in performing Product Management-related tasks including but not limited to: researching markets and customers; analyzing customers and products; and developing and maintaining a product vision and roadmap.
3. Support the Cloud PMO in working with product delivery teams to test and prioritize delivery of product capabilities in order to maximize customer value and mission impact and derive growth from digital initiatives.
4. Provide subject matter expertise to support project execution across any of the in-scope IT services as required.
5. Provide cloud infrastructure and IT systems in support for project execution across any of the in-scope IT services as required.

## Innovation, Ideation, and Modernization

The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services.  Includes enterprise architecture solutions that enhance and modernize DOS services.

The Contractor shall:

* Support the program by providing CPMO with special studies and analyses, expert services, innovation, modernization and management analyses.
* Work collaboratively and cross functionally with engineering and operations to implement continuous integration, continuous delivery, production monitoring, and production support.
* Review, experiment with, and potentially adopt different technologies, tools, practices, processes, and techniques to drive innovation and facilitate continuous delivery, continuous feedback, continuous improvement, and encourage rapid and flexible response to change.
* Use industry best practices such as Lean Product Management, User-Center Design, and Extreme Programming (XP) to deliver innovative, cost-effective, high-quality, and rapid solutions that range from niche native mobile capabilities to enterprise capabilities.
* Provide capability for The State Department to invest in advanced forms of analytics to leverage big data and find new business intelligence discoveries. Implement self-service models and data visualization for next generation business analytics and business intelligence. Make advanced data discovery accessible to business users irrespective of their technical knowledge and skills.
* Capitalize on advances in AI and ML creating intelligent data models and automated analytics. Make acquiring new data easy, so it can be available for data science & quick analysis.
* Participate in integrated program and project teams and DevSecOps teams to enhance communication, share lessons learned and facilitate rapid identification of dependencies between various functional entities to ensure that the projects deliver the right solutions and value to the business and end-users. This collaboration may include providing recommendations to the government staff as the government attempts to stand up or execute an agile project.
* Work with the product owner, product manager end users and requirements analysts to refine and groom user stories.
* Work with the product owner, product manager and agile resources to design application solutions to include user research, experience design, and service design.
* Create and maintain an automated test suite for the purposes of performing automated testing on user stories and for ongoing regression testing to ensure functionality and quality of the overall system. This includes but is not limited to testing methodologies, such as Behavior Driven Development (BDD), Test Driven Development (TDD), and Acceptance Test Driven Development (ATDD). The contractors will work with the DevOps and Testing Services (DOTs) contractors for additional testing to include 508.
* The Contractor shall participate in working groups or panels, as determined by the Program Manager.  This may include providing support to other IRM offices, as directed.

## Product and Project Management

Resources involved with managing and supporting IT related projects and/or continuous product development (e.g., Agile) across business and IT-driven initiatives.

The Contractor shall:

1. Support the Cloud PMO’s Product Management approach for conceiving, defining, delivering, monitoring, and refining products to maximize mission results.
2. Support the Cloud PMO in performing Product Management-related tasks including but not limited to: researching markets and customers; analyzing customers and products; and developing and maintaining a product vision and roadmap.
3. Support the Cloud PMO in working with product delivery teams to test and prioritize delivery of product capabilities in order to maximize customer value and mission impact and derive growth from digital initiatives.
4. Provide subject matter expertise to support project execution across any of the in-scope IT services as required.
5. Provide cloud infrastructure and IT systems in support for project execution across any of the in-scope IT services as required.

## Special Requirements / Instructions

## Standards (e.g., 5 FAM 600)

The Contractor shall ensure that all work is completed in accordance with US Government and Department of State standards, policies, procedures and guidelines as provided.

## Government-Furnished Equipment / Information (if applicable)

The Government may furnish workspace and other appropriate furnishings, computer hardware and software, telephones and other material appropriate to the performance of tasks. All computer resources in use at the U.S. Government facility will be Government furnished.

Any Government furnished materials, data, or property shall remain the property of the Government and will be returned upon completion of the support services. Government furnished equipment shall be tracked through applicable procedures that will be provided by the Contracting Officer in accordance with the Federal Acquisition Regulation (FAR).

## Place of Performance

Work under this task order shall be performed primarily at DoS facilities in the Washington, DC metropolitan area, including primarily State Annex (SA-34) at 7374 Boston Blvd., Springfield, VA 22153, the Harry S. Truman Building and other State Annexes in the Washington, DC area. Additional support may be required at the State Annex 26 in Beltsville, MD and/or the ESOC West Data Center in Denver, Colorado and SA-20 – Rosslyn.

The Government authorizes offeror personnel to telework for the performance of their work functions. If telework or remote work is contemplated for the performance of tasks in this PWS, it shall be conducted per Government telework policies and be authorized by the COR or the CO

## Standard Work Hours

The Department of State normal work hours are 8:15 a.m. to 5:00 p.m., Monday through Friday. Contractor personnel are to be available both during normal working hours and as required for after-hours on-call support, when approved in advance by the GTM.

Unless other hours are specified in the task order, hours of performance on the contract will be an 8-hour workday, excluding lunch, but start times may vary depending on the task assignment. The Contractor will be required to cover the core hours from 0900 to 1500, Monday through Friday. During times of emergency and under unusual conditions, i.e. declared emergencies, civil unrest etc., the Contractor shall be prepared for 24-hour performance.

## Period of Performance

This task order comprises of a one-year base period of performance, with up to four, one-year option periods.

Base Year: Beginning and End Dates to be inserted at IDIQ award

Option Year 1:

Option Year 2

Option Year 3:

Option Year 4:

## Security Clearance Requirements

Contractor personnel assigned to this contract shall possess up to a TOP SECRET with Special Compartmented Information (SCI) personnel security clearance issued by the Defense Counterintelligence and Security Agency (DCSA) commensurate with the level of access required, prior to contract performance. All Contractor personnel supporting this contract will possess at least the minimum-personnel security clearance issued by the Defense Security Service commensurate with the level of access required and as specified in the DD Form 254, prior to contract performance, unless otherwise notified.

Security clearance requirements for contractors accessing DoS information systems shall be in accordance with Volume 12, Foreign Affairs Manual, Section 600. Furthermore, while at DoS locations, the Contractor shall comply with applicable DoS regulations relative to the protection of classified and/or sensitive information. The Office of Information Security (DS/IS/ISP/INB) is responsible for inspecting the Contractor’s activities with at Department locations.

Contractor personnel shall meet the personnel security clearance requirements identified in the DD-254 and task order/s. Most contractor personnel supporting the contract are expected to have a SECRET level security clearance, at a minimum. Additional security clearance requirements may be stipulated by the GTM. The prime or, in the case of a joint venture (JV), the owners of the JV (all primes) must have a TOP SECRET facility clearance by the date of the proposal submission, or it will be considered non-compliant. Subcontractors do need a cleared facility based on the highest-level clearance of their employees.

Visit requests are to be sent to DS/IS/ISP/INB, SA-20, 13th floor, Rosslyn, Virginia 22209. Letters of Consent issued by the Defense Security Service must be attached to all Visit Authorization Requests (VARs). All DD Form 254 for subcontracts shall be forwarded to DS/IS/ISP/INB for certification prior to issuance to the subcontractor.

See the contract clauses and DD 254 for the complete security requirements.

## Non-Disclosure Agreement

The Contractor shall sign a non-disclosure agreement with the Department of State when working with sensitive and/or proprietary information (forms to be executed and maintained by the Contracting Officer Representative (COR)). The Contractor and its employees shall exercise the utmost discretion in regard to all matters relating to their duties and functions. The Contractor shall not communicate to any person any information known to them by reason of their performance of services under this task order which has not been made public, except in the necessary performance of their duties or upon written authorization of the contractor officer.

All documents and records (including photographs) generated during the performance of work under this task order shall be for the sole use of and become the exclusive property of the U.S. Government. Furthermore, no article, book, pamphlet, recording, broadcast, speech, television appearance, film or photograph concerning any aspect of work performed under this task order shall be published or disseminated through any media without prior written authorization of the contracting officer. The contractor shall include the substance of this provision in all contracts of employment and in all subcontracts.

## Organizational Conflict of Interest (OCI)

* 1. Determination. The Government has determined that this effort may result in an actual or potential conflict of interest or may provide one or more Offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting (description to be included in task order request).
  2. If any such conflict of interest is found to exist, the TO Contracting Officer may (1) disqualify the Offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the Offeror and include the appropriate provisions to mitigate or avoid such conflict in the task order awarded. After discussion with the Offeror, the TO Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the Offeror may be found ineligible for award and if the task order has already been awarded and new information comes to light such as a Corporate Change as described in section f, the government may terminate the contract for connivence.
  3. Disclosure: The Offeror hereby represents to the best of its knowledge that:
     1. \_\_\_\_It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this task order, or
     2. \_\_\_\_It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with paragraph (d) of this provision.
  4. Mitigation/Waiver. If an Offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the Offeror shall submit a mitigation plan to the Government, IRM/BMP/ITA/CM, for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan. If not defined, then this provision applies fully.
  5. Other Relevant Information: In addition to the mitigation plan, the TO Contracting Officer may require further relevant information from the Offeror. The TO Contracting Officer will use all information submitted by the Offeror, and any other relevant information know to DOS, to determine whether an award to the Offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.
  6. Corporation Change. The successful Offeror shall inform the TO Contracting Officer and Evolve Program Manager within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

Flow-down. The contractor shall insert the substance of this clause in each first-tier subcontract that exceeds the simplified acquisition threshold.

## Associate Contractor Agreements

Within the first 30 days of task order award the contractor shall provide a draft ACA to the Evolve Program Manager for review and approval. An example is provided in Attachment J-7, Associate Contractor Agreement Sample.

Table in paragraph (g) below will be populated once prime task order contract awardees are known.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(a) The Contractor shall enter into Associate Contractor Agreements (ACA) for any portion of the contract requiring joint participation in the accomplishment of the Government’s requirement. The agreements shall include the basis for sharing information, collected mission requirements, code, data, technical knowledge, expertise, and/or resources essential to the integration of the Evolve

Program and individual task order objectives, software baselines, and components, which shall ensure the greatest degree of cooperation for the development of the program to meet the terms of the contract. Associate contractors are listed in paragraph (g) below.

(b) ACAs shall include the following general information (See template to utilize):

(1) Identify the associate contractors and their relationships.

(2) Identify the program involved and the relevant Government contracts of the associate

contractors.

(3) Describe the associate contractor interfaces by general subject matter.

(4) Specify the categories of information to be exchanged or support to be provided.

(5) Include the expiration date (or event) of the ACA.

(6) Identify potential conflicts between relevant Government contracts and the ACA; include

agreements on protection of proprietary data and restrictions on employees.

(7) Identify the process through which contractors will ensure interoperability of processes and technology used under each task order. For example, ensuring that no tool can only be operated by one contractor

(c) A copy of such agreement shall be provided to the awardees by the Government for review

before execution of the document by the cooperating contractors. All awardees need to collaborate on finalized ACA.

(d) The Contractor is not relieved of any contract requirements or entitled to any adjustments to

the contract terms because of a failure to resolve a disagreement with an associate contractor.

(e) Liability for the improper disclosure of any proprietary data contained in or referenced by any agreement shall rest with the parties to the agreement, and not the Government.

(f) All costs associated with the agreements are included in the negotiated cost of this contract.

Agreements may be amended as required by the Government during the performance of this

contract.

(g) The following contractors are associate contractors with whom agreements are required:

1. Associate Contractors

|  |  |  |
| --- | --- | --- |
| **Contractor** | **Address** | **Program/Contract** |
|  |  |  |
|  |  |  |

## Travel

Personnel assigned to this contract may be required to travel. All officially directed travel, per diem and associated miscellaneous expenses required as a result of work performed under this contract shall strictly adhere to all Government travel regulations. Travel is receipt reimbursable. Unless otherwise specified in the task order, travel to work locations within 50 miles of the National Capital Beltway (495) is considered local travel and will not be reimbursable.

## Other Direct Costs

Other direct costs may be required to deliver the services in the PWS.

## Funding

This task order will be incrementally funded.

## Task Order Management

TO management are mandatory for all TOs placed under the Evolve contract. The objective of contract and TO management is to provide the program management, project control and contract administration necessary to manage a high volume, multiple contract type TO process for a large, diversified team so that the cost, schedule and quality requirements of each order are tracked, communicated to the government, and ultimately attained.

The use of commercially available automated tools and the application of expertise on processes and metrics that support task order management are encouraged to achieve the above objectives. The objective of the tools is to provide quicker access, improved accuracy, and enhanced accessibility for Contractors/clients, real-time monitoring of status/deliverables, tracking the quality of work products and gauging overall customer satisfaction.

## Key Personnel

The Contractor shall identify key personnel and provide resumes for the positions identified as key personnel for this task order. If the proposed key personnel are not current employees, then the resume must be accompanied with a signed letter of intent that states the prospective employee has authorized their resume to be submitted, intends to accept employment if the Offeror is selected for award, and that the parties have agreed to salary parameters. If any of the key personnel candidates become unavailable at any point during the evaluation process, the Offeror shall immediately notify the Contracting Officer. The contractor shall be able to replace key personnel within 15 business days. Replacement requires government approval and personnel must meet same criteria as the original employee.

Listed below are minimum key personnel considered essential to the performance of work for this Task Order.

1. Task Order Key Personnel

| Labor Category | Description |
| --- | --- |
| Task Order Program Manager | Acts as a single technical point of contact (POC) who shall work closely with the Government Program Manager (PM), Contracting Officer Representative (COR), and Government Technical Monitor (GTM).  **The Task Order PM shall:**   * Serve as the program manager typically responsible for organizing, directing, and managing all aspects of contract operational support functions involving multiple complex and inter-related project tasks that often require managing teams of contractor personnel at multiple locations. * Manage and maintain contractor interface with the senior levels of the customer’s organization. * Manage the customer engagement and relationship management aspects of cloud services, driving processes to understand current and emerging customer requirements, pain points, and concerns. * Consult with customer and contractor personnel to formulate and review task plans and deliverables, ensuring conformance with program and project task schedules and costs and contractual obligations. * Establish and maintain technical and financial reports to show progress of projects to management and customers, organize and assign responsibilities to subordinates, oversee the successful completion of all assigned tasks, and assume the initiative and provide support to marketing personnel in identifying and acquiring potential business. * Support the government financial management of cloud services, including defining how cloud costs are funded (e.g. chargeback, centrally funded, showback), what architecture principles around cost optimization should be implemented, and the ability to forecast cloud costs.   **Minimum qualifications:**   * 10 years of relevant experience * Bachelor’s degree in a related field, with a preference for a Masters degree in Business Administration (MBA) or Information Technology * ITIL Certified * PMP Certified (current) * Agile certification highly desired * Demonstrated progressive IT experience in the Functional Area which the offeror is proposing. At least one project shall have occurred within the past three (3) years of similar scope with a total contract value greater than $10M and global delivery in a highly complex environment. Oversight or management of at least one project shall have been conducted in accordance with a CMM certified, Agile, and ITIL approach. * Demonstrate proven experience and documented success supervising large IT services contracts, including people of various job categories and skills. * Demonstrate expertise in the management and control of costs and resources and demonstrated capability in managing projects of this type and complexity. * Demonstrated experience providing system modernization and innovation that resulted in increased operational efficiency or cost savings. |

## Substitution of Key Personnel

The Contractor shall notify the TO CO and the TO COR prior to making any changes in Task Order Key Personnel. No changes in TO Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the TO Key Personnel being replaced. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The TO CO shall be notified in writing of any proposed substitution at least forty-five (45) days, or sixty (60) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include:

1. an explanation of the circumstances necessitating the substitution;
2. a complete resume of the proposed substitute; and
3. any other information requested by the TO CO to enable him/her to make a key personnel replacement determination

The Evolve Program Manager and the contract level CO will evaluate substitutions at the contract level and the TO CO and TO COR will evaluate TO level substitutions. Requests will be reviewed promptly the Contractor will receive timely written notification of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days of receipt of the written denial by the Contractor. The Contractor shall allow a minimum of a two-week transition of key personnel.H.11 Insurance

Insurance of the following kinds and minimum amounts shall be furnished at any time at the request of the CO and maintained during the period of performance of this contract:

1. Worker's compensation and employer's liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(a).
2. General liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(b).
3. Automobile liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(c).

## Meetings / Conferences

## Task Order Kick-Off Meeting

The purpose of the Kick-Off Meeting is to achieve a clear and mutual understanding of all task order requirements and to identify and resolve potential problems.

The Contractor shall:

* Attend a task order kick off meeting convened by the Government, onsite or virtual, within 30 days after task order award;
* Introduce key personnel during the meeting and present management and risk management processes to be used under the task order, addressing key risks to include dependencies and mitigation for each identified risk; and
* Update and present the following:
  + - Updated Transition-In Plan
    - Updated Project Management Plan (PMP)
    - Master Milestone Schedule
    - Associate Contractor Agreement(s)
    - Updated Earned Value Management Plan
    - Agile Reporting Tool (if applicable)

## Task Order Deliverables

1. Unless the Government identifies otherwise, all deliverables must be submitted in English and in electronic, Microsoft Office compatible, format via email.
2. The Government will review each deliverable product and may provide oral and written comments. The Contractor shall review and incorporate comments or implement directed changes no later than five (5) business days thereafter. This time period may be extended, at the sole discretion of the Government, by written approval of the Contracting Officer or COR (if responsibility has been delegated by the CO).
3. All documentation and reports developed or provided by the Contractor shall become the property of the U.S. Government. Reports shall not contain any markings or legends which will restrict the Department’s use of such reports in any way. All deliverables, including attachments, shall comply with the data right clauses incorporated in the contract. The Government will reject all deliverables containing markings contradicting said clauses.
4. Deliverables longer than 5 pages shall include a table of contents. Attachments, if any, shall include the attachment number, deliverable name and number, and contract number and task order number.
5. For purposes of delivery, all deliverables shall be made by close of business (COB) 4:30 P.M. local time (Washington, DC) at destination, Monday through Friday, unless stated otherwise.
6. All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.
7. Each deliverable shall be accompanied by a cover letter from the Contractor. Multiple deliverables may be delivered with a single cover letter describing the contents of the complete package.
8. In the event the Contractor anticipates difficulty in complying with any task order-level deliverable, the Contractor shall provide written notification immediately to the task order-level Contracting Officer and TO COR. Each notification shall give pertinent details, including the date by which the Contractor expects to make delivery; PROVIDED, that this data shall be informational only in character and that receipt thereof shall not be construed as a waiver by the Government of any contract delivery schedule, or any rights or remedies provided by law or under this contract.

Schedule of Deliverables

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Deliverable | Section Reference | Due Date | Update Frequency | Distribution |
| Associated Contractor Agreement | 3.9 | 30 days after every new task order award and updated as applicable | As needed | Evolve Program Manager |
| Meetings/Conferences (Meeting notes/action items) | 4.2 | 3 working days after meeting / conference | As required | CO, TO COR, Evolve Program Manager |
| Monthly Cost Performance Report | 4.3.1 |  |  |  |
| Monthly Master Milestone Schedule | 4.3.2 |  |  |  |
| Project Management Plan, to include Quality Control Plan | 4.4.9 | Within 30 calendar days after TO award (Draft) | Annually, or upon request |  |
| Quality Assurance Surveillance Plan | 5.2.2 |  |  |  |
| Task Order Kick Off Meeting (Draft Schedule) | 4.2.1 | Prior to task order start date | N/A |  |
| Task Order Monthly Status Reports | 4.3.3 | 1 month after award of first task order | Monthly | CO, COR, Evolve Program Manager |
| Transition-in Plan | 4.3.4 | 30 calendar days from award of first task order | One-time | TO CO, TO COR, TO CPM |
| Transition-out Plan | 4.3.5 | NLT 120 calendar days prior to the end of contract or 60 calendar days following the Government’s request | One-time | TO CO, TO COR, TO CPM |

## Monthly Cost Performance Report

The Contractor shall provide a Cost Performance Report (CPR) that provides DOS management with costs incurred and progress against the previous monthly schedule. These costs shall tie back to the CWBS. The report shall include cumulative data from contract inception through the report month. The report shall include the actual and invoiced costs. The data shall be reported in accordance with the standards indicated in the task/delivery order showing earned value and variances. A CWBS increment of work (e.g., the task area level) shall be considered out-of-tolerance if the year-to-date actuals exceed the budgeted amount by 2 percent or more. A variance analysis shall be provided as explanation for out-of-tolerance variances.

## Monthly Master Milestone Schedule

The Contractor shall provide a monthly Master Milestone Schedule (MMS) that shall contain projected and actual schedules versus progress with technical direction deliverables and other milestones clearly identified. Approved modification of baseline schedules shall be clearly delineated from the original baseline.

## Task Order Monthly Status Reports

The Contractor’s PM shall develop and provide an MSR via electronic mail to the CO, COR and GTM by the 10th of the following month. The Contractor shall consult with the COR on the format of the report. The MSR shall include, at minimum, the following:

Activities during reporting period, by task (include: on-going activities; new activities; activities completed; progress to date on all above-mentioned activities). Start each section with a brief description of the task

Problems and corrective actions taken. Also include all new and pending issues or concerns and proposed resolutions to address them

Personnel gains, losses, and status

Government actions required

Project schedule (major tasks, milestones, deliverables, planned and actual start and completion dates, etc.)

List of all documents submitted during reporting period to include version number and last revision date.

If applicable, submit a summary of trips taken, conferences attended, etc.

At the CO’s, COR’s, or GTM’s request, a monthly status meeting may be held. In addition, the contractor shall meet as necessary with the government to discuss progress and problems. These meetings shall enable problems to be identified and resolved quickly. The contractor shall document the problems and the solutions.

## Transition-In Plan

The contractor shall develop a Transition-in Plan that details activities that shall be completed no later than 30 calendar days from the effective date of performance.

The Transition-In Plan shall include the following:

* Planned transition activities
* Transition activity timelines and milestones
* Transition resource requirements (includes the retention of current staff, as applicable and appropriate)
* Transition security implications
* Transition risks and mitigation or avoidance strategies; and
* Transition notifications and training of users

## Transition-Out Plan

The contractor shall develop a Transition-out Plan that facilitates the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the contractor.

The contractor shall provide a final Transition-Out Plan NLT 120 calendar days prior to the end of the contract, or 60 calendar days after the Government requests the deliverable.

The Transition-Out Plan shall include the following:

* Project management processes
* Points of contacts
* Location of technical and project management documentation, data, and methods of providing these to these to the incoming service provider
* Status of ongoing technical initiatives
* Appropriate contractor-to-contractor coordination to ensure a seamless transition
* Transition of Key Personnel
* Schedules and milestones
* Actions required of the Government
* Methods of measuring transition risks that includes a complete inventory of the transition risks, with assigned severity and probability, and response plans to address the risks either through avoidance, mitigation, or other means
* Method of permitting the successor service provider to observe and become familiar with any and all operation specified in this PWS for a minimum of 120 calendar days prior to the expiration or termination of the contract
* Method of establishing and maintaining effective communication with the incoming service provider for the period of the transition via weekly status meetings; and
* Method for ensuring that all information assets and related configuration information is up-to-date and available for the Government’s review at least 120 calendar days prior to the end of the contract

## Project Management Plan

The Project Management Plan (PMP) shall define policies and procedures for managing and directing the effort for productivity, quality, cost control, and early identification and resolution of problems. The PMP shall include schedules, milestones, tasks, and subtasks required in the PWS.

* The PMP shall provide a Work Breakdown Structure (WBS) or epics with user stories, and associated roles and responsibilities of the Contractor.
* The PMP shall include the Contractor’s Quality Control Plan (QCP), Transition Plan Overview, and the stakeholder management and communication plan. The Contractor shall provide the Government with an initial PMP draft.
* The Contractor will be prepared to review and discuss the initial PMP outline at the Project Kick-Off Meeting. The PMP is a “living document” and shall be updated as necessary to reflect current tasks, objectives, and deliverables. The Contractor shall work from the latest Government approved version of the PMP

## Performance Requirements

## Quality of Reports and Deliverables

General quality measures, as set forth below, will be applied to each work product received from the Contractor under this contract.

1. Accuracy: work products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
2. Clarity: work products shall be clear and concise. Any/all diagrams shall be easy to understand and be relevant to the supporting narrative.
3. Consistency to Requirements: All work products must satisfy the requirements of this contract and specific task orders.
4. Timeliness: work products shall be submitted on or before the due date specified herein or submitted in accordance with a later scheduled date determined by the Government.

## Acceptance Criteria and Inspection

Acceptance of all written documents and other deliverables will be contingent upon Government Task Manager (GTM) review and approval. The GTM will discuss each specific task with the Contractor to ensure that the goals and objectives are clearly defined. Required graphs, charts, columns and rows of data shall be legible and properly formatted. Unless valid justification is cited to the contrary, the GTM comments will be incorporated into the respective final documents and reports. If GTM comments given do not conform to safe business practices, or are deemed technically unsound; it is the responsibility of the Contractor to advise the GTM. Consensus is required between the GTM and the Contractor; however if consensus is not achieved, actions will be as directed by the GTM.

Upon approval of the final draft, deliverables will be submitted in final form to the GTM. All deliverables shall be delivered to the GTM in both hard copy and electronic format, which will be determined upon contract award.

## Quality Control and Quality Assurance

## Quality Control

The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor’s quality control program is the means by which it assures that the work complies with the requirement of the contract.

After acceptance of the quality control plan the contractor shall receive the contracting officer’s acceptance in writing of any proposed change to his QC system.

## Quality Assurance

The Government will utilize several quality assurance procedures to ensure contractor compliance with this task order, as detailed in attachment J-X: QASP. The QASP sets forth the procedures and guidelines that the Department of State, Bureau of Information Resources Management will use in ensuring the required performance standards or services levels are achieved by the contractor

Examples include inspection of deliverables, review of reports, and onsite progress meetings, performance evaluations, etc. to ensure that, at a minimum, the PWS requirements have been met; sufficient consideration has been given to alternative approaches for implementing the components of the project; and defensible explanations have been provided to justify recommendations, etc.

The contractor shall maintain the highest degree of quality for all activities performed throughout the period of performance of the task order. The Government shall regularly evaluate the Contractor’s performance including, but not limited to:

* Inspections of deliverables identified within this PWS for completeness, accuracy and timeliness; note that it is the Contractor’s responsibility to ensure adherence to the submitted QCP to ensure acceptable performance under the award.
* Assurances that validated and correct implementation strategies have been selected for the program.
* The contractors’ ability to retain quality individuals to perform the contact requirements.