Logo

Description automatically generated

U.S. Department of State

Evolve

Attachment J-34

Sample Task Order

for

Application Development Services

SOLICITATION

19AQMM22R0029

OCTOBER 2022

Performance Work Statement

Table of Contents

[1.0 General - 1 -](#_Toc107236318)

[1.1 Introduction - 1 -](#_Toc107236319)

[1.2 Background and Purpose - 1 -](#_Toc107236320)

[1.3 Objectives - 1 -](#_Toc107236321)

[1.4 Scope - 2 -](#_Toc107236322)

[1.5 Tools, Technology and Applications - 3 -](#_Toc107236323)

[1.6 Critical Elements - 4 -](#_Toc107236324)

[1.7 Type of Contract - 5 -](#_Toc107236325)

[2.0 Task Order Performance Requirements - 5 -](#_Toc107236326)

[2.1 Task Area 1: Systems Design and Development - 6 -](#_Toc107236327)

[2.1.1 Business Process Re-Engineering - 6 -](#_Toc107236328)

[2.1.2 DevSecOps - 8 -](#_Toc107236329)

[2.1.3 Quality Control/Validation and Verification - 12 -](#_Toc107236330)

[2.1.4 Monitoring and Reporting - 17 -](#_Toc107236331)

[2.1.5 Application Security and Compliance - 17 -](#_Toc107236332)

[2.1.6 Training Development and Support - 19 -](#_Toc107236333)

[2.1.7 Big Data Analytics - 19 -](#_Toc107236334)

[2.1.8 Cloud Computing - 20 -](#_Toc107236335)

[2.1.9 Other - 20 -](#_Toc107236336)

[2.2 Task Area 2: Systems Operations and Maintenance - 22 -](#_Toc107236337)

[2.2.1 IT Service Management (Change, Configuration, Release, Incident, Problem) - 22 -](#_Toc107236338)

[2.2.2 Application Environments - 29 -](#_Toc107236339)

[2.2.3 Deployment Support - 30 -](#_Toc107236340)

[2.2.4 Code Maintenance - 31 -](#_Toc107236341)

[2.2.5 Technical Support - 38 -](#_Toc107236342)

[2.2.6 Operations and Maintenance Monitoring and Reporting - 41 -](#_Toc107236343)

[2.2.7 Code Migration - 42 -](#_Toc107236344)

[2.2.8 Quality Assurance (QA) / Quality Management (QM) - 42 -](#_Toc107236345)

[2.2.9 Customer Engagement - 43 -](#_Toc107236346)

[2.3 Task Area 3: Innovation - 44 -](#_Toc107236347)

[2.4 Task Area 4: Cross-Functional Requirements - 45 -](#_Toc107236348)

[2.4.1 Compliance - 45 -](#_Toc107236349)

[2.4.2 Security - 46 -](#_Toc107236350)

[2.4.3 Disaster Recovery - 50 -](#_Toc107236351)

[2.4.4 Client Management - 50 -](#_Toc107236352)

[2.4.5 IT Service Management - 50 -](#_Toc107236353)

[2.4.6 Product and Project Management - 50 -](#_Toc107236354)

[2.4.7 Innovation, Ideation, and Modernization - 52 -](#_Toc107236355)

[3.0 Special Requirements/Instructions - 52 -](#_Toc107236356)

[3.1 Standards (e.g., 5 FAM 600) - 52 -](#_Toc107236357)

[3.2 Government-Furnished Equipment / Information - 52 -](#_Toc107236358)

[3.3 Government-Data - 53 -](#_Toc107236359)

[3.4 Intellectual Property Rights - 53 -](#_Toc107236360)

[3.5 Place of Performance - 53 -](#_Toc107236361)

[3.6 Standard Work Hours - 53 -](#_Toc107236362)

[3.7 Facilities - 53 -](#_Toc107236363)

[3.8 Security Clearance Requirements - 54 -](#_Toc107236364)

[3.8.1 Non-Disclosure Agreement - 54 -](#_Toc107236365)

[3.9 Organizational Conflict of Interest (OCI) - 55 -](#_Toc107236366)

[3.10 Associate Contractor Agreements - 56 -](#_Toc107236367)

[3.11 Travel - 57 -](#_Toc107236368)

[3.12 Other Direct Costs - 57 -](#_Toc107236369)

[3.13 Funding - 57 -](#_Toc107236370)

[3.14 Invoice Approval - 57 -](#_Toc107236371)

[3.15 Earned Value Management System Requirements - 57 -](#_Toc107236372)

[4.0 Task Order Management - 57 -](#_Toc107236373)

[4.1 Key Personnel - 58 -](#_Toc107236374)

[4.2 Transition - 62 -](#_Toc107236375)

[4.2.1 Transition-In - 62 -](#_Toc107236376)

[4.2.2 Full Operational Capability - 62 -](#_Toc107236377)

[4.2.3 Transition-Out - 63 -](#_Toc107236378)

[4.3 Task Order Kick-Off Meeting - 64 -](#_Toc107236379)

[4.4 Task Order Monthly Status Reports (MSR) - 64 -](#_Toc107236380)

[4.4.1 Technical Deliverables - 65 -](#_Toc107236381)

[4.4.2 Small Business Participation Report - 65 -](#_Toc107236382)

[4.4.3 Agile or Iterative Project Reporting - 65 -](#_Toc107236383)

[4.4.4 Schedule of Deliverables - 65 -](#_Toc107236384)

[4.4.5 Acceptance Criteria and Inspection - 66 -](#_Toc107236385)

[4.5 Points of Contact - 66 -](#_Toc107236386)

[4.6 Environmental and Energy Conservation Objectives - 67 -](#_Toc107236387)

[5.0 Performance Requirements - 68 -](#_Toc107236388)

[5.1 Quality Control and Quality Assurance - 68 -](#_Toc107236389)

[5.1.1 Quality Control - 68 -](#_Toc107236390)

[5.1.2 Quality Assurance - 68 -](#_Toc107236391)

[5.2 Basic Performance Standards - 68 -](#_Toc107236392)

[5.3 Performance Requirements Summary - 69 -](#_Toc107236393)

1. List of Tables

Table 1. Application Development Task Areas - 2 -

Table 2. Tools - 3 -

Table 3. Applications - 4 -

Table 4. Typical Administrative Functions - 11 -

Table 5. Cross Functional Requirements - 44 -

Table 6. Federal Information Processing Standards Publications - 46 -

Table 7. National Institute of Standards and Technology Publications - 47 -

Table 8. Office of Management and Budget Publications - 47 -

Table 9. Security Policies - 47 -

Table 10. Associate Contractors - 56 -

Table 11. Key Personnel - 58 -

Table 12. Task Order Deliverables - 65 -

Table 13. Performance Requirements Summary Table - 68 -

1. General
   1. Introduction

This Performance Work Statement (or “PWS”) sets forth the roles and responsibilities of the Parties for Application Development provided under the EVOLVE IDIQ contract as part of the IT Management Services Functional Category. Application Development Services are the services and activities, as further detailed in this PWS, required to deliver a wide range of application development, operations and maintenance services to Department of State (DOS) and its partners.

* 1. Background and Purpose

The Bureau of Information Resource Management (IRM), led by the CIO, empowers the Department of State (from here on, “Department” or “DOS”) to achieve its foreign policy mission by providing modern, secure, and resilient information technology (IT) services. Rapid changes in technology are transforming how our diplomats advance U.S. foreign policy by altering the way we connect with others and communicate information. Our diplomats require powerful new technologies to advocate policy positions, promote awareness, and enhance transparency – that is where IRM comes in. IRM is seeking to award multiple performance-based Task Orders (TOs) to govern, manage, design, engineer, operate, maintain, improve, and secure the Department’s mission critical IT infrastructure and its associated programs.

IRM’s foremost objective is to foster innovative, effective, and interconnected diplomacy by constantly improving, modernizing, and refreshing tools and services. IRM is expanding the use of collaborative information development and refinement to provide end users with accurate and useful information – anytime, anywhere. IRM supports new IT solutions that provide access to collaborative tools and enables mobility, while simultaneously protecting our information and IT assets against evolving cyber threats and vulnerabilities.

The Department has a demonstrated need for software applications to fulfill process and functional needs in order to make work more efficient, to make data more available, and to use technology to further diplomatic efforts. The Department utilizes many kinds of software including commercial-off-the-shelf, custom-built, and Open Source to satisfy business needs across the enterprise. This portfolio requires resources with a wide breadth of IT knowledge and capabilities to not only determine the best possible solution to meet a business need but also to implement and support that solution for years to come.

This document will define required functional areas for those resources and the expectations for work to be performed.

* 1. Objective

DOS is seeking an industry partner to provide software development and maintenance services.

The objective of this task order is to:

* Develop and implement enterprise and departmental-level applications. These applications may have inter-related service processing components extending across/beyond the enterprise or be unique to a particular bureau’s mission requirements.
* Provide production, deployment, implementation, integration, and software application maintenance to ensure DOS applications and databases will enable their users to meet their mission goals and objectives.
  1. Scope

The scope of work for this effort will include holistic, customer-centric software application development, testing, security, release, data management and operations support. It addresses key enablers such as Agile development capabilities, human centered design, change management and end-user adoption. It leverages fully integrated CI/CD pipeline capabilities built on enterprise cloud platforms, integrated into the enterprise dev/sec/ops model to support rapid development capabilities. It includes multiple code bases and application types including Open Source, SaaS/aPaaS, and custom development activity. In addition, it supports the management and security of APIs needed to share data between multiple applications and analytics platforms. Furthermore, it supports the integration of new and emerging technologies at the application layer to include RBA, A/I, IoT, block chain, etc. Scope includes:

* Resources involved with the analysis, design, development, code, test, and release packaging services associated with application development projects
* Operations, support, fix, and minor enhancements associated with existing applications
* Distributed and mainframe databases, middleware systems and DBMS software and tools support
* Distributed database services focused on the physical database (versus the logical design) including DBAs, DBMS, tools, and operational support
* Distributed platform, application and system integration resources enabling cross application development, communications, and information sharing

The following task areas are outlined in this document.

1. Application Development Task Areas

| **Application Development Task Areas** |
| --- |
| 1. Systems Design and Development    * Business and Systems Analysis    * Solution Architecture    * DevSecOps    * Quality    * Robotic Process Automation    * Big Data Analytics    * Security and Compliance    * Training Development and Support    * Business Intelligence    * Cloud Computing    * Other |
| 1. Systems Operations and Maintenance    * IT Service Management (Change, Configuration, Release, Incident, Problem)    * Application Environments    * Deployment Support    * Application Maintenance    * Technical Support    * Operations and Maintenance Monitoring and Reporting    * Code Migration    * Quality Assurance (QA) / Quality Management (QM)    * Customer Engagement |
| 1. Innovation |
| 1. Cross-Functional Requirements |

* 1. Tools, Technology and Applications

The following tools and technology are currently utilized in support of Application Development activities. The applications identified are a sub-set of the DOS portfolio Contractor shall support.

* + 1. Tools

DOS currently uses the following tools and technology to support development and delivery of Application Development services:

1. Tools

| Tool / Technology |
| --- |
| Active Directory |
| Amazon Web Services |
| Atlassian JIRA |
| Azure DevOps - Code repository, work effort tracking, user stories/epic collections, pipeline definitions, reporting |
| ERWIN |
| F5 Load Balancer |
| GITHUB - Manage defects and statuses |
| GitLab - Code repository and collaborative software development platform for large DevOps and DevSecOps projects |
| GSuite |
| Informatica |
| iMatrix |
| iPost |
| iSchedule |
| MicroFocus Fortify - Static code analysis scanning tool |
| MS Azure |
| MS O365 - SharePoint Online, Dynamics Online, PowerBI, OneDrive, PowerApps, Forms, and Flow |
| MS Project Server |
| MS Visio |
| MS Visual Studio/VS Code - IDEs for code development; some users require Visual Studio features while for others VS Code is sufficient |
| ServiceNow |
| Salesforce |
| UiPath |
| SAP Business Objects |
| Team Foundation Server - Requirements and source code management, manage defects and statuses |

* 1. Applications

The following list includes, but is not limited to, the applications requiring development and/or operations and maintenance support.

1. Applications

| Application / Application Type |
| --- |
| Enterprise Messaging Services - State Messaging and Archive Retrieval Toolset (SMART), Common LAN outbound Telegram (CLOUT), Printing Archival Profiled External Requests (PAPER), enterprise Cross Domain System (CDS), State Automated Messaging System Multi Functioning Interrupter (SAMS-MFI), Automated Message Address Distribution System High Speed Channel Link (AMADS HSCL), Information Transport Service (ITS), and State Automated Message System Relay (SAMS-R), links to other government agencies, electronic records (eRecords) system transport and records storage activities, and Top Secret Messaging (TSM). |
| ITSM, IMDB, eDiscovery |
| Custom Google Development (digital signage, Apps Script, GCP) |
| Workflow Solutions (public-facing and internal-only) |
| Back-Office Utilities and Management Systems |
| Collaboration Services (public-facing and internal-only) |

* 1. Critical Elements

The Evolve contractors are expected to provide high-performing, skilled teams. Critical elements shall be:

* High productivity
* High quality work
* Collaboration and cooperation with other teams and participants
* Technical skills and expertise as necessary (see below)
* Estimation and planning skills
* Innovation and creativity in problem solving
* Efficient use of team resources to maximize productivity in named tasks

The providers of Evolve services shall adopt evolving DOS design and coding standards in the course of their application development. The Contractors shall provide technical methods, techniques, and concepts that are innovative, practical, cost-effective, and conducive to Agile application development and Lean sustainment. The Contractors shall maintain applications based on requirements that are evolving and emerge as the business climate shifts. Evolve developers will be required to develop high quality code and are responsible for any technical debt that is incurred as a result of their sustainment-related development activities.

Agile development work involves some degree of analysis, requirements collection, design, development, and test, in addition to the support functions of configuration management, planning, project management, infrastructure, service desk support, reporting, security, and system administration.

Evolve currently consists of applications listed in Table 3. Given that the Department is changing and evolving additional applications and tools may be added during the performance of this requirement.

The Evolve Contractors will be expected to work with a technical architecture and design specified by the Government, and to work within the Agile process and SELC frameworks defined by the Government. Individual sustainment teams at the IRM programmatic level will include Government employees functioning as product owners, product managers, integrators, business area subject matter experts (SME), and so on, as well as other Contractors with roles in infrastructure, continuous integration, quality assurance, and Independent Verification and Validation (IV&V). Evolve Contractors are expected to work well in these team environments and demonstrate a highly collaborative and cooperative attitude. It is expected that Evolve Contractors adopt commercial industry best practices into our ability to accelerate product delivery in the fast changing and agile environment of DOS IRM.

* 1. Contract Type

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

1. Task Order Performance Requirements

The Contractors shall coordinate efforts with the Government team that is assigned technical and management responsibilities for applications. The Contractors shall organize, direct and coordinate planning and execution of all task activities. The Contractors shall manage all Contractor resources and supervise all Contractor staff in the performance of work on this task order. The Contractors shall manage and coordinate its team(s) on a day-to-day basis and ensure plans are communicated to team members. Likewise, the Contractors must ensure that the health and progress against those plans are adequately reported.

For all task areas described herein, the contractor shall:

* Ensure all work activities are performed in a timely and cost-effective manner while maintaining the highest quality of performance to achieve expected outcomes.
* Document all processes utilized in the successful execution of activities.
* Ensure communications are thorough, accurate, timely, and tailored to the audience for both IRM stakeholders and the customer.
* Collaborate with other technical and non-technical teams across DOS as needed to effectively accomplish goals.
* Organize, conduct, and attend meetings as required.
* Develop and deliver timely, complete, and accurate meeting artifacts as required.
* Use DOS designated repositories and tools for all deliverables as required.
  1. Task Area 1: Systems Design and Development

The Contractor shall perform the following tasks/subtasks.

* + 1. Business Process Re-Engineering

Business process re-engineering includes the activities associated with defining how technology solutions can best solve business problems for DOS. Examples include conducting analysis on the feasibility and impact of proposed solutions, defining the functional and non-functional requirements for new applications or application enhancements, participating throughout the software development lifecycle.

The Contractor shall:

1. Provide analysis and support development of long / short-range plans for technology selection, development, maintenance, and production activities.
2. Participate in technical and business planning sessions as required to establish standards, architecture, and project initiatives.
3. Formulate and define systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements.
4. Provide consultation on complex projects and be considered the top-level contributor/specialist of most phases of systems analysis, while considering the business implications of the application of technology to the current and future business environment.
5. Conduct Analysis of Alternatives (AoA)/Alternative Analysis (AA) to identify potential solutions to meet the need of IRM’s customers. The outcome of the analysis shall be documented and presented with decision analysis for leadership consideration.
6. Conduct cost-benefit analyses for solutions
7. Conduct feasibility studies for the implementation of new technologies.
8. Support transition of offices moving from Waterfall application development to Agile Methodology
9. Provide business requirements definition services associated with understanding business needs and supporting customer challenges for new or existing endeavours; as well as support the development of business requirements that are mapped to programmatic needs and will be transitioned to implementation services internal or external to DOS.
   1. Facilitate the identification of sound functional and non-functional requirements ensuring they are captured accurately, thoroughly and without ambiguity. Communicate requirements that may conflict or cause hardship, work with stakeholders to remediate, escalating where appropriate.
   2. Lead efforts with stakeholders to identify solutions to problems through interviews, meetings with requirements groups and user representatives group workshops, surveys, and other tools.
   3. Develop functional requirements documents, logical and physical data model and/or identified requirements or process documents associated with the project.
   4. Ensure requirements are consistent with existing policies and frameworks and do not comprise security.
   5. Ensure analysis is consistent with agile scrum processes and CMMI requirements processes at a maturity level of 3 or higher and at a minimum must include elicitation, documentation, validation, configuration control of requirements artifacts and objects, and quality control of produced outputs.
10. Provide business process re-engineering needs
11. Provide evaluations of existing procedures, processes, techniques, models, and systems related to management problems or contractual issues that would require a report and recommend solutions.
12. Build Proof of Concepts (POCs), prototypes, or pilot systems to test design ideas and assumptions. The main purpose of developing a POC is to demonstrate the functionality and to verify a certain concept or theory that can be achieved in development. Prototypes and pilots will be a working interactive model of the end products that demonstrate the design, navigation, and layout. The outcome of prototype tasks will show how the target solution will be developed.
13. Support Test Driven Development.
14. Develop and/or modify procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results, including analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications.
15. Perform and/or participate in operational planning for capacity and performance purposes, disaster recover, security, and other activities related to application development and maintenance.
16. Participate in technical and business planning sessions as required to establish standards, architecture, and project initiatives.
17. Collaborate with customers and stakeholders to define and document governance, rules of behavior, and customer Service Level Agreements.
18. Quality Assurance includes but is not limited to the following:
19. Reviewing and auditing project documentation for accuracy and compliance with DOS standards.
20. Performing process (control gate) audits, product reviews, and other audits as needed on projects/programs.
21. Participation in risk management meetings, peer reviews, formal customer reviews or other process improvement team meetings; and
22. Preparing quality assurance plans and maintaining records of quality assurance audit results and suggestions for improvement.
23. Participate in all necessary software development phases and/or rituals plus quality management and process definition activities for maturing and enhancing business analysis services.
    * 1. DevSecOps

DoS is a high performing environment where contractors are expected to deliver high quality, production-ready functionality in an incremental fashion using Agile development practices and methods by conducting scrum or Kanban ceremonies. The Contractor is required to delivery all requested documentation including, but not limited to, lifecycle management gate reviews, status, metrics, process flows, presentations, minutes, flow charts, designs, project and research plans. Currently, DoS uses Atlassian’s Jira and Confluence to document, plan, track and manage the development and the overall program. Necessary Agile Documentation shall all be available in Confluence and Jira.

DoS requires the contractor to provide modern digital services that use development, security and operations (DevSecOps) techniques that embrace cloud based, scalable architecture, immutable infrastructure, automated testing and continuous integration and continuous deployment. In addition, deliver secure and tested mobile and web designs and applications using automated testing frameworks that utilize services, microservices and containers.

Application development includes, but is not limited to, the activities associated with development of new applications, building extensions to and interfaces between new and existing applications; and making changes and enhancements to existing applications, custom applications, business intelligence data sources, database and data warehouse applications, GOTS/COTS applications, and physical databases. The extent of any or all of these activities is based on the needs of DOS. It also includes design services, programming and development services, integration services, code migration services, software configuration management services, and technical change management services.

* + 1. Human-centered Design

The Contractor shall:

1. Apply Human-centered design methodologies to enhance the usability, human factors, and user experience.
2. Ensure documentation that specifies all components, program modules, data stores, interfaces, interface components and associated operations procedures for the technical environment.
3. Incorporate architectural guidelines into the design, including application extensibility, maintainability, scalability, robustness and reliability.
4. Create detailed design document from the business Identify technical requirements, logical and physical data models.
5. Conduct site surveys for design efforts as required.
6. Develop and maintain the application integration architecture.
7. Develop and maintain the data architecture.
8. Design modern software User Experiences (UX).
9. Design Graphical User Interfaces (GUI).
10. Create prototypes, mock-ups and presentations.
11. Work with test team to develop test cases as defined in testing plan.
12. Define implementation and deployment procedures, project schedules and staffing requirements to meet deployment and delivery requirements.
13. Develop and maintain release specific application architectures.
14. Implement Responsive Web Design (RWD).
15. Utilize technology to maximize maintainability and reusability of designs.
16. Comply with Section 508 accessibility requirements.
17. Comply with mobile ready requirements.
18. Document all processes utilized in the successful execution of application design and development activities.
    * 1. Development

The Contractor shall:

1. Provide rapid delivery in small batches, increasing the frequency and pace of releases, applying the continuous integration and continuous delivery practices.
2. Integrate security into the DevSecOps workflow in a collaborative way by employing a “DevSecOps” approach and deliver the system with built-in security.
3. Account for each member of the contractor’s DevSecOps team to be responsible for security.
4. The contractor shall employ design patterns that enable code simplicity, user’s needs, and future maintainability.
5. Employ microservice architecture on OpenShift Platform, as a design approach, to build applications as a set of small services, organized into aggregates, with transactional consistency.
6. Employ Infrastructure as Code (IAC) as a practice enabling the cloud’s Application Programming Interface (API)-driven model to interact with infrastructure programmatically.
7. Have estimation and planning skills for analyzing user stories for size and requirements.
8. Be responsible for providing continuous production support and maintenance.
9. Develop monitoring, alerting systems, and logging practices to help stakeholders stay informed of performance in real-time.
10. Incorporate monitoring solutions like Hygieia, New Relic, etc. The contractor may suggest new methods or tools; however, developers shall add health checks to code so that monitoring tools can detect changes with appropriate metrics.
11. Ensure that the system complies with the Agency’s security policies to safeguard the system against external and insider threats.
12. Ensure that teams implement proactive approaches to reduce vulnerabilities and to improve responsiveness to unforeseen events.
13. Ensure that the system has quality build-in, by prioritizing Availability, Maintainability, Vulnerability, and Reliability.
14. Collaborate and cooperate with government and other contractor teams to improve the user experience, to baseline and re-establish key performance parameters for the system, and to address all gaps as part of continuous improvement and collaboration.
15. Immediately fix any escaped defects that have a significant impact on business operations.
16. Adopt DOS design and coding standards during their application development.
17. Provide technical methods, techniques, and concepts that are innovative, practical, cost-effective, and conducive to the Department’s processes and quality standards.
18. Adhere to Test Driven Development when implementing solutions.
19. Develop applications based on requirements that are evolving and emerge as the business climate shifts.
    * 1. System and Database Administration

The Contractor shall:

1. Provide system and database administrators for the engineering/development environments.
2. Support the execution of emergency backups in coordination with other infrastructure operational components; support the development of contingency plans, including disaster recovery and COOP testing, and operation failover testing consisting of documented contingency plans; develop contingency plans for supported applications.
3. Routinely evaluate the need to upgrade database servers and application software while determining compatibility with current application versions.
4. Configure database environments, or support other parties who will configure those environments, for Functional Qualification Testing (FQT), regression testing, Independent Test & Evaluation (IT&E), user acceptance testing, integration testing, database security testing, installation/migration testing, configuration/compatibility testing, and performance, load, and stress testing, as requested.
5. Support the migration of databases from the non-production to the production environment, as well as migrations of applications and databases between data centers, as requested.
6. Provide technical assistance to infrastructure stakeholders to resolve failures or address network related issues, and support incident management and problem management activities.
7. Coordinate OS upgrades, patches, fixes, and testing with data center staff.
8. Monitor application usage and storage, and provide advance warning when thresholds are reached. Provide advice and implementation support to address application high availability issues and requirements.
9. Perform periodic database clean-up and maintenance of training environments in support of end-user training classes.

Each application’s administrative requirements are different (administrative actions needed will change with time as the application and organization change). *Table 4: Typical Administrative Functions* describes application and database administration functions at a general level.

1. Typical Administrative Functions

|  |  |  |
| --- | --- | --- |
| **Function** | **Frequency** | **Description** |
| Account management | As required | Complete and process access requests (e.g., user profiles/preferences, password reset) for systems and applications. |
| Monitor logs and alerts | Daily | Monitor system event logs,  application event logs, and monitoring tool alerts. |
| System Performance Monitoring | Daily | Monitor systems CPU, memory, disk, network utilization, and other key performance indicators prescribed by the application. |
| System maintenance activities | Daily | Move or clear logs, daily backups, or  other activities required to continue daily operations. |
| Patch management | Monthly | Identify required patches, download and test, coordinate installation. |
| System updates | As required | Identify and recommend required  configuration changes, deployment updates, plan and schedule update  activities, test updates, coordinate installation. |
| Troubleshooting support | As required | Provide research and corrective  actions for event logs, alerts, or  incidents that indicate a system loss  or degradation of function. |
| User account and organization hierarchy | As required | Add new user meta-data, update existing users’ meta-data, Management, create/update DOS locations/sites, create/update user positions,  update user responsibilities, etc. |
| Monitor logs and alerts | Daily | Monitor system event logs,  application event logs, and monitoring tool alerts. |
| System Performance Monitoring | Daily | Monitor systems CPU, memory, disk, network utilization, and other key performance indicators  prescribed by the application. |
| System maintenance activities | Daily | Move or clear logs, daily backups, or other activities required to continue daily operations. |
| System updates, configuration changes, deployments | As required | Identify and recommend required updates, plan and schedule update activities, test updates, coordinate installation. |
| Troubleshooting support | As required | Provide research and corrective actions for event logs, alerts, or incidents that indicate a system loss or degradation of function. |
| User account and organization hierarchy management | As required | Add new user meta-data, update existing users’ meta-data, create/update DOS locations/sites,  create/update user positions,  update user responsibilities, etc. |

* + 1. Coordination and Collaboration

The Government requires coordination and collaboration, which will allow all parties to work closely with the Government IRM-PM and business owners to create, groom, develop, design, prioritize, and test user stories that will serve as the foundation for the work to be performed. The IRM-PM in concert with the business owner provides guidance on the vision, requirements and priority of work and validates those tasks meet the acceptance criteria. The IRM-PM provides technical oversight in concert with the Contracting Officer’s Representative (COR) who provides contractual oversight. The IRM-PM will coordinate upcoming workload with the COR for administration with the Contractor’s PM to ensure workload direction is in line with intent and scope of task orders and tasks. Any contractual terms, conditions, scope and adjustments are only permitted from the Contracting Officer (CO). The CO shall be involved if/when there is disagreement amongst Evolve contractors and/or other parties within the task order.

* + 1. Quality Control/Validation and Verification

Quality control involves ensuring fit-for-purpose and fit-for-use of all IT solutions produced. To enable this, it is expected that the quality control team function at CMMI maturity level of 3 or higher in their production and management of validation and verification processes and artifacts to include, but not limited to: test planning, test coverage, functional testing, automated regression testing, load/performance testing, logging defects discovered during DME testing, recording test results and recommending appropriate actions according to those results.

Members of the quality control team are expected to actively participate in quality management and process definition activities for maturing and enhancing quality control services.

* + 1. Integration and Testing

The Contractor shall:

1. Perform activities associated with ensuring all individual program components configured with or added to the applications environment work together properly as a single system performing all of the intended functions.
2. Perform all appropriate life-cycle integration and in-house development tests (e.g., unit testing, end-to-end testing, stress testing, regression testing, and 508 compliance testing).
3. Perform selective random independent testing, where the random selection includes some complex modules.
4. Meet with testers (and application stakeholders as needed) to review test results.
5. Support user acceptance and assurance testing, baseline acceptance testing, and related Information Assurance and Assessment and Authorization (A&A) testing.
6. Develop database scripts to provide data used for testing.
7. Document systems architectures, components, and interfaces.
8. Monitor, protect and cleanse data used for testing.
9. Perform all appropriate issue tracking and management functions in support of lifecycle integration and in-house development tests.
10. Stage systems before implementation.
11. Perform modifications and performance enhancement adjustments to system software and utilities as a result of test and integration results.
12. Develop and review required documentation for the Integration and Testing Process in accordance with MSP IT methodology. Documentation will vary based on development methodology.
13. Conduct bandwidth and network performance testing in conjunction with network team to ensure acceptable performance of applications across the wide area network.
14. Review results of bandwidth and network performance testing in conjunction with network team to ensure acceptable performance of applications across the wide area network.
15. Document all processes utilized in the successful execution of integration and testing activities.
    * 1. System Testing

The Contractor shall:

1. Perform automated and manual testing to assess the quality of systems compared to requirements.
2. Support functional, performance, and technical testing in a lab-like setting (environment which as closely as possible mirrors production) and provide any necessary testing services for stakeholders.
3. Develop test methodologies, test plans, and test scripts to perform new and regression tests for supported applications.
4. Perform rigorous testing using industry standard best practices.
5. Maintain a repeatable regression test process, ensure existing test scripts are up to date with current system functionality, convert defect fix tests into repeatable regression test scripts as needed, and ensure regression tests reflect real world conditions including changes to business requirements and DOS IT infrastructure.
6. Consult with developers, business subject matter experts, and observe DOS documentation to ensure that testing fully and accurately assesses requirements.
7. Conduct requirements mapping to ensure the suite of tests provide full coverage of all requirements.
8. Produce a Security Test and Evaluation (ST&E) Plan to account for information security issues.
9. Interface with other DOS bureaus and IRM offices to support the coordination of testing dependencies between supported applications and DOS enterprise applications and infrastructure.
10. Assist in requirements analysis, use-case analysis, design and development of new features and bug fixes for supported systems.
11. Assist in reviewing and documenting system designs, implementation plans, system maintenance, and test plans.
12. Maintain a suite of automated testing tools to ensure the toolsets are current and that test scripts and other testing data is properly backed up and can be restored from back up media if needed.
13. Document all processes utilized in the successful execution of integration and testing activities.
    * 1. Defect Tracking

The Contractor shall:

1. Implement and maintain a documented and structured defect tracking, reporting methodology and process that encompasses all stages of the SDLC including requirements definition, design and analysis, programming, and testing (including regression testing) for all in-scope software being supported by the Contractor.
2. Include all levels of source code developed/supported by the Contractor including the unit, module, and system-level code in the defect tracking and reporting methodology.
3. Leverage the defect tracking and reporting methodology to optimize the identification and resolution of application defects prior to production release.
4. Capture and manage defects in the designated system. Team Foundation Server, Azure DevOps, the DOS enterprise ITSM system (e.g., ServiceNow) and GITHUB are used to manage defects and statuses. This list is subject to change at any time.
5. Use defect management to ensure the Contractor delivers database physical and logical environment structures, metadata configurable parameters, and data content, as well as compiled object code to DOS for system-level testing that is compliant with the systems specifications as approved by DOS, including all applicable Section 508 constraints, and that the code does not contain any Severity 1 defects and minimal Severity 2 defects.
6. Severity 1 is defined as a defect that affects critical functionality or data and does not have a work around.
7. Severity 2 is defined as a defect that affects major functionality or data but does have a workaround that is not obvious and is difficult.
8. Incorporate the following components into defect tracking methodology:
9. Defect tracking repository
10. Identification and documentation
11. Communication / escalation process
12. Prioritization scheme
13. Evaluation and analysis
14. Resolution and verification testing (including regression testing where appropriate)
15. Reporting (defect density, defect age, defect trend) by type / priority
    * 1. Test, Integration and Deployment

The Contractor shall:

1. Be responsible for creating test cases, automated test scripts to support test automation activities, and thoroughly testing the code.
2. Collaborate with other teams to support test-driven development and continuous code integration.
3. Share test scripts (manual and automated) as needed with other testing entities.
4. Work to increase the code coverage, the degree to which the source code of a program is executed when a particular test suite runs, and quality, as specified by government leadership.
5. Perform alpha and beta testing.
6. Assist with constructing validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.
7. Support the activities of the Integration and Configuration team to ensure the automatic build and deployment process works effectively across all environments, including the contractor’s development/test enclave. Deployment and testing in the development/test environment should mimic closely the actions performed for deployment and testing in staging and production.
8. Thoroughly test changes and remediate all known security issues before committing them into the CI/CD pipeline.
9. Use their DevSecOps personnel to perform deployments of some or all code directly to production, as directed by the Government.
10. Not depend on independent inspections to achieve quality and security.
    * 1. Continuous Integration/Continuous Delivery (CI/CD)

The Contractor shall:

1. Create DOS-specific transition plans that encompass business process, operations (business and IT), and technology support plans that need to be in place to mitigate implementation risk.
2. Create DOS-specific system and user documentation, including any changes to policies or procedures, as needed to supplement software and hardware vendor documentation and provided in coordination with site-specific end user training activities
3. Create problem management processes for testing and implementation/ migration.
4. Create clearly defined, efficient procedures for distribution and installation of changes.
5. Create execution and back-up plans as approved by DOS.
6. Create operational procedures for interim and final implementation stages and cutover.
7. Create business continuity/disaster recovery plans and procedures to achieve continuity requirements. Plan shall include plans for data, backups, storage management, and contingency operations.
8. Create end-user and technical documentation on the use of application-specific tool sets and development methods.
9. Create business process support documentation and associated business rules
10. Create communications documents, presentations, and training documents associated with full operational use of the implemented application.
11. Create technical documentation and materials related to test environment management, change control management, and performance tuning.
12. Create, maintain, and update maintenance schedules and maintenance reports that include, but are not limited to, software version and installation location and patches applied.
13. Provide electronic documentation that clearly and sufficiently details that all applicable Section 508 constraints have been appropriately met, and separate electronic documentation that provides DOS verification and validation/acceptance and sign-off with regard to Section 508 constraints.
    * 1. Operations and Maintenance Documentation

The Contractor shall:

1. Respond to production incidents, including but not limited to breakages of functionality, system outages, performance problems, security incidents, or user complaints. This responsibility includes, but is not limited to, investigating and triaging incidents, rolling systems back to earlier states, developing and deploying fixes (on software they may or may not have developed), engaging with other contractors and federal employees to fix related systems, and running incident retrospectives to ensure permanent fixes.
2. Be responsible for the operation in production of the capabilities they develop.
3. Build monitoring triggers to effectively reveal production issues in a timely fashion.
4. Provide root cause analysis on all outages with actionable recommendations on how to prevent issues going forward.
5. Ensure streamlined operations to make processes more efficient.
6. Build application health monitoring and alerting functions into the system, to ensure system is monitored effectively, to reveal any production issues, when they happen.
7. Ensure that the system is monitored to reveal user analytics and interactions and provide the capability to automatically report on such activities.
8. Ensure that there is an automated way to monitor for dependency and network-related production issues, providing the capability to rule out application issues.
9. Continuously refine and improve every process, while simultaneously reducing the likelihood of major outages.
   * 1. Monitoring and Reporting

The Contractor shall:

1. Provide monitoring and reporting services pertaining to ongoing health checks, status reporting, and problem management (ongoing surveillance, tracking, escalation, resolution, and tracking of problems) for development and support activities.
2. Prepare and submit all reports in a form and format acceptable to DOS and ensure they are Section 508 accessible throughout the duration of the contract. Report types include, but are not limited to project schedule status reports, operational efficiency reports, error/defect/problem detection/resolution reports, and release planning reports. All reports shall include the project title, number, user agency, and description of work performed (indicating which project tasks are being billed for).
3. Support the Project Manager to generate, provide, maintain, and update from the following types of reports, depending on the individual project:
4. Project plans, identifying critical path dependencies, major critical milestones, status of incorporating Section 508 constraints, and project deliverables.
5. Weekly status reviews and progress reports for selected projects.
6. Project Risk Register –including risk identification, risk mitigation, and reporting.
   * 1. Application Security and Compliance

The Contractor shall:

1. Perform all application and data development activities associated with defining, designing, building, and testing the physical and logical security of the application development processes, application development source code, data and data stores, all aspects of the development environment, and all application development tools and components (hardware and software) according to all applicable federal laws (e.g., FISMA, The Privacy Act of 1974) and security industry standards and best practices (e.g., NIST, CERT, SANS, etc.).
2. Use application security development best practices as a fundamental component of application development and maintenance methodology that encompasses the following security design rules:
3. Alignment to the DOS enterprise architecture plans, policies and strategies
4. Circular A-11 Part 7 Guidance on Exhibit 300 – Planning, Budgeting, Acquisition, and Management of IT Capital Assets – to include IT Dashboard, Earned Value, Operational Analysis, Integrated Baseline Reviews Incorporate security as part of the design
5. Assume a hostile environment
6. Use open standards as much as possible
7. Perform proper input validation
8. Minimize and protect trusted system elements
9. Encrypt and protect data at the source (i.e., in process, transit, and storage)
10. Limit access to need-to-know
11. Authenticate following HSPD-12 directives and guidelines
12. Do not subvert in-place security protections
13. Fail Securely
14. Log, Monitor, Audit
15. Validate use of accurate system date and time
16. All processes utilized in the successful execution of IT security activities shall be documented
17. Implement and integrate with DOS IT security and compliance policies, procedures, and documentation pertaining to the ALM services for which the Contractor has responsibility. At a minimum, these policies, procedures, and documentation requirements shall address IT security and compliance operations, administration, and governance services, and IT security for the applications and application platforms as it relates to the DOS mission requirements.
18. Ensure that appropriate IT controls, reporting, and documentation are in place for all ALM Services for which the Contractor has responsibility. Applicable standards include but are not limited to:
19. Data Center Consolidation
20. Federal Information Security Modernization Act (FISMA) of 2014
21. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)
22. The Privacy Act of 1974
23. Homeland Security Presidential Directive 12 (HSPD-12)
24. Identity, Credential and Access Management (ICAM)
25. OMB Ipv6 Memo
26. The 25 Point Implementation Plan to Reform Federal Information Technology Management – to include Cloud First, Shared Services, and TechStats
27. Section 508 (29 U.S.C. 794d; 36 CFR 1194)
28. Monitor all work performed by assigned Contractor personnel to ensure the ongoing and continuous incorporation of all appropriate IT Security and Compliance requirements.
29. Implement all required safeguards for securing and managing the security of the systems and IT environments it uses for work on DOS projects.
30. Comply with all certification and accreditation requirements and documentation specified by DOS and the U.S. Government. In support of this monitoring.
31. Provide cyber security support and risk management for the information systems owned or maintained by each office.
32. Continually monitor and report iPost (DOS’s method for continuous risk monitoring) findings and scores for information systems owned or supported by each office to minimize information security risks.
33. Coordinate with Project Managers to collaborate and develop security documentation for all systems within each office and maintain an up to date central repository.
34. Ensure systems meet all security requirements.
    * 1. Training Development and Support

The Contractor shall:

1. Provide end-users and end-user organizations with the necessary knowledge, skills, tools and capabilities to operate the specific IT solutions produced by the Program Office and in the governance structures underpinning the IT solutions.
2. Provide training services to include, but not limited to: needs analysis, curriculum design and development, knowledge article/user guide editing, training planning, training execution, and evaluation.
3. Have members of the training team actively participate in quality management and process definition activities for maturing and enhancing training services.
4. Support developed training services associated with the improvement of skills through initial and continued education and instruction for IRM developed applications/systems, including data management and data integration products and services. Delivery methods the Contractor is required to offer for training include instructor-led (virtual or live) and computer-based instruction.
5. Develop or secure and provide any training related documentation (e.g. on-line help, etc.) and coordinate with the Foreign Service Institute (FSI) in the delivery of end user training.
6. Coordinate and manage all technical and operational training on custom or COTS products, including training facilities, materials, equipment, environments, instructors, scheduling, delivery, and tracking. Stakeholders include, but are not limited to, agency users, supervisors, help desk support, technical, operational, and training personnel.
7. Provide milestone-specific knowledge transfer related to products developed or configured under this task order, as required, with clear deliverables for each set of activities.
8. Conduct all training in consideration of Section 508 constraints.
   * 1. Big Data Analytics

The Contractor shall:

1. Provide support for the collecting, aggregating, extracting, transforming, integrating, maintaining, and operating of databases which bring together historical and near-real time data from disparate sources into a format that is conducive to accurate and reliable analysis for the purpose of reporting from historical, aggregated, trended, and forecasted perspectives.
2. Provide support for developing and maintaining reports and dashboards. Reports may be standard, recurring, parameter driven, drillable, web based, etc.
3. Support ad hoc reporting for some customers.
4. Assist with deriving customer reporting requirements. Current BI tools include but not limited to: SAP Business Objects, the DOS enterprise ITSM system (e.g., ServiceNow) Microsoft PowerBI and Informatica. This list is subject to change at any time.
   * 1. Cloud Computing

The Contractor shall:

1. Implement and maintain administrative, technical, and physical safeguards and controls for multiple cloud computing models, with the security level and services required in accordance with DOS FAM/FAH cloud computing policies as well as Federal Risk and Authorization Management Program (FedRAMP) standards. Current cloud computing services include, but are not limited to: MS O365 (including SharePoint Online, Dynamics Online, PowerBI, OneDrive, PowerApps, Forms, and Flow), Amazon Web Services, and Microsoft Azure. This list is subject to change at any time.
   * 1. Other

The following list provides the type of support that is required, broken into the following task areas:

1. Legacy System Integration: Achieve end-to-end digital workflow processing.
2. Architecture: Continuously improve and evolve the product architecture, user experience, Agile development, and DevSecOps practices. Establishing consistent and effective use of cloud-based environments and modernizing some of the legacy applications.
3. Innovation: Review, experiment with, and potentially adopt different technologies, tools, practices, processes, and techniques in order to drive innovation and facilitate continuous delivery, continuous feedback, continuous improvement, and encourage rapid and flexible response to change.
4. Solution Delivery: 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.
5. Analytics: Provide capability for USCIS 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.
6. Artificial Intelligence (AI) and Machine Learning (ML): 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.
7. Legacy O&M: Continue to sustain current capabilities and maintain the current existing applications Service Oriented Architecture (SOA) Services.
8. Cross-Functional Collaboration: 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.
9. User Story Collaboration: Work with the product owner, product manager end users and requirements analysts to refine and groom user stories.
10. User Centered Design: Work with the product owner, product manager and agile resources to design application solutions to include user research, experience design, and service design.
11. Code Development: Use a modern technology stack to define, author, and deliver application code that conforms to requirements and application architecture provided by the government. This includes but is not limited to customizing Commercial Off-The-Shelf (COTS) products for Same government use, developing, executing, and reporting on unit testing, and performing and documenting software code peer reviews. The contractors are expected to discover and reuse existing code, along with making newly developed code reusable on other government projects.
12. Automated Testing: 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.
13. Data Migration: Develop and execute data migration strategies and plans.
14. Deployment Activities: Plan, create and validate the implementation and deployment of scripts for use during application deployment and provide release planning and management support.
15. DevSecOps: Work collaboratively and cross functionally with engineering and operations to implement continuous integration, continuous delivery, production monitoring, and production support. The contractor will support its own code, while in production.
16. Configuration Management and Change Control: Support effective and efficient configuration management and change control to support the agile development processes.
17. User Training: Provide user-centered, task-based training to users in support of system deployment.
18. Metrics Reporting: Develop and communicate project metrics. Metrics may include but are not limited to dashboards, Agile burn down charts, release roadmaps, and schedule.
19. Production Support: Provide primary support during 8AM – 6PM EST. For after hours, contractors are expected to provide on call support with a primary and backup team member. Contractors must respond within 60 min to acknowledge interruption in production systems, provide available information and steps being taken as well as provide status updates every 2 hours until issue is resolved. The contractors shall provide a report detailing issues, analysis and recommendations to avoid or prevent future occurrence within 2 days of resolution. The contractors shall ensure that automatic monitoring of system status is created and maintained for each system. The contractors shall work with OIT to ensure the appropriate stakeholders receive automated alerts on system status. The on-call support responsibilities include responding to production emergencies (outages) and critical issues. Operational support should be centralized within two teams to allow for Tier 2 and Tier 3 operational support and ticket queue management. The centralized support model is needed due to the volume of tickets received for these applications. There is one primary queue manager for all application covered under these task orders, who ensures tickets are assigned to the correct teams.
20. Scaled Agile Practices: Conduct program increment planning following mature Agile practices.
    1. Task Area 2: Systems Operations and Maintenance
       1. IT Service Management (Change, Configuration, Release, Incident, Problem)

The contractor shall perform IT service management in accordance with ITIL best practices, including but not limited to those defined here.

* + - 1. Change Management

The contractor shall:

1. Develop, implement, update, and monitor Change Management processes in accordance with governance processes for submitting and reviewing changes to defined IT services and systems to reduce risk to the enterprise, coordinate with affected customers, and de-conflict change schedules.
2. Use a holistic approach in developing the Change Management processes and methodologies to ensure that both the technical and non-technical aspects of a Change Request are taken into consideration in planning the introduction of new or previously approved software, hardware, and policy, and/or procedural changes.
3. Ensure Change Management processes and activities are inter-related and complementary with Release Management and Configuration Management processes.
4. Collaborate with all other support teams which are directly affected or impacted by the results of the Change Management activities, such as governing bodies and stakeholders.
5. Document and maintain Standard Operating Procedures and Processes as they pertain to Change Management.
6. Submit and process Change Requests for all systems covered in this document.
7. Organize and facilitate Change Management meetings as required, including preparing reports, agendas, writing meeting minutes, and documenting outcomes from Change Request reviews.
8. Coordinate with external boards and organizations, such as the ITCCB and ICAB.
9. Provide subject matter expertise and administrative support for Change Management initiatives.
10. Maintain Change Management records in the DOS enterprise ITSM system (e.g., ServiceNow), and provide support for the configuration and customization of the tool (as applicable) to better align with IRM procedures.
    * + 1. Asset and Configuration Management

The contractor shall:

1. Improve design and fully populate an Inventory Maintenance System with pertinent purchase order information including renewal and expiration dates, user information and ownership for all hardware and software items and applications. The Contractor shall update and maintain DOS application inventory in a Section 508 accessible softcopy format and/or an electronic system such as iMatrix.
2. Provide System Configuration Management Services including the identification and maintenance of system components and the relationships and dependencies among them.
3. Establish a Configuration Management Plan for all tasks and maintain the Configuration Management Database (CMDB); perform monitoring, auditing, and reporting all configuration items for data integrity.
4. Capture and store application-to-component and component-to-component relationships.
5. Maintain the history of those relationships and transformations required to appropriately manage and document (e.g., source control, version control, profiles, IA plans) configuration changes affecting the application and its processing environment.
6. Record configuration items and applicable technical artifacts in the designated Configuration Management system to maintain the integrity of the products throughout the lifecycle.
7. Create configuration baselines and periodically meet to review proposed baseline changes and adjudicate trouble reports prior to the submission of change request.
8. Support the releases and associated changes to authorized baselines.
9. Support Enterprise IT Change Control Board (ITCCB) Requirements.
10. Follow Department policies and procedures for configuration management (described in greater detail in 5 FAM 115.6-1, 5 FAM 651 and the ITCCB Standard Operating Procedures).
11. Ensure that IT products (commercial software, software applications and hardware) are described clearly to the enterprise Change Control Board; and meet enterprise standards for accessibility, antivirus interoperability, cost effectiveness, data management and protection, deployment, encryption, license management, network impact and support requirements, patch management, privacy, remote access, redundancy, security, source management, user and administrator training, and version control well in advance of deployment. Such registration is congruent with and not instead of approval from the relevant IRM office.
12. Evaluate and make recommendations based on such product descriptions, which will determine to what extent the product(s) can be deployed on DOS networks. Failure to properly baseline products prior to deployment is identified in DOS security policy as a significant security violation and may be cause for remedial action.
13. Perform activities to appropriately manage and document changes to the application(s) and any of the constituent components being developed or modified. This requires management and documentation of changes to the underlying application development environment components, as well as the application source code base. The Contractor shall perform the following activities in support of Software Configuration Management Services:
14. Library Management—the classification, control and storage of the physical components of an application.
15. Version Control—the maintenance, tracking and auditing of modifications to an application’s components over time, facilitating the restoration of an application to prior development stages.
16. Turnover Management—the automated promotion of software changes across different phases of the life cycle (e.g., development, unit test, systems test and production), including management of the approval process, production turnover and software migration control.
17. Support to the IT Configuration Control Board (ITCCB) – a group of stakeholders responsible for planning for, authorizing, and managing technical change across the enterprise (e.g. A&A, 508 Compliance, Cybersecurity, and GAP).
    * + 1. Release Management

The contractor shall:

1. Develop, implement, update, and monitor Release Management processes and policies for implementing approved changes to defined IT services, both the software and the hardware.
2. Use a holistic approach in developing the Release Management processes and methodologies to ensure that both the technical and non-technical aspects of a Release are taken into consideration in planning the introduction of approved software, hardware, and policy, and/or procedural changes.
3. Ensure Release Management processes and activities are inter-related and complementary with the Change Management process, as well as Configuration Management and Problem Management.
4. Collaborate with all other support teams which are directly affected or impacted by the results of the Release Management activities, such as governing bodies and stakeholders including Change Management, Configuration Management, Problem Management, Service Desk, Testing, Production operations, and other pertinent IT support groups, to address support interdependencies and incorporate appropriate linkages and dependencies into the Release Management processes.
5. Address and operate in accordance with DOS Enterprise Release Management procedures at a minimum.
6. Ensure systems are upgraded, maintained, and installed with minimal disruption to users and business processes.
7. Leverage and enforce the use of DevSecOps practices to the maximum extent practical.
8. Recommend Release Management policies, procedures, processes, and training requirements per the Release Management process components outlined above.
9. Establish, manage, update, and maintain the overall Release Plan and Release Schedule for all planned Releases.
10. Establish and administer the version control schema as it relates to Release Management of DOS custom applications.
11. Develop, manage, update and maintain formal Release Plans for each Release in coordination with Change Management.
12. Develop quality plans and back-out plans as appropriate for each Release.
13. Provide Release Management Plans and Schedules including resource levels to DOS for review.
14. Conduct site surveys, as necessary, to assess existing hardware and software being used to validate Release package requirements and dependencies.
15. Ensure that any new software, hardware, or support services required for the release are procured by DOS and available when needed.
16. Ensure that all necessary testing environments are available and properly configured to support Release testing.
17. Ensure there is segregation of duties between the application developer testers and the release management testers.
18. Conduct User Acceptance Testing (UAT) as required.
19. Schedule and conduct Release Management meetings to include review of planned releases and results of changes made.
20. Identify and document all Configuration Items (CIs) that need to be included in the Release, as well as all system inter-dependencies.
21. Provide Release documentation as required.
22. Reviews Release Management details and alter as appropriate to meet the needs of DOS (e.g., back out plan, go/no go decision).
23. Notify DOS affected clients of Release timing and impact and provide communications to the service desk.
24. Implement Release in compliance with Change Management requirements and adherence to detailed release plans.
25. Modify configuration database, asset management items, and service catalog (if applicable) to reflect changes to Cis due to the Release.
26. Conduct post-mortem of Releases that necessitated implementation of the back-out plan and develop and implement appropriate corrective or follow-up actions to minimize future occurrences.
27. Provide DOS Release Management reports as required and defined by DOS.
28. Establish, document, support and maintain local Change Control Boards (CCBs) with appropriate stakeholders, as required, for defect tracking, reporting, decisions and release planning.
    * + 1. Incident Management

The contractor shall:

1. Support DOS in developing and establishing Incident Management policies, processes, and procedures that support DOS’s Incident Management requirements and document them in the Standard Process and Procedures Manual.
2. Implement and comply with DOS-defined and –specified incident management Priority classification processes and prioritization schemas.
3. Respond to and closely coordinate incident resolution and ongoing resolution status of all support requests escalated to Contractor by the DOS IT Service Center (ITSC).
4. Support the DOS IT Service Center in accurately recording, updating, and closing Incident Management system records and capturing the resolution actions and knowledge in the DOS’s IT knowledge management database, which are used to record, update, track, monitor, and report status on incident resolution progress and related resolution disposition.
5. Provide unrestricted read access by the DOS-authorized staff and other Government and third party personnel to all current and historical Contractor-maintained Incident records and knowledgebase data and read/write access for a limited number of DOS-authorized personnel.
6. Monitor the server and storage system and Incident Management system for automatically generated and logged Incident alerts and events.
7. Resolve incidents on the first occurrence of escalated incident notification or automated alerts in accordance with the Procedures Manual, knowledge database documents, configuration database(s), and performance requirements.
8. Provide accurate and timely incident status resolution progress status updates to the DOS ITSC.
9. Identify and classify incidents to a priority level and handle in accordance with documented Incident response procedures.
10. Diagnose and resolve incidents and where possible, implement appropriate corrective actions for known errors (e.g., workarounds for known unresolved problems).
11. Escalate incidents to the appropriate next-level service group within Contractor, DOS, or third-party IT service provider as soon as it is clear that the incident is unable to be resolved without additional assistance or as required to comply with service level response times.
12. Coordinate resolution of escalated incidents with the DOS IT Service Center, as well as designated DOS personnel and any third parties involved in troubleshooting and resolving an incident.
13. Monitor and track incident resolution progress through to final closure and record/update incident record status as appropriate.
14. Provide expert technical, functional, and process knowledge and resolution assistance as requested, for resolving incidents related to any in-scope DOS IT environment applications and systems at Level 2 or Level 3 resource, as required.
15. Provide Tier 2 assistance to inquiries on the features, functions, and usage of DOS IT environment applications and systems solutions.
16. Provide training and Tier 1 scripts for the DOS IT Service Center for initial diagnosis and identification of incidents.
17. Verify that all records (e.g., inventory, asset and configuration management records) are accurately and timely updated to reflect completed / resolved incidents.
18. Assist with questions relating to functionality and use of in-scope DOS solution hardware and software.
19. Document solutions to resolved incidents in a/the central knowledgebase. Accurately update all information pertinent to trouble ticket, including general verbiage, codes, etc.
20. Notify designated DOS personnel of all Priority 1 and Priority 2 incidents within the designated timeframe (priority 1 is 2 hours and priority 2 is 24 hours).
21. Maintain current and historical records of all incident support request calls and the resolution of those calls for the life of the contract and provide reporting and trend capabilities.
22. Troubleshoot, diagnose and resolve incidents for all in-scope hardware and software devices (both in warranty and non-warranty), including removing and replacing, or repairing physically broken or inoperable devices.
23. Provide and manage, in coordination with the DOS IT Service Center, the end-to-end incident identification, recording, diagnosis, escalation, trouble ticket tracking and updating, resolution, documentation, and closure for all incidents, including supporting those tickets escalated to third parties, in compliance with Service Level Agreement (SLA) requirements.
24. Determine, whenever possible, whether a problem ticket should be opened to address an incident (especially for automatically generated alerts).
25. Track ongoing status of any incident and their corresponding problem record to ensure that identified problems are addressed and resolved in accordance with IRM’s customers’ SLA requirements.
26. Ensure incident resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual.
27. Coordinate and manage resolution for Contractor ITSM-specific incidents with the Government and all necessary or involved third parties (e.g., public carriers, Internet service providers, other third party IT service providers).
28. Review the status of open, unresolved Incidents and related problems and the progress being made in addressing problems.
29. Participate in Incident Management review sessions and provide listing and status of same categorized by incident Priority impact.
30. Coordinate with the DOS IT Service Center on the close-out and resolution documentation for incidents that were resolved satisfactorily.
31. Provide Incident Management reporting as required.
32. Coordinate with the Government and third-party Level 2 support groups to acquire and transfer knowledge on incident and problem resolutions and record this knowledge gained into the knowledge base to facilitate increased ability for the Level 1 DOS IT Service Center in providing first-call resolution.
33. Coordinate with all appropriate DOS and IT service provider, Service Delivery and Service Support groups (e.g., Change Management, Release Management, maintenance technicians, other help desks, etc.) in planning and managing all scheduled / planned system outages.
34. Obtain all appropriate DOS authorizations and validate that notices have been distributed prior to performing any maintenance activities requiring a planned system outage.
35. Coordinate with the DOS IT Service Center in communications to the DOS and end users regarding upcoming planned prescheduled outages.
    * + 1. Problem Management

The contractor shall:

1. Develop and implement appropriate processes, procedures, and methodologies that support DOS-approved Problem Management requirements that include:
   1. Problem Detection
   2. Problem logging
   3. Problem categorization
   4. Problem prioritization
   5. Problem investigation and diagnosis
   6. Workarounds
   7. Raising known error records
   8. Problem resolution
   9. Problem closure
   10. Performing major problem review
2. Maintain and update Problem Management records in a/the DOS-specified Problem Management knowledgebase where information about Problems, Root Cause, Known Errors, Workarounds and problem resolution actions are recorded and tracked (this knowledgebase may be the same knowledgebase as used for Incident Management).
3. Provide unrestricted access by DOS-authorized staff and other DOS designated personnel to all current and historical Problem Management records and knowledgebase data.
4. Perform all Problem Management activities in conformance with defined Change Management procedures set forth in the Procedures Manual.
5. Coordinate Problem Management activities of all problems (e.g., detection, logging, root-cause analysis,) with appropriate Incident Management teams.
6. Coordinate, escalate and track Problem Management activities within DOS and third parties related to problems determined to reside in the IRM applications.
7. Flag all Priority 1 and Priority 2 incidents that require further root-cause analysis to be conducted.
8. Ensure recurring problems that meet defined criteria related to the Contractor’s responsibility area are reviewed using root-cause analysis procedures.
9. Work directly with DOS and third-party personnel to ensure that proactive trend analysis is being performed on incidents, problems, and other data elements to identify recurring situations and points of failure.
10. Coordinate and monitor status of root-cause analysis activities performed by DOS and other third party IT service providers.
11. Monitor processes for documenting and updating Problem Management knowledgebase with information regarding problem resolution actions, activities, and status (e.g., root cause, known errors, workarounds,) and notify all appropriate parties of availability of information.
12. Coordinate with DOS, IT service providers and other third-parties, as required, to ensure that IT knowledge pertaining to Problems related to other IT service areas are captured and entered into the common Problem Management knowledgebase accessible by all personnel authorized by DOS.
13. Ensure problem resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual.
14. Provide status reports detailing the root cause and procedure for correcting recurring Problems and Priority 1 and Priority 2 Incidents until closure as determined by DOS.
15. Conduct Problem Management review meetings and provide listing and status of same categorized by problem impact.
16. Periodically review the state of open incidents and related problems and the progress being made in addressing Problems.
17. Create Request for Change (RFC) documentation with recommended corrective actions to be taken to resolve a problem and submit to Change Management for review and approval.
18. Conduct periodic problem management proactive review sessions.
19. Provide Problem Management reporting as required.
    * 1. Application Environments
         1. Environment Support

The contractor shall:

1. Provide routine and emergency system administrative support on all production servers used to support applications under the purview of the associated Offices. The goal is to ensure the confidentiality, availability, integrity, and security of the servers.
2. Support the physical and virtual servers whether on-premises or in the cloud, and the supporting infrastructure such as the F5 load balancers and Data Domain devices in support of these servers.
3. Manage the Active Directory (AD) infrastructure on all relevant domains on all production networks.
4. Ensure compliance with the Office of Diplomatic Security (DS) security configuration standards from acceptance of new servers through patch management of existing servers to final disposition of data on servers.
5. Manage service account passwords, replication, overseeing management of audit change logs and production software backups, as well as server performance monitoring and alerting, server health monitoring and alerting, anti-virus updates, and mitigation of iPost findings.
6. Ensure compliance with the E-CISO, Cybersecurity Operations and Office of Diplomatic Security standards.
7. Ensure adherence to customer service level agreements (SLAs) and provide documentation for supported systems.
8. Work with Customer Technical Support in conducting Test Restore Drills.
   * + 1. Production Environment- Enterprise Messaging

The contractor shall:

1. Manage the Department’s Organizational Messaging environments for all Department locations and supported end users, including overseas posts, domestic sites, and remote work force personnel. The specific activities include, but are not limited to the following:
   1. Maintain SMART functionality and services, including legacy systems;
   2. Maintain eRecords transport and archive storage functionality and services;
   3. Maintain TSM functionality and services;
   4. Support Organizational Messaging interfaces;
   5. Provide remote access capabilities to unclassified Organizational Messaging Services;
   6. Provide secure mail (diplomatic cables) including encryption and authentication;
   7. Maintain audit trails;
   8. Provide a single point of contact (postmaster) for administering cable services, including managing errors in cable processing/distribution;
   9. Support end user SMART accounts and other Organizational Messaging Accounts (currently there are approximately 29,000 user accounts on ClassNet and 59,000 user accounts on OpenNet).
   10. Maintain enterprise CDS functionality and services.
       1. Deployment Support

The Contractor shall:

1. Develop, implement, update, and monitor system deployment processes to provide new applications and/or application upgrades to Department users worldwide.
2. Ensure system deployment processes and activities are inter-related and complementary with Release Management.
3. Develop deployment plans, including schedules, approaches, team composition, milestones, quality assurance assessments, etc. to deploy a range of messaging and desktop applications both domestically and overseas.
4. Analyze product needs and recommend deployment methodologies tailored to needs of post, bureau, administrators, and end users (e.g., training, communications, user-impact).
5. Assess the technical feasibility and technical, organizational, and adoption risks of packaging deployments.
6. Provide structured business practices, high quality customer service, and technical support domestically, abroad, and with external agencies as required. Overseas deployments are in-scope and typically requires 1-2 contracts SMEs to support.
7. Implement changes to deployment plans, methods, schedules, etc. based on feedback from beta usability (including Section 508 considerations) and pilot groups.
8. Facilitate change management efforts and reasonable level of expectations for the customer.
9. Provide direct deployment assistance where feasible and necessary to administrators, users, POCs, or VIPs, as needed.
10. Provide technical expertise to system administrators and users in at Post and in domestic bureaus and offices.
11. Serve as principal IRM liaison with post and bureau administrators for site surveys, software deployment.
12. Provide for seamless transition to O&M capability at deployment’s conclusion.
13. Recommend Deployment Methodology (on-site/remote), and Type (HW/SW/Mixed).
14. Develop a monitoring approach to assess the status of deployments and provide management status reports including deployment issues and corrective action.
15. Implement software deployment in accordance with DOS standards.
16. Provide written feedback from users to assist with maintaining a knowledge base of support procedures, lessons learned, and/or trouble reports or system defect reports.
17. Ensure all site-specific requirements and preparation have been completed and built into the schedule.
18. Ensure DevOps practices involving the use of scripted, pipeline automated, and containerized deployments are used to the maximum extent possible.
    * 1. Code Maintenance

Code maintenance tasks involve changes to software code, whether the codecode is modified by the Contractor directly or through third party vendors, such as for COTS upgrades. Maintenance may arise based on needs of IRM and business stakeholders. Code maintenance activities are categorized as corrective, adaptive, or relevance, as described below:

* **Corrective Maintenance:** Correct software failures, performance failures, and implementation failures that result from design errors, logic errors, and coding errors.
* **The Adaptive Maintenance:** Upgrade or convert the application because of changes in the operating environment. The term environment refers to all the conditions and influences which act from outside upon the application, such as business rule, Government policies, legislative changes, work patterns, or software and hardware platform changes.
* **Relevance Maintenance:** Accommodate new or changed user requirements or to increase the application performance or enhance its user interface.

The Contractor shall submit artifact deliverable items required by DoS as specified by DOS to the DOS electronic document library and/or to other recipients as directed. The Contractors shall comply with a standard and accessible change control process in accordance with DOS policy. A change is an addition, modification, or removal of approved, supported, or baseline hardware, network, software, application, system, image, or associated documentation. The Contractor shall:

1. Perform the full suite of code maintenance tasks using Agile methodologies, including, but not limited to participating in creating user stories for both business functionality, technical requirements and defining acceptance criteria; estimating the size of stories; solution design; development; and testing.
2. Collaborate with stakeholders, support Contractors, and third-party vendors throughout system integration, performance, security, Section 508, system acceptance, user acceptance, usability, and test and evaluation reporting.
3. Document each aspect of the development process, report outcomes and forecasts, document developing epics, user story features, release trains and other agile artifacts.
4. Work with stakeholders to analyze data, complexity, and risks to ensure identification during the planning process. The Contractors will gather project requirements and will meet stakeholder expectations and present task risk assessments associated with each project.
5. Create change requests as required and submit them to the Government for approval.
6. Develop fully commented executable code and other artifacts against the user stories documented in this task or as assigned by the Government.
7. Develop code that does not add new technical debt to a release; the Contractors shall correct any defects identified by testers, code reviewers, automated tools, or as part of the CI/CD activities etc.
8. Deliver fully commented executable code and code revisions that follow Agile industry best practices, to include version control, automated builds, automated testing, and continuous integration.
9. Produce output that conforms to the architecture and standards provided by the Government and the Agile processes set up by the DOS team. This will include providing input to any documentation required to maintain compliance with DOS standards, as specified by DOS.
10. Produce code that meets the functional and non-functional requirements, meets database development requirements, and is deployable and fully tested in preparation for DOS Independent Validation & Verification (IV&V) review.
11. Perform database and application software upgrades and migrations.
12. For code maintenance test and integration:
13. Create test cases and automated test scripts to support test automation activities.
14. Collaborate with other teams to support continuous code integration.
15. Share test scripts (manual and automated) as needed with other testing entities.
16. Assist with crafting validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.
17. Support the activities of the integration and configuration team to ensure the automatic build and deployment process works effectively across all environments, including the Contractors’ dev/test enclave. Deployment and testing in the dev/test environment should mimic closely the actions performed for deployment and testing in staging and production.
18. Perform development testing before the commit stage in the continuous integration pipeline
19. Support DOS Application Maintenance activities associated with resolving, repairing, and preventing the occurrence of errors and defects in new or existing applications and logical databases; providing technical support services for configuring and tuning the configurable elements of the applications to achieve optimal application system performance; and installing application service patches, version upgrades, minor enhancements, and API codes extensions in accordance with this document.
20. Operate and maintain in-scope production servers, on classified and unclassified networks on a 24x7x365 basis. Example: For enterprise messaging there are approximately 300 virtual and on-prem servers across the OpenNet, ClassNet, and TSNet production servers.
    * + 1. Enterprise Messaging Maintenance (Operations and Management)

The contractor shall:

1. Operate and maintain all Organizational Messaging production servers, on classified and unclassified networks on a 24x7x365 basis, currently there are approximately 300 virtual and on-prem servers across the OpenNet, ClassNet, and TSNet production servers, including:
   1. Updating and patching servers
   2. Monitoring and remediating server problems using tools such as NetIQ and/or SCOM
   3. Performing password resets at 60 day intervals
2. Upgrade Organizational Messaging systems with vendor released patches and minor upgrades in accordance with Department change management processes.
3. Adjust Organizational Messaging system capacity to meet demand requirements.
4. Monitor all Organizational Messaging queues for outstanding alarms, reject messages and traffic on specific line queues (on average there are approximately 311 operational alerts on ClassNet and 152 on OpenNet).
5. Monitor and react to Information Transport Service (ITS) messages using the ITS dashboard.
6. Monitor and address status of SMART Search and SharePoint search.
7. Repair broken hyperlinks for SMART and archive messages.
8. Filter and disseminate cables and activate rulesets for all discrete posts (currently there are, approximately 1,054 discrete posts on ClassNet and 1,035 discrete posts on OpenNet).
9. Conduct research on and manage inbound/outbound organizational messages from/to other agencies to include SMART Portal, ITS, OAC, and TSM identifying and correcting any problems with traffic flow or processing of individual messages.
10. Manage delivery and receipt of TSM message traffic.
11. Perform Top Secret message delivery format conversions to include, but not limited to conversions between TSM and SAMS-R lines and conversions from ACP-127 format to Extended Electronic Delivery System (EEDS) format for the Bureau of Intelligence and Research (INR).
12. Configure split channel/diversion on SAMS product suite.
13. Clear routing table traffic loop conditions.
14. Manage routing tables, divert tables, and system tables to include change, delete, and modifying tables, to include maintaining line parameters, routing indicators (RI), and queue associations.
15. Establish and configure alternate routes (altroutes) due to circuit problems.
16. Coordinate circuit issues with local maintenance groups and distant end operations and engineers for circuit outage resolutions.
17. Escalate and document procedures for all anomalies to management, bureau, and affected agencies.
18. Manage alert and response activities for High Precedence (e.g. CRITIC, FLASH, NIACT) traffic.
19. Manage and respond to spill and reject queues, including:
20. Respond to message spills that are not processed due to anti-virus rejects
21. Manage CLOUT spills that need to be corrected and entered into the SMART network for processing
22. Provide Reasonable Human Review (RHR) support for all spilled message traffic from the CDS system to ensure messages will not compromise security before releasing to classified and unclassified enclaves
23. Address various Spill and Reject Queues to include SMART, CLOUT, and ITS
24. Address spills and rejects on SAMS-MFI (ClassNet only – on average, there are approximately 30 a month)
25. Address Spill Queues (on average, there are approximately 1,766 a month on ClassNet, 205 a month on OpenNet)
26. Address eRecords data transport spills and rejections (OpenNet and ClassNet);
27. Manage and respond to messaging failures, including:
28. Manage and correct SMART message archive failures – e.g. system was unable to successfully PDF message (on average, there are approximately 216 a month on ClassNet and 18 a month on OpenNet)
29. Address cross-enclave message failures (on average, there are approximately 45 a month on ClassNet and 35 a month on OpenNet) and send-to-self problems (OpenNet only)
30. Address domestic No-Hits (on average, there are approximately 1,100 a month on ClassNet and 105 a month on OpenNet)
31. Address eRecords message archive failures (OpenNet and ClassNet);
32. Address Service Queues, including:
33. Address SMART to SMART (S2S) Service Queues (on average, there are approximately 44 a month on ClassNet, 189 a month on OpenNet)
34. Address Analyst Queues
35. Address NDR Queues and alerts;
36. Address results from Kibana reports
37. Address Organizational Messaging Inquiries, including:
38. Address policy-related inquires
39. Address S2S related inquires
40. Address routine customer issues
41. Address eRecords customer inquiries;
42. Address other Organizational Messaging queues, including:
43. Address Message Section Queue (ClassNet only – on average, there are approximately 780 a month)
44. Address Service Message Desk Queue (Classnet only – on average, there are approximately 1,200 a month)
45. Address Analyst Queues (on average, there are approximately 33 a month on ClassNet, 61 a month on OpenNet)
46. Address non-delivery receipts (NDR) Queues (on average, there are approximately 589 a month on ClassNet, 231 a month on OpenNet);
47. Complete and deliver shift operations report to the Messaging Communication Office, at shift changes.
48. Coordinate circuit issues with local maintenance groups, vendors, and distant end locations for connections traversing MSO controlled space.
49. Coordinate cryptographic support with local maintenance groups and distant end locations and perform operational COMSEC functions.
50. Provide enterprise CDS support for all rejected, quarantined, spilled, and failed files from the enterprise CDS system to ensure files will not compromise security or violate DOS policy before releasing to classified or unclassified enclaves. Support will be via the CDS RHR or CDS Dashboards.
51. Provide support for Cyber Incident Response Team (CIRT) spill cleanup on OpenNet and ClassNet, as directed by Diplomatic Service incident tickets.
    * + 1. Email & Microsoft Teams (or designated platform) Services (Operations and Management)

The contractor shall:

1. Manage and support all Email and Microsoft Teams (or designated platform)& Services, including classified and unclassified systems, keeping the services stable, high performing, and secure.
2. operate, maintain, and monitor all components of the services and interfaces with other services and systems.
3. fulfill service requests, respond to incidents, and resolve problems related to these services.
4. provide engineering services to optimize capacity, availability, performance, stability, security, and usability of the services and underlying systems to meet evolving Department requirements.
5. maintain service and system documentation and knowledge base materials.
6. assist the system owner and Information Systems Security Officer (ISSO) in the Authorization and Assessment (A&A) process.
7. follow and participate in standard Information Technology Infrastructure Library (ITIL) best practices to maintain the services, including maintaining ISO20000 Certification.
8. Manage DOS Email and Microsoft Teams (or designated platform) environments for all DOS locations and supported end users, including overseas posts, domestic sites, and remote work force personnel. The specific activities include, but are not limited to the following:
9. Operate and Maintain all production Microsoft Exchange servers for classified and unclassified environments (approximately 100)
10. Administer Exchange Online and Microsoft Teams in the M365 Government Community Cloud
11. Support messaging functionality and services accessed through Department approved software solutions, such as Microsoft Outlook, Microsoft Outlook Web Access, and the Global OpenNet (GO) Remote Access clients
12. Provide email, Calendar, Scheduling, Contacts, and Tasks services across all supported services
13. Provide instant messaging service on classified and unclassified networks, including OpenNet and ClassNet (synchronized with Active Directory and/or other directories as necessary)
14. Interface between Messaging and Web Conferencing
15. Enable remote access to email
16. Provide “Push Mail” and “Pull Mail” service for sending and receiving emails
17. Support secure mail through encryption and authentication
18. Enable mass mailing
19. Provide distribution list capabilities for both manual and auto-populated lists;
20. Maintain audit trails of activity and provide reports as needed
21. Maintain a subscriber database with all information required by the Department and Microsoft Exchange;
22. Perform email and attachment virus scanning, policy management, encryption, and authentication;
23. Support Anti-Virus and Anti-SPAM programs designed and developed by IRM and DS security teams
24. Administer email services, including managing errors in email processing
25. Enable personal and shared mailboxes, calendars, and task lists
26. Enable meeting scheduling via Microsoft Outlook, Teamsand other integrated applications
27. Maintain the Department’s Global Address List (GAL)
28. Support end-user mailboxes, including service requests
29. Administer and support audio/video conferencing in Microsoft Teams
30. Administer and support Microsoft Teams Phone Service
31. Integrate approved applications and services with Microsoft Outlook and Teams clients
32. Operate and maintain the on-premises Microsoft Exchange Services. The specific activities include, but are not limited to by the following:
33. Remediate security vulnerabilities
34. Upgrade systems with vendor released patches and minor upgrades in accordance with Department change management processes
35. Adjust capacity to meet demand requirements
36. Modify configuration to accommodate changes to underpinning support services (e.g., changes to directory services, supporting platform architecture, hosting datacenter, etc.
37. Conduct regular compliance and system health checks
38. Monitor and analyze email traffic and performance data to proactively identify performance issues (incidents or problems) and to plan for future capacity needs
39. Recommend and implement enhancements to improve availability and operations
40. Create role-based policies in coordination with Active Directory and other directors, as required
41. Develop server, application, and device monitoring rules and solutions
42. Manage, maintain, and troubleshoot email server and application technology infrastructure
43. Maintenance activities for all production servers, currently 28 OpenNet and 80 ClassNet production servers on a 24x7x365 basis, including:
    * 1. Update and patch email servers
      2. Provide server verifications
      3. Provide technical documentation and artifacts
44. Support Hybrid Office 365 implementation and coexistence with on-premises Exchange
45. Support all Department email-enabled accounts and mailboxes, currently there are approximately:
    * 1. 140,000 mailboxes on OpenNet
      2. 52,000 mailboxes on ClassNet
46. Perform deployment activities to include Build/Configure/Test/Deploy email servers (approximately 40/year)
47. Respond to Tier 2 and Tier 3 Microsoft Exchange escalations
48. Perform Incident Management on a 24/7/365 basis
49. Utilize Microsoft SCOM or other tool to proactively monitor on-premises server health
50. Identify and Resolve Problems through a proactive Problem Management program
51. Provide Reason for Outage (RFO) reports as required after Incidents
52. Perform Email and Microsoft Teams Service Request Management by responding to and resolving service requests in accordance with Department policies and procedures for a global user community on a 24/7/265 basis. Approximately 25,000 Service Requests per year.
53. Perform supplementary engineering and technical support activities to make incremental improvements to supported services and technologies. The specific activities include, but are not limited to the following:
54. Facilitate the transition to Cloud-based services on OpenNet and ClassNet when available
55. Support the integration of new Cloud services with existing Email and Microsoft Teams services
56. Design and implement improvements to on-premises Exchange server and application technology infrastructure
57. Design and document infrastructure changes and perform required enhancements
58. Perform server or appliance builds, application installations, and configurations
59. Create and maintain all build guides, technical drawings and schematics and test plans in conjunction with the quality assurance team
60. Create and or modify scripts, programmatic enhancements and upgrades, web server infrastructure implementations and enhancements
61. Perform necessary research, development, and testing/validation (in lab environment) prior to transitioning the product to production
62. Assist lab management with configuration similarity between production and lab environments by alerting lab management to production system changes and making necessary lab adjustments
63. Operate and maintain test environments, including servers and supporting IT infrastructure
64. Assist with and execute engineering and operational plans and revise as appropriate to meet changing needs/requirements, and communicate/enforce standards
65. Maintain close communication with Program Office, senior technical lead and/or project manager, so that all are well informed of status of all Email & Instant Messaging Engineering efforts
66. Work well within a diverse technical team, contributing consistently and with excellence
67. Comply with and support Department change management policies
68. Comply with and support Managing State Projects for Information Technology (MSP-IT) and iSchedule methodologies and requirements
    * 1. Technical Support

The Contractor shall:

1. Provide expert technical assistance required for the tuning of applications and logical databases for optimal system performance. These services include:
   1. Expert Tier 2/Tier 3 technical assistance for end-users and IT professionals.
   2. Documentation and maintenance of Repair and Maintenance policies and procedures.
   3. Maintenance of application maintenance plan or operations guide.
   4. Technical and functional support to application development for centralized and distributed systems.
   5. Technical and functional support for stakeholder groups, both domestically and at posts worldwide.
   6. Notification of appropriate offices of changes and upgrades to third party application systems.
   7. Diagnostics on software and services.
   8. Release packaging of software changes.
   9. Support for regular Assessment and Authorization (A&A) requirements.
   10. Assist Enterprise IT Service Center with coordination of user support activities.
   11. Respond to escalated trouble ticket items in accordance with established procedures.
   12. Routine system management on applications and logical databases.
2. Perform centralized Tier 2 and Tier 3 incident functions as assigned by the Enterprise IT Service Center for DOS applications listed in the Scope of this document using the DOS enterprise ITSM system (e.g., ServiceNow). Tier 1 will be performed by the respective DOS Enterprise IT Service Center Contractor.
3. Provide Tier 2 and Tier 3 (Tier 3 support generally provided by a developer) support 24x7x365.
4. For Tier 2 support, receive all tickets from the IT Service Center and provide basic support on application software and/or hardware issues.
5. For Tier 3 support, provide code-related support and platform support on complex application system software issues.
   * + 1. Enterprise Messaging

The contractor shall perform supplementary engineering and technical support activities to make incremental improvements to Organizational Messaging Services. The specific activities include, but are not limited to the following:

1. Utilize enterprise architecture standards to support engineering design, prototyping, and integration, activities including, but not limited to: SMART, eRecords, CfA, FOIAExpress
2. Coordinate implementation of technical support for system modifications or deployments of new systems
3. Ensure proper design, review, control, implementation, and documentation of equipment design changes
4. Provide engineering support for non-Messaging circuit and server functions hosted in MSO space
5. Provide engineering support for Microsoft and Unix-based operating systems, supporting messaging operations
6. Engineering support of TSNet network environment
7. Perform necessary research, development, and testing/validation (in lab environment) prior to transitioning the product to production
8. Assist lab management with configuration similarity between production and lab environments by alerting lab management to production system changes and making necessary lab adjustments
9. Operate and maintain test environments, including servers and supporting IT infrastructure
10. Assist with and execute engineering and operational plans and revise as appropriate to meet changing needs/requirements, and communicate/enforce standards
11. Modify configuration to accommodate changes to underpinning support services (e.g., changes to directory services, supporting platform architecture, hosting datacenter, etc.)
12. Recommend and implement enhancements to improve availability and operations;
13. Comply with and support Department change management policies and procedures as specified in section 4.3.1 Change Management
14. Comply with and support MSP-IT and iSchedule methodologies and requirements as specified in section 4.6 Service Improvement and Engineering Support
15. Provide engineering services to optimize capacity, availability, performance, stability, security, and usability of the services and underlying systems to meet evolving Department requirements.
16. Provide backup support to the Messaging Communications Officers during time of shortages or emergencies as follows:
    1. Provide direct communications support to State Operations Center and 7th Floor Principal Offices
    2. MCO Shift Narrative: Make applicable entries
    3. Monitor, Manage and take Action SMART MSMC Admin Queues:
       1. High Precedence
       2. Spills
       3. MCO Inbound
       4. MCO Outbound
       5. Message Tracking
       6. S2S Service Desk
    4. Format Messages: For Transmission via SMART
       1. Organizational Message (Cable)
       2. Message Directly Addressed (MDA)
       3. For The Record (FTR)
    5. Handle SMART Messages including Captioned Traffic and ALDACs:
       1. Release
       2. Correct
       3. Recall
       4. Kill
       5. Forward
       6. Copy
    6. Update TSM Report Logs
    7. Traffic Restriction List: Print for posting within MSMC
    8. Maintain Field and Department SMART Collectives
    9. Phone Calls/E-mails: Manage and monitor shared mailbox for MCO action (escalate or redirect requests when needed)
       1. Messaging Comm Officer
       2. MSMC Help Desk
       3. SMART Operations
    10. Create, Update, Resolve incidents and service request received from ServiceNow
    11. Non-pro Courier:
    12. Provide escort upon arrival/departure
        1. Ensure pouch is received by MCO
        2. Ensure required documents are signed and received by MCO
        3. (1) Completed copies for filing in the MCO
        4. (2) Completed copies for delivery to HST classified pouching facility
        5. during normal business hours
        6. Update report in SharePoint
        7. Operations and Maintenance Monitoring and Reporting

The Contractor shall:

1. Provide monitoring and reporting services pertaining to ongoing health checks, status reporting, and problem management (ongoing surveillance, tracking, escalation, resolution, and tracking of problems) for development and support activities.
2. Prepare and submit all reports in a form and format acceptable to DOS and ensure they are Section 508 accessible throughout the duration of the contract. Report types include, but are not limited to, project schedule status reports, operational efficiency reports, error/defect/problem detection/resolution reports, and release planning reports. All reports shall include the project title, number, user agency, and description of work performed (indicating which project tasks are being billed for).
3. Determine, depending on the individual project, which reports will be necessary to generate, provide, maintain, and update from the following types of reports:
   1. Monthly service-level performance reports against each IRM SLA, including trends for each and summary view
   2. Reports that capture service requests demands and measure of ability to satisfy demand
   3. As required, reports that represent general health of environments (e.g., number of stranded transports, patches not yet applied, overall uptime of system servers, services in the laboratory and production environments) as well as reports that represent demand fulfillment in end-customer terms (e.g. defect corrections/change requests that have slipped against commitment, backlogged defects/change requests, Priority 1, 2, and Priority 3 defects)
   4. Monthly rolling analysis reports on the Contractor’s service delivery performance relative to requirements measure and tracked
   5. Service Improvement Plans (SIPs) for any services deemed by DOS as failing to meet service performance requirements
   6. Service Request Response Time management reports (including a trend line) for new testing work that reflects time to provide time and cost estimates
   7. Average Defect Response Time by Priority level
      1. Code Migration

The Contractor shall:

1. Provide Code Migration Services, including activities associated with promoting new and modified code, configuration, and scripts in support of new and existing applications through development, test, and production; where possible this shall be done via automated pipelines using containers or other artifacts to reduce manual intervention and possible migration errors
2. Recommend operations and administration procedures related to code migration.
3. Define test-to-production turnover requirements and instructions for each project or release.
4. Report on results from test-to-production activities, if applicable.
5. Migrate code amongst enclaves when required and identified in the project planning and requirements steps.
6. Track migration status and notification.
7. Support environment setup and decommissioning for new and changed environments, data, and infrastructure.
8. Migrate correction code.
   * 1. Quality Assurance (QA) / Quality Management (QM)

These quality requirements stand apart from the quality control and validation and verification functions ascribed earlier in this document within the project/DME function of the organization. They relate specifically to the contract quality assurance and quality control plan (how will the contract ensure quality control over the execution of the contract as opposed to the execution of a project).

The Government and Contractor define acceptance of the deliverables as follows:

* Deliverable passes all new automated and manual acceptance tests that were defined before the most recent iteration.
* Deliverable passes all prior automated and manual acceptance tests, verifying that no regression has occurred.
* Deliverable conforms to the “definition of done” that was defined before the iteration.

The Contractor shall:

1. Provide and perform the following Quality Assurance and Quality Management Services and utilize a Quality Management System (QMS) framework that provides a standard, formal, and consistently applied approach for quality management, including quality requirements and criteria, key IT processes and their sequence and interaction, and the policies, criteria and methods for defining, detecting, correcting and preventing non-conformity and potential quality gaps.
2. Establish, maintain, and update a QA and QM documentation repository where all QA and QM records, reports, and plans are stored and provide DOS free and open access to the repository at all times.
3. Identify, implement, and maintain standards, policies, processes, and practices for key IT processes to guide the organization in meeting the intent of the QMS.
4. Develop and implement QA Process Implementation Plan.
5. Develop definitions and lists of the steps to be taken to ensure configuration control is maintained.
6. Perform QA auditing of compliance of its services with designated standards, processes, and procedures.
7. Develop and document QA and QM process, work product, and service management refinement and improvement recommendations and implementation plans.
8. Implement all approved QA and QM refinement and improvement recommendations and plans in a manner that is transparent to Government and its end-users.
9. Identify and communicate any noncompliance QA or QM issues and ensure that actions are taken to resolve or correct those issues.
10. Create QA and QM Compliance Reports and Communication Plans.
11. Distribute Communication Plans and QA and QM reports to Government managers and all other appropriate parties.
    * 1. Customer Engagement

The Contractor shall:

1. Demonstrate expertise in the area of cost optimization for both on-premise and cloud environments. The Contractor shall establishment and support governance and processes for cost optimization.
2. Establish and monitor service agreements for on-premise IT services and cloud services.
3. Monitor customer consumption and utilization, produce showback/chargeback statements, and establish/update agreements and memos for on-premise and cloud services.
4. Provide support for creating and monitoring Service Agreements per the DOS 5 FAM 150 Service Agreements and the 5 FAH-11 Exhibit H-822.4(1) the Interconnection Security Agreement. The Agreements to which relevant Program Offices are a party, pertain to services, or involve systems and networks for which an in-scope Program Office is the information system owner, domestically and abroad.
5. Provide subject matter expertise and administrative support for Agreements initiatives.
6. Maintain and provide support for Agreements Tracker tool (as applicable) to better align with IRM.
7. Monitor and analyze customer consumption and utilization for on-premise and cloud IT Services in order to provide showback/chargeback or analyze on Department IT costs.
8. Demonstrate expertise with business intelligence tools and produce trending reports and support capacity planning efforts that can be used to assist DOS and customers in maximizing compute and storage for on-premise and cloud IT services.
9. Maintain Service Agreements and customer showback/chargeback in a document repository.
10. Coordinate with the Budget Office to process customer reimbursements/transfers.
    1. Task Area 3: Innovation

The Contractor shall:

1. Provide research and development activities on an as-needed basis. Multiple activities, efforts or projects may fall under this task and run concurrently. Each project will be scoped, scheduled, funded and managed separately.
2. Provide appropriate skill level and quantity of staff needed for each project. All reporting, documentation of findings and status are required and provided for Government review and acceptance based on the schedule and agreements. The activities include but not restricted to: IT research, whitepapers, analysis of products and/or solutions, proof-of-concept, prototyping, software development, software configuration, testing, analysis of alternatives and lifecycle cost estimating.
3. When requested by the DOS, identify and designate individual(s) expertly qualified to address IT technology and service delivery subject areas related to:
   1. New products/technology
   2. IT service performance
   3. Solutions architecture
   4. IT application security management
   5. Standards, process management, and quality assurance management
   6. Cloud Computing
   7. Transition management
   8. IT applications training
   9. Customer outreach efforts in promoting and communicating major system changes to the field
   10. Other IT-related subject areas where the DOS deems it lacks appropriate skills and proficiency
4. (Subject matter experts) Meet with the DOS to develop and make recommendations on potential courses of action and develop actionable plans to address DOS-approved course(s) of action.
5. Build Proof of Concepts (POCs), prototypes, or pilot systems to test design ideas and assumptions. The main purpose of developing a POC is to demonstrate the functionality and to verify a certain concept or theory that can be achieved in development. Prototypes and pilots will be a working interactive model of the end products that demonstrate the design, navigation, and layout. The outcome of prototype tasks will show how the target solution will be developed.
   1. Task Area 4: Cross-Functional Requirements

The following table summarizes the Cross-Functional categories that all contractors are required to support in all task orders.

1. Cross Functional Requirements

| Requirements Category | Description |
| --- | --- |
| 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.). |
| Client Management | Resources or “account managers” aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects. |
| 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. |

* + 1. Compliance
       1. IT Compliance

IT Compliance resources includes 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.
   * + 1. 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>
  + 1. 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.

* + - 1. 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.

* + - 1. 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), 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 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.

* + 1. Disaster Recovery

Disaster Recovery services are the services and activities required to prevent and/or respond to a disaster event through the restoration of key computing functions as swiftly and smoothly as possible. A “disaster event” in this context is any event that prevents a mission-critical system from maintaining an operational state at the client production data center.

The Contractor shall:

1. Design, maintain, update, and enhance IRM’s business continuity for all applications developed or supported by the vendor detailed in Continuity of Operations Plan (COOP) and demonstrated Disaster Recovery (DR) capability to maintain the same level of operational support and ensure that the alternative capability meets SLAs and COOP guidelines.
2. Coordinate the involvement of all Vendor and third-party resources managed by the Vendor in the development, maintenance, testing, and execution of the disaster recovery and COOP plan.
3. Develop, evaluate, and maintain a Disaster Recovery Plan IAW IRM COOP and NIST SP 800-34 and review and update annually.
4. Ensure changes are accurately reflected in Continuity of Operations Plan (COOP) and Disaster Recovery (DR) as necessary.
5. Develop, maintain, test, and support disaster preparedness, high availability, and recovery procedures in accordance with the IRM hosted server environment.
6. Provide a single point-of-contact upon the declaration of a Disaster to coordinate with DOS or their designee and all appropriate third parties
   * 1. Client Management

Resources or “account managers” aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects.

The Contractor shall:

1. Designate a single point of contact to liase directly with the Program Offices utilizing services delivered via this Task Order
   * 1. 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). This task order provides specific ITSM activities for application development in PWS Section 2.2.1.

* + 1. Product and Project Management

The contractor shall provide Product and Project Management services as it relates to the work performed under this task order. Product and project management include all activities relating to the eight project performance domains identified as critical for effectively delivering project outcomes in the PMBOK® Guide (i.e., stakeholders, team, development approach and lifecycle, planning, project work, delivery, measurement, and uncertainty) and spans the full range of development approaches (agile, hybrid, predictive).

The Contractor shall perform the following task order project management activities:

1. Manage projects utilizing sound project and product management practices (i.e., Managing State Projects (MSP), Project Management Body of Knowledge (PMBOK®), and adhere to the program, project, and product lifecycle processes and standards developed by the offices.
2. Tailor the project management approach, governance, and processes to best suit the project environment. This includes selecting the approach (i.e. agile, predictive) or combination of approaches (hybrid) that is most appropriate for the unique characteristics of the project. The approach selected should consider balancing competing demands including, but not limited to, the following items:
3. Speed to delivery
4. Minimizing project costs
5. Optimizing value delivered
6. Quality of deliverables or outcomes
7. Adhering to standards
8. Satisfying stakeholder expectations; and
9. Adapting to change
10. Organize and manage project team(s) into a cohesive unit to achieve mission goals and performance objectives, ensuring teams have the necessary skills to execute project activities utilizing the selected development approach for the effort
11. For agile project delivery:
    1. Be responsible for development teams performing the full suite of development tasks using Agile methodologies, including, but not limited to participating in creating user stories for both business functionality, technical requirements and defining acceptance criteria; estimating the size of stories; solution design; development; and testing
    2. Assist in the documentation of user stories, acceptance criteria and tasks to be completed to fulfill the definition of done for a story
12. Organize, conduct, and attend meetings
13. Collaborate with other vendors supporting the Evolve Contract and the ITS Division, to include but not limited to providing requested inputs to support internal data calls and Office of Management and Budget (OMB) reporting requirements, provide updates to project and portfolio management tools, such as ServiceNow PPM to monitor project schedules, weekly project status, etc.
14. Ensure communication is thorough, accurate, and timely to both stakeholders as well as the customer. Maintain full and open communications with the DOS COR and the Government Technical Monitors (GTM) on all matters
15. Develop, document, update, and maintain overall project artifacts in accordance with MSP-IT framework and GTM requirements
16. Develop, document, update, and maintain overall project schedules using DOS specified tools, which at a minimum includes Microsoft
17. Adhere to baselined project schedules and formally request changes to those baselines when applicable, through existing and established project review processes and/or boards
18. Identify issues and risks to project success, develop a risk management tracking log and log all identified issues / risks, along with issue/risk mitigation recommendations / plans, and facilitate
19. Provide other project management support services as required. Support and meet all established control gates, documentation, and deadlines as required by the Project Review Board (PRB), eGoveGov PMO,, IRM Executive Committee/Steering Committee.
20. Document all processes utilized in the successful execution of project management activities
21. Use the DOS designated repositories for all deliverables as required
    * 1. 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:

1. Supply value engineering reports as needed.
2. Provide the most cost effective, efficient, state-of-the-art, integrated turnkey solutions while incorporating practical innovations and technologies.
3. Determine and develop best practice processes by building upon ones already in place at IRM to improve operational efficiency.
4. Identify, develop, and advance the IRM vision and strategic plan to reform IT acquisitions by bringing industry standard best practices and driving innovations.
5. Ensure IRM remains current with evolving requirements and technology advances.
6. Special Requirements/Instructions
   1. 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.

* 1. Government-Furnished Equipment / Information

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).

* 1. Intellectual Property Rights

The software developed as the result of the task orders of the contract are the property of the US government. This provision excludes any open-source or proprietary tools/code that were used that were developed outside of the scope of this contract.

The source code and associated documentation shall also belong to the US government, including the right to use or modify it as seen fit.

In the event of contract termination, the US government shall own whatever code has been completed thus far.

Any materials created during the development, such as wireframes, designs or plans shall be the property of the US government and are subject to the non-disclosure section of this document.

At the same time, the development company may only reassign the rights to the property that they created. If any, they will remain public.

* 1. 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

* 1. Period of Performance

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

Base Year:

Option Year 1:

Option Year 2

Option Year 3:

Option Year 4:

* 1. 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.

* 1. 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.

* 1. 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.

* 1. Organizational Conflict of Interest (OCI)

**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).

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.

**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.

**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.

**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.

**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.

* 1. 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** |
|  |  |  |
|  |  |  |

* 1. Travel

In performance of this task order, occasional travel to other locations may be required. Travel is receipt reimbursable and in accordance with the Joint Travel Regulation. Travel related expenses should be in accordance with contract clause B.7.

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.

* 1. Other Direct Costs

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

* 1. Funding

This task order will be incrementally funded.

1. Task Order Management

TO management is 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.

* 1. 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. Key Personnel

| Labor Category | Description | |
| --- | --- | --- |
| Task Order Program Manager | | Acts as a single technical point of contract (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:**   * Be ultimately responsible for ensuring the Contractor’s performance meets all task order requirements. * Have the requisite authority for full control over all company resources necessary for task order performance; * Have the authority to approve task order modifications in emergent situations; and * Be ultimately responsible for personnel management, management of Government material and assets, and personnel and facility security. * Demonstrate progressive IT experience in the functional area of the task order of 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.   Additional minimum qualifications for the PM include:   * 10 years of experience * Bachelor of Science (BS) degree in Information Technology (with a preference for Master’s degree in Business Administration (MBA) or Information Technology) * ITIL Certified, or equivalent * PMP Certified (current), or equivalent |

* + 1. 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).
   1. Meetings/Conferences
      1. 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 PAC convened by the Government, onsite or virtual, within 30 days after task order award;

Introduce key personnel during the PAC 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)
  1. 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.
9. Schedule of Deliverables

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Deliverable | Section Reference | Due Date | Update Frequency | Distribution |
| Associated Contractor Agreement | 3.10 | 30 days after every new task order award and updated as applicable | As needed | Evolve Program Manager |
| Statement of Full Operational Capability | 4.4.2 | Upon completion of the Transition period |  |  |
| Meetings/Conferences (Meeting notes/action items) | 4.2 | 3 working days after meeting / conference | As required | CO, TO COR, Evolve Program Manager |
| Project Management Plan, to include Quality Control Plan | 4.3.2 | 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 | 4.5.1 | 30 calendar days from award of first task order | One-time | TO CO, TO COR, TO CPM |
| Transition-out Plan | 4.5.3 | 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 |

* + 1. Transition
       1. Transition-In

The contractor shall develop a Phase-In Transition 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, but is not limited to:

* 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.
  + - 1. Full Operational Capability

The contractor shall provide a statement of assumption of Full Operational Capability (FOC) upon completion of the Transition period. The Contractor shall be assuming and following the existing processes and procedures of the prior contractor. At this time, no implementation of new processes or recommendations to standardize or enhance shall occur without GTM approval. The contractor will receive FOC by meeting and demonstrating milestones and deliverables in each of the functional areas below as agreed upon between the contractor and the GTM.

* Systems Development
  + - Design and Development
    - Change Management
    - Quality Management
* Enterprise Service Support
  + - Asset and Configuration Management
    - Release and Deployment Management
    - Service Monitoring and Reporting
    - Customer Service Support
    - Knowledge and Training Management
* Enterprise Service Operations
  + - Infrastructure Management
    - Database Management
    - Security Monitoring and Support
    - Development Network Support
      1. Transition-Out

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, but is not limited to:

* 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.
  + 1. 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.
  + 1. Task Order Monthly Status Reports (MSR)

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.

* 1. Meeting Minutes

Sharing meeting minutes as a record of information shared at the meeting is a guiding principle for the task order.

All formal meetings’ minutes for staff in an organizational unit shall be shared with Office Directors of the organizational unit at a minimum, either via email or, with the Office Director’s concurrence, a shared online repository. If meetings are informal or non-recurring, then requirements for meeting minutes will be determined by the Government staff in the meeting. Meeting minutes may be shared with additional Government personnel as requested by team leads, Government leadership, and COR/COs. Meeting minutes will only be used for evaluating contract staff if that requirement is coordinated with the COR prior to the start of the meeting and should not be used as a primary performance source

1. Performance Requirements
   1. 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.

* 1. Quality Control and Quality Assurance
     1. 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.

* + 1. Quality Assurance

The Government will utilize a number of quality assurance procedures to ensure contractor compliance with this task order. 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

Appendix A: Basic Performance Standards

The contractor shall meet all the requirements listed in this PWS. Specific minimum performance requirements are listed for some tasks. Where specific minimum requirements are not listed, the basic standard is assumed to be an accurate, timely, high-quality product that effectively performs its intended function. The Government may review performance on any and all requirements contained in this PWS. Failure to meet the basic performance standards could result in administrative actions.

Performance Requirements Summary

Program office performance will utilize a combination of operational metrics and customer-facing metrics. The operational metrics are Government-defined metrics, subject to change, that measure day-to-day technical and business value. The customer-facing metrics are the SLAs that IRM has with their customers. The DOS may, for its internal purposes, manage, provide oversight, and assess overall performance of the task order. The Contractor shall recommend and adhere to DOS-approved policies, procedures, measurement and evaluation practices, and monitoring and reporting requirements for managing IT infrastructure components and applications to obtain optimal performance.

The following operational metrics are a set of measurements used to aid in the day-to-day monitoring and management of IT services. These metrics are a living, internal Government framework that is provided by the Government to the Contractor to facilitate clear communication about the Government’s plans with regard to routine oversight and assessment.

1. Performance Requirements Summary Table

| Performance Evaluation Category | Performance Based Metrics | Detailed Descriptions | Program Office Quality Level | |
| --- | --- | --- | --- | --- |
| Target Met | Target Exceeded |
| Task Order  Performance | Business protected  against  violations/  infractions | This measurement is designed to count the number of violations or infractions  committed by the vendor and reported to the service desk, ISSO, or other legitimate authority. “Violations or Infractions” consist of security breaches, as defined in 12 FAM 590 and 12 FAM 550, as well as lack of compliance with the rules of behavior outlined in the annual Security Awareness Training (PS800) provided by the Foreign Service Institute.  Frequency: Monthly  This measurement will be applied throughout the life of the project. | 0 Violations  and Infractions | N/A |
| Task Order  Performance | Timely Hiring of Staff | The contractor replaces departing personnel within 14 days of the employee’s departure | 8-14 days | 0-7 days |
| Task Order  Performance | Turnover Ratio | Contractor shall strive to minimize overall staff attrition and maintain organizational knowledge to the maximum extent possible | 5% monthly staff attrition over last twelve months or life or contract – whichever is less | 2% monthly staff attrition over last twelve months or life or contract – whichever is less |
| Program Management | Project Management Variance (CV & SV) | Percent Cost Variance (CV) and Schedule Variance (SV) at each phase of development  CAPA Control: 14.99% | Control: +/- 5- 10% | Exceed: < 4.99% |
| Program Management | Requirements Artifacts | Planned vs. Actual Delivery of Requirements Artifacts. Excludes Artifacts with valid change record(s).  CAPA Control: > 3 days from Planned | Control: +1-3 days from Planned | Exceed: < 1 days from Planned |
| Program Management | Testing Artifact | Planned vs. Actual Delivery of Testing Artifacts. Excludes Artifacts with valid change record(s).  CAPA Control: > 3 days from Planned | Control: +1-3 days from Planned | Exceed: < 1 days from Planned |
| Systems Development | Design and Development | Average Code Review Checklist form results. The Code Review Checklist will be completed for each promotion of code/solution from Development to Test and Test to Production. The items on the form will be based on Design and Development standards TBD by the Design and Development team.  CAPA Control: > 20% out of compliance | Control: 5-20% out of compliance | Exceed: < 5 % out of compliance |
| Systems Development | Customer Satisfaction | CAPA Control: 1.9 | Control: 2.0-4.6 | > 4.7 |
| Systems Development | Defects introduced to Production | # of Defects introduced to Production per Release  CAPA Control: 5+ | Control: 0 Major or Critical, 1-5 all other Severity | Exceed: 0 |
| Enterprise Service Operations | Assessment and Authorization (A&A) | All A&A activities delivered according to IA quarterly deliverables. This metric will be measured and reported quarterly but applies throughout the life of the project | No more than 1 missed deliverable per quarter | Zero missed deliverables per quarter |
| Enterprise Service Operations | Mean Time Between Failure | Mean Time between Failures (in hours) [unplanned] Defined by an outage caused at the application layer. Time between 2 outages. | >360 hours | >504 hours |
| Enterprise Service Operations | Mean Time to Recovery | Mean Time to Recovery (in minutes) [unplanned]. The average of all recovery times/number of outages. | <65 minutes | <40 minutes |
| Enterprise Service Operations | Hours over Planned Outage | Aggregated hours over quarter exceeding planned scheduled maintenance. Actual amount of hours for maintenance vs. scheduled hours of maintenance. This metric will be measured and reported quarterly. | <4 hours | <2.25 hours |
| Enterprise Service Support | Incident Resolution – High Priority | Percentage of tickets completed within 12 hours for High Priority tickets | >/= 90% (or one with less than 10 tickets) | >93% |
| Enterprise Service Support | Incident Resolution – Routine | Percentage of tickets completed within 24 hours for all ticket categories | >90% | >93% |
| Enterprise Service Support | Incidents Reopened | Percentage of tickets reopened within 24 hours | <5% | <3% |
| Enterprise Service Support | Initial Incident Response | Initial response time from ticket assignment to customer service response | <120 min/ticket  average (2  hours) | <60 min/ticket  average (1  hour) |
| Enterprise Service Operations | iPost Score (OpenNet) | iPost score captured once a week at the CCB and then take the average for the Month. (35 = A) | <22 | <19 |
| Enterprise Service Operations | iPost Score (ClassNet) | iPost score captured once a week at the CCB and then take the average for the Month. (1750 = A+) | <1750 | <875 |