



U.S. Department
of Transportation

**Federal Highway
Administration**

DOT OCIO

Statement of Work

For

Department of Transportation (DOT) Cloud Services

Contract

NOTE TO OUR CUSTOMERS: THIS TEMPLATE MUST BE TAILORED FOR YOUR NEED BY INCLUDING YOUR UNIQUE REQUIREMENTS, QUANTITIES FOR WORKLOAD (HOURS), SPECIFIC SURVEILLANCE TECHNIQUES, ETC. ANY QUESTIONS REGARDING THIS TEMPLATE SHOULD BE ADDRESSED TO THE COR.

1.0 Overview

This is a non-personal services contract to provide IT Services. The Government will not exercise any supervision or control over the contract service providers performing the services herein. Such service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government as defined in this Statement of Work (SOW). The Contractor shall perform to the standards herein.

1.1 Background

Currently, there are several modal workloads that exist in the Amazon Web Services (AWS) East-West Cloud Environment that the Department of Transportation Office of the Chief Information Officer (DOT OCIO) does not have visibility into from oversight, cybersecurity and operational perspectives. In addition, these modal cloud environments, in some cases, do not follow best practices from architectural and security defense in depth standpoints resulting in risks to the respective modes and DOT overall. DOT OCIO seeks to remedy these risks by implementing a robust and secure multi-tenant enterprise cloud environment that is built on DOT enterprise standards and security controls. DOT OCIO will operate and manage this enterprise cloud environment and migrate existing modal AWS workloads under this enterprise cloud environment whereby modal workloads will inherit enterprise standards and controls that results in a secure AWS DOT-wide cloud environment based on current best practices.

1.2 Objectives

For this SOW, the term 'parent/landlord' equates to DOT OCIO while the term 'child/tenant' equates to modes and operating administrations (e.g., FMCSA, FHWA, NHTSA, etc.) within DOT.

- The contractor will provide Amazon Web Services for DOT-wide cloud environments that accomplish the following:
 - One multi-tenant cloud environment will exist in AWS East-West with implemented to achieve 100% fail over redundancies within the primary cloud facility proper, regionally and nationally with appropriate geographic separation in the event of a man-made/human disaster affecting one region. DOT expects to authorize 'moderate' and 'low' FISMA classified workloads to be housed in this cloud environment.
 - The other multi-tenant cloud environment will exist in AWS Government Cloud environment, and associated (or linked) to one commercial account. The AWS Government Cloud environment shall be implemented to achieve 100% fail over redundancies within the primary cloud facility proper, regionally and nationally with appropriate geographic separation in the event of a man-made/human disaster affecting one region. DOT expects to authorize 'high' FISMA classified workloads to be housed in this cloud environment.
 - Both DOT-wide cloud environments will be built on security defense in depth principles adhering to applicable NIST standards to include but not be limited to
 - NIST 800-53 Rev. 4:
 - <https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components>
 - <https://www.nist.gov/cyberframework>
 - https://www.cisecurity.org/benchmark/amazon_web_services/

1.3 Detailed Requirements

Scope

The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, training, training materials, and other items and non-personal services necessary to provide Amazon Web Services.

The scope of the contract includes the provisioning of IT commodities and solutions as defined in FAR 2.101(b) and further clarified in the Clinger-Cohen Act of 1996 within the Federal Government. It includes IT products, IT commodities, software, solutions, cloud services (Managed service, DevOps, CloudOps, SecOps, etc.) and future technologies as defined under the FAR. Where applicable, the Contractor shall provide IT commodities that may be deployed using the models as listed below: Managed Services Model (includes deployment on the Public Cloud): As demonstrated by market conditions and trends over the last 5 years, along with several federal policies such as FedRAMP, the Cloud First Initiative, the 25-point plan and data center consolidation initiatives, the Contractor deploys IT commodities via managed services and the Cloud. Note that Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) capabilities are becoming more commonplace where the commodity service is managed through a Service Level Agreement (SLA) and is based on a subscription model. In addition, under the scope of this contract, the Contractor may provide commodity enabling services that shall ensure the successful operation and sustenance of the IT commodities

The scope of this contract covers all DOT Operating Administrations except FAA and is organized in the nine following major tasks:

- Task 1 – Project Management
- Task 2 – Consumption of AWS Services
- Task 3 - Transition-Out Planning

.

Tasks

General Requirements

- The Contractor shall facilitate a Kick Off meeting
- The Contractor shall prepare and present a Work Plan detailing the proposed schedule and required resources to complete the assigned work.
- The Contractor shall prepare and present a Gap analysis, and Requirements Review.
- The Contractor shall prepare and present Project/Implementation plan
- The Contractor shall prepare Bi-Weekly Project Status Meeting/Reports.
- The Contractor shall prepare for a Contract closeout meeting.

Specific Tasks

The Contractor shall perform the following specific requirements

1. Task 1 – Project Management

For the Project Management subtask, the contractor shall conduct the following activities:

- Project Planning and Scheduling
- Task Management
- Risk Management
- Status Reporting
- Integrated Baseline Management and Control for Scope, Schedule, and Budget
- Quality Management

Subtask 1.1 – Task Kickoff Meeting

1.1.1. The contractor shall facilitate a project kickoff meeting to discuss the tasks and subtasks for this contract with the COR (TO) and invited stakeholders. The kickoff meeting agenda shall include the following: Strategy and methods for meeting the Task Goals and Objectives, handling purchases of software licenses and Other Direct Costs (ODC), Stakeholder Communications including the coordination with Business Milestones and the methods for achieving signoffs and approvals

Subtask 1.2 Task Planning and Scheduling, Subtask Management, Risk Management, Status Reporting, and Communications.

1.1.1. The Contractor shall deliver a Management Plan for the Task. The contractor shall present the draft plan to the Cloud Integrated Project Team for feedback. The contractor shall produce the final plan and shall maintain it under formal change control for the duration of the task. The Task Management Plan shall include the following sections:

Strategy and methods for meeting the Task Goals and Objectives including the Agile Development method

Integrated Baseline Control for the Task Scope, Schedule, and Budget

Risk Management for the Task

Quality Management for the Task Deliverables

Technical and System Architecture Control for Requirements, Design, Technical Decisions, and key Documents

Stakeholder Communications Plan including the critical engagements for Coordination with Business Milestones and the methods for Achieving Signoffs and Approvals

1.1.2. The Contractor shall report status on a weekly basis using a format that is agreed upon by the DOT OCIO Project Manager. The Contractor shall include updates for the status of all work that is currently being performed or that has recently been completed. The contractor shall include issues and new risk items identified during the reporting period into the status reports.

1.1.3. The Contractor shall attend periodic status meetings with the DOT OCIO Project Manager and other DOT OCIO staff. The Contractor shall provide reports from the task leads and Questions-and-Answers (Q&A) support at the status meetings. The Contractor shall include support for risk management discussions, including the results from monitoring defined risks and any new risks.

- 1.1.4. The Contractor shall provide a resource loaded work breakdown structure (WBS) in the current MS Project software version that encompasses milestones, activities, tasks and deliverables for the full duration and scope of the project. Once the federal project manager/contracting officer's representative (COR) approves the baseline WBS, the Contractor shall provide bi-weekly updates against this baseline.

Note: The definition of these activities can be found in the Project Management Institute's Project Management Body of Knowledge (PMBOK) or a best practice guideline provided by the DOT OCIO IT Project Management Office (IT-PMO).

1.3. Subtask 1.3 – Integrated Baseline Management and Control for Scope, Schedule, and Budget

- 1.3.1. For Integrated Baseline Management, the Contractor shall electronically store all documentation including baseline change requests and the baseline change control log. The contractor shall record all proposed, approved, and completed changes in the Baseline Change Control Log.

1.4. Subtask 1.4 – Quality Management

- 1.4.1. For quality management, the contractor shall conduct Quality Assurance and Quality Control activities consistent with the Task Management Plan and appropriate to the project tasks and report results at status meetings.

1.5. Subtask 1.5 – Project Management Project Management

- 1.5.1. The Contractor shall provide government approved key personnel resource(s) to perform the function of the AWS Project Manager and Technical Conversion Project Manager. Project management includes but is not limited to the following six major work streams for: Project Management, Training, Communication, User Help Desk, Requirements Elicitation, and Solution Architecture.

1.6. Subtask 1.6 Project Management for migrating existing AWS instances

- 1.6.1. The Contractor shall meet with stakeholders and key personnel, as identified by the COR to review the tasks, discuss task administration, agree on plans and schedules, and discuss objectives for planned migrations. The Contractor shall reach out to the COR to set up the initial meeting with all pertinent stakeholders in the week prior to the go-live date for the migration(s) working to identify all participants and create an agenda. Once the schedule is finalized, the resource will support the following required tasks:
- 1.6.2. Provide daily management support for project activities related to ongoing development, communications, training, requirements gathering, architecture and Help Desk implementation;
- 1.6.3. Develop input to strategy related to all post-Release tasks with consideration given to all impacted user groups;

- 1.6.4. Attend and facilitate, where requested, required meetings and prepare reports, briefings, schedule updates and agendas for detailed requirements gathering sessions.
- 1.6.5. The Contractor shall attend all meetings, record minutes, provide agendas, and conduct presentations as requested by COR(TO). The Contractor shall use a common collaboration solution such as SharePoint to maintain project documentation.

2 Managed Services/Ordering

1. Scope of Services from Amazon Web Services

The scope of this contract includes all currently existing and, upon announcement, new or enhanced Amazon Web Services (AWS). For Amazon public cloud regions, all AWS services available to commercial customers shall be made available to DOT. For Amazon GovCloud regions, all AWS service available to GovCloud customers shall be made available to DOT. DOT will be solely responsible for controlling Identity and Access Management (IAM) access to all AWS Linked Accounts associated with this contract. The reseller shall provide no restrictions on DOT's ability to acquire Reserved Instances or Spot Instances directly from AWS.

DOT does not initially plan to use Reserved Instances that have been pre-purchased by the reseller to potentially realize increased discounts, but this will be considered in the future if beneficial to DOT and mutually agreeable with the reseller.

2. Pricing Transparency and Price Reduction Pass-through to DOT

Due to the constant downward pricing trend in commercial cloud services driven by new technology and competition, coupled with the absolute minimum level of value-add services requested of the reseller in this SOW, the metered AWS service unit cost paid by DOT under this contract shall never exceed the AWS unit pricing published on the AWS Website that is effective at the time the unit of service is consumed by DOT. The same requirement exists for non-metered AWS services consumed by DOT such as Enterprise support.

The AWS published unit pricing shall never be exceeded under this contract. DOT encourages the reseller to offer discounts that apply to Amazon unit pricing, both at the beginning of the contract, and ideally, subsequently increasing discounts for DOT as the reseller market for AWS becomes more competitive, DOT resource consumption increases under this contract, and the resellers processes for meeting the requirements of the delivery become more refined and efficient.

Since DOT users of information technology are both extremely aware of published pricing and very sensitive about ensuring DOT receives the best possible pricing, the reseller's application of appropriate discounts presents the best opportunity for this contract to be viewed as responsive to Agency needs on an on-going basis and realize steadily increasing use. Further, CSSO will constantly be assessing the dynamic cloud services marketplace on behalf of the DOT user base to ensure this contract remains the best possible vehicle for, cost-wise and other, acquiring AWS services to meet the Agency's very diverse needs.

Additionally, since the reseller will provide consolidated billing services for DOT, discounts associated with volume pricing tiers across applicable usage dimensions shall be passed on to DOT commensurate with each DOT AWS Linked Account's portion of the reseller's consolidated AWS payer account.

Amazon applies current pricing at time of consumption and calculates volume pricing tiers

associated with applicable usage dimensions as part of its standard billing and cost management approach for consolidated billing, so it is envisioned that meeting this requirement will not put an additional administrative burden on the reseller.

Additionally, AWS has been known to make special cost concessions targeted at specific entities/customers using AWS services. It is envisioned that such concessions (e.g., elimination of data transfer out charges, elimination of the minimum \$15,000 monthly cost of Enterprise level support, free AWS resources provided by Amazon to a DOT team or researcher as part of science grant, etc.) may be made available to DOT by AWS through the reseller within the period of this contract). The reseller shall pass on any such cost concessions that may materialize to DOT.

3. Consolidated Billing

The reseller shall provide DOT with consolidated billing services for new AWS Linked Accounts requested and provisioned under this contract. Consolidated billing services and all related capabilities shall be ready for DOT access within five (5) business days of contract award.

Upon request by DOT, the reseller shall also provide consolidated billing services, after transfer of the account, for existing AWS Linked or prior Payer Accounts used by DOT directly or used indirectly by DOT through other arrangements with other resellers, integrators, or federal contractors. Requests to transfer existing AWS Linked or existing Payer Accounts will include coordination by DOT with the existing AWS account owner, including ensuring their approval, cooperation, and involvement in AWS Account transfer steps. Upon provisioning of a new AWS Linked Account for DOT or completing the transfer of an existing AWS Account (associated with DOT use through another arrangement as indicated above) for purposes of the AWS reseller providing consolidated billing services, DOT will be responsible for all subsequent costs incurred within the Account. The reseller shall not discontinue consolidated billing services for a DOT AWS Linked Account within the term of the contract without DOT approval.

The reseller shall provide one or more separate DOT Consolidated Billing Accounts exclusive to managing the payment of DOT AWS Linked Accounts. The reseller shall not manage any non-DOT AWS Linked Accounts within the DOT Consolidated Billing Account. AWS has indicated that resellers have the flexibility to establish separate Consolidated Billing Accounts for customers.

The first situation involves the potential concern that a reseller may have in giving DOT direct access to their Consolidated Billing Account's Billing Reports, including Programmatic Billing Access, since such access may potentially provide DOT with access to the billing data associated with other non-DOT AWS Linked Accounts that are associated with the resellers Consolidated Billing Account. Likewise, DOT's billing data shall similarly never be accessible by a non-DOT Linked or Payer account, nor any other non-DOT entity or individual without an explicit request made in writing by DOT. (The Cloud Management Platforms and Tools that may be used by DOT may have the requirement for a non-DOT AWS Account to have Programmatic Billing Access to DOT consumption and billing data associated with DOT AWS Link Accounts managed for Consolidated Billing Purposes by the reseller. DOT will make explicit requests for such access in writing to the reseller, and the reseller shall enable the access within five business days.)

More information about Programmatic Billing Access and the associated access limitations addressed by the requirement for a separate DOT Consolidated Billing Account can be

found at:

<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/detailed-billing-reports.html>.

The second situation dictating the requirement for a separate DOT-only Consolidated Billing

Account involves the potential for Reserved Instances to be used by non-DOT AWS Linked Accounts associated with a common Consolidated Billing Account. Per Amazon's AWS Website, "For billing purposes, Consolidated Billing treats all the accounts on the consolidated bill as one account. This means that all accounts on a consolidated bill can receive the hourly cost benefit of Amazon EC2 Reserved Instances purchased by any other account." This requirement addresses a similar situation that exists with Amazon Relational Database Service (RDS) Reserved Instances managed within a single multi-customer Consolidated Billing Account.

Further, if the management and use of EC2 and RDS reserved instances across DOT AWS Linked accounts under a single DOT Consolidated Billing Account becomes unmanageable for DOT, or inequitable for DOT users, due to the way Amazon allocates unused reserved instances across multiple DOT AWS linked accounts within a single Consolidated Billing Account, DOT may require additional Consolidated Billing Accounts.

More information about Consolidated Billing and the special rules applied to Reserved Instances can be found at the link below (see Consolidated Billing non-usage Charges Section):

<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidatedbilling.html#consolidated-billing-ec2> .

A minimum of one DOT Consolidated Billing Accounts will be sufficient at contract start. The reseller shall provide additional DOT consolidated Billing Accounts on upon request at no additional charge. However, DOT plans to intentionally minimize both the number of Consolidated Billing Accounts and AWS Linked Accounts it uses under the contract to reduce the governance, operational, and business burden of managing multiple accounts.

4. Root Credentials for Linked Accounts:

For new AWS Linked Accounts requested by DOT, the AWS reseller shall provide DOT with temporary root credentials to the new account. Immediately upon receipt of the temporary root credentials, DOT will change the root credentials to eliminate AWS reseller access to the account. Upon award of the AWS contract, DOT will indicate the name of the individual approved to request new AWS Linked Accounts and to whom temporary root credentials shall be provided by the AWS reseller.

5. AWS Account Holder:

After establishment of each AWS Linked Account for the Agency by the AWS reseller under this SOW, for all intents and purposes, DOT shall be considered the "Account Holder" with all associated rights and responsibilities, excluding the direct payment to AWS, which will be the responsibility of the reseller as described in the requirement for Consolidated Billing Services.

DOT's role as the "Account Holder" explicitly includes DOT's unrestricted and exclusive rights and ownership of all data placed into the Account by DOT, all DOT-developed and DOT-licensed software operating within the Account, and all mechanisms configured, constructed, or developed by DOT for purposes of operating DOT workloads, applications, and services within the Account. No system integration services are being acquired via this AWS award such that the reseller would be required, or be allowed, to develop, apply, or

create reseller intellectual property to configure, operate, or support DOT data, DOT workloads, DOT applications, and DOT services within the Account. As a condition of contract acceptance, the reseller agrees it will not subsequently claim ownership of, nor intellectual and other types of property rights to, any of the above assets operating within a DOT AWS Linked account for which the reseller is providing consolidated billing services.

6. Administrative Account Transfer:

DOT intends to acquire cloud services under this contract up to the value and duration stated, subject to demand. However, given that AWS is a contract vehicle and there shall be no reseller-owned physical, virtual, software, data, or intellectual property assets associated with AWS Linked Accounts with which DOT's role is the Account Holder (as described above), DOT retains the right, no sooner than one Month after contract award, to administratively transfer, with at least 15-days notice, its AWS Linked Accounts to an Amazon consolidated billing account assigned to another reseller, integrator, federal contractor, or federal agency should DOT determine this is the Government's best interest.

Similarly, DOT may subsequently choose to change any Linked Account to become a direct DOT "payer" Account upon removal from the AWS reseller's consolidated billing account. In all cases involving the transfer of a DOT AWS Linked Account from the AWS reseller's consolidated billing account, DOT will be responsible for paying the reseller under this award for all DOT AWS Linked Account charges incurred prior to the transfer. The AWS reseller agrees to support, without additional cost, the administrative transfer (de-linking) of the DOT AWS Linked Account, upon request by DOT, out of the resellers consolidated billing account without requiring any termination or interruption of active AWS services within the DOT AWS Linked Account during the transfer process.

Information about AWS consolidated billing and enabling AWS linked accounts for consolidated billing is found at:

<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html> .

7. Access to Selected Pages and Information from the AWS Billing Management Console:

For each AWS Linked Account managed by the reseller for purposes of providing consolidated billing services for DOT, the following access and use is required by DOT from the Linked Account Billing Management Console:

- a. Full access to view and use Billing Dashboard
- b. Full access to view and use the Bills page (including downloading bills)
- c. Full and Enabled access to, and use of, Cost Explorer
- d. Full access to, and use of, the Account Setting page and options
- i. As stated previously, DOT will not utilize the Amazon Reserved Instance Marketplace with any AWS Linked Accounts under this contract
- e. Full and Enabled access to, and use of, AWS Reports

For each AWS Linked Account managed by the reseller for purposes of providing consolidated billing services for DOT, the following Settings are required by DOT, on the Billing Management Console associated with each DOT Consolidated Billing Account:

7.1 Enable Cost Explorer:

The reseller shall enable DOT to use “Cost Explorer” for all DOT AWS Linked Accounts by selecting the “Enable Cost Explorer” option for each Consolidated Billing Account used to provide DOT with Consolidated Billing Services for its AWS Linked Accounts.

7.2 Receive Billing Alerts:

The reseller shall enable DOT to receive direct “Billing Alerts” for all DOT AWS Linked Accounts and for AWS Services operating within the accounts by selecting the “Receive Billing Alerts” option in the Preferences section of each Consolidated Billing Account used to provide DOT with Consolidated Billing Services for its AWS Linked Accounts.

7.3 Receive Billing Reports:

The reseller shall enable the generation of “Detailed Billing Reports” for each DOT AWS Linked Account by selecting the “Receive Billing Reports” option in the Preferences section of each Consolidated Billing Account used to provide DOT with Consolidated Billing Services for its AWS Linked Accounts.

Unfortunately, AWS Linked account access to three important AWS Detailed Billing Reports is not an automatic option today under Consolidated Billing Services. However, DOT requires access to these Detailed Billing Reports to responsibly manage Agency costs, so unrestricted access via reseller action under this contract shall be required as indicated below for each Detailed Billing Report.

a. Monthly report: Lists AWS usage for each product dimension used by an account and its IAM users in monthly line items. Can be downloaded from the Bills page of the Billing and Cost Management console. <AWS account number>-aws-billing-csv-yyyy-mm.csv

i. DOT Access Frequency Requirement: On-demand access to latest updates from Billing Management Console (No reseller action required due to there being no existing AWS Linked Account access restrictions).

b. Detailed billing report: Lists AWS usage for each product dimension used by an account and its IAM users in hourly line items. <AWS account number>-aws-billing-detailed-line-items-yyyy-mm.csv.zip

i. DOT Access: On-demand via manual and programmatic method

ii. The reseller shall meet this requirement by providing DOT with direct access to the S3 object within which AWS places this report. DOT’s access to the object shall be as timely as the access that AWS makes available to the reseller.

c. Monthly cost allocation report: Contains the same data as the monthly report, but also includes any cost allocation tags that DOT has created. <AWS account number>-aws-cost-allocation-yyyy-mm.csv

i. DOT Access: On-demand via manual and programmatic method

ii. The reseller shall meet this requirement by providing DOT with direct access to the S3 object within which AWS places this report. DOT’s access to the object shall be as timely

as the access that AWS makes available to the reseller.

d. Detailed billing report with resources and tags: Contains the same data as the detailed billing report, but also includes any cost allocation tags DOT has created and ResourceIDs for the AWS resources used by the account. <AWS account number>-aws-billing-detailed-line-items-with-resources-and-tags-yyyy-mm.csv.zip

i. DOT Access: On-demand via manual and programmatic method

ii. The reseller shall meet this requirement by providing DOT with direct access to the S3 object within which AWS places this report. DOT's access to the object shall be as timely as the access that AWS makes available to the reseller.

The DOT-designated Points of Contact (POCs) who are approved for manual and/or access to the Billing Reports will be provided to the reseller.

End of Month versions of the Billing Reports (a., b., c., d. above) shall be kept available for manual and programmatic access by DOT for three months.

More information about the Detailed Billing Reports, described above, can be found at: <http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/DetailedBillingReports.html>

Note: DOT understands the detailed billing reports indicated above are not actual bills, but an estimate of costs and charges for AWS usage.

For each AWS Linked Account managed by the reseller for purposes of providing DOT with consolidated billing services, DOT will only access the following capabilities available from the Billing Management Console in accordance with the conditions provided below:

a. Access to Payment Methods Section (only for purposes of administrative account transfer)

b. Access to the Consolidated Billing Section (N/A for Linked Accounts)

c. Access to the Credits Section (when redeemable credit codes are provided by reseller)

d. Access to the DevPay Section (never)

8. Cost Allocation and Usage Tags:

DOT plans to use Cost Allocation and Usage Tags for granular cost and other reporting within all AWS Linked Accounts. As such, DOT will regularly provide the reseller with a list of new and no-longer-required Cost Allocation and Usage Tags so the reseller can indicate which Cost Allocation and Usage Allocation Tags will be included or excluded in the Billing Reports required by DOT above. The reseller shall ensure Cost Allocation and Usage Tag updates are made for each AWS Linked Account by the close of the next business day (5 p.m. Eastern time) so the Tags are reflected within the Billing Reports. As preferred alternative, DOT will perform the steps necessary to address this requirement if provided adequate access by the reseller to the DOT Consolidated Billing Account.

9. Master Payer Account:

The contractor must allow DOT to run AWS organizations with all features enabled in the

Master Payer account.

10. Enterprise Support:

The contractor must provide AWS Enterprise Support

2.1 Consumption of AWS services

- 2.1.1 The contractor may be requested to support the acquisition of products or services from third party vendors that are needed to support the execution of activities in support of this contract, and may purchase these items through this contract as other direct costs (ODC). This includes cloud services, software licenses, vendor software support services, and other items. Department and government-wide enterprise software license providers shall be the preferred method to obtain licenses when most cost-effective, and the contractor shall work with DOT to ensure these are assessed and potentially used before making any licensing purchases.
- 2.1.2 The contractor shall acknowledge the receipt of all service orders and confirm that the service can be provided by the requested service need date as determined by DOT.
- 2.1.3 The contractor may be requested to operate DOT's AWS environment on-site at DOT HQ while providing OJT to DOT's federal and contractor staff until DOT's staff is fully trained and capable of managing the environment. These managed services will be on a time and material basis.

2.2 ODC's

- 2.2.1 DOT will utilize ODC's for licensing and the contractor will purchase the license with written DOT approval.
- 2.2.2 DOT will utilize ODC's for AWS training classes with written DOT approval.

3 Transition-Out Planning

3.1 Documentation

- 3.1.1 The contractor shall provide updated and current architectures, inventories, standard operating procedures (SOPs), diagrams, configurations, and other documentation by the end of the transition-out period (this includes documentation explicitly stated in this SOW, requested by DOT throughout the period of performance, and completed by Contractor resources to execute their completion of contract requirements and DOT cloud services environment (CCoE) support activities.)
 - 3.1.1.1 The contractor shall require a written (electronic) receipt that the items in this section are received by DOT and are valid.
 - 3.1.1.2 The contractor shall delete or otherwise destroy the items in this section at the direction of the DOT and only after a written receipt is received by the contractor from DOT
 - 3.1.1.3 The contractor shall confirm with DOT in writing that all items in this section have been processed and that no copies are maintained with the contractor on any media.
- 3.1.2 The contractor shall provide detailed reports on the current state of all operations, maintenance, optimization, sustainment, and other efforts in progress but not yet

- completed and will include the locations and names of all in-process files/code being updated, explanations of what is completed and what is left to complete for the effort in terms of requirements, sustainment, and testing, as well as a list of issues or uncertainties encountered that still exist, limitations, and any test results.)
- 3.1.3 The contractor shall transfer responsibility for current support services.
 - 3.1.4 The contractor shall transfer custody of historic and current data, documentation, processes, training, and tools.
 - 3.1.5 The contractor shall transfer user and system administration for all systems and tools.
 - 3.1.6 The contractor shall transfer administrative user accounts and all other privileges user access credentials.
 - 3.1.7 The contractor shall transfer all assets (GFE/GFI/other within DOT's CCoE.)
 - 3.1.8 The contractor shall transfer and checking in of all source code and system configurations (all versions, updates, and patches) to the centralized, DOT-owned code repository.
 - 3.1.8.1 The contractor shall require a written (electronic) receipt that the items in this section are received by DOT and are valid.
 - 3.1.8.2 The contractor shall delete or otherwise destroy the items in this section at the direction of the DOT and only after a written receipt is received by the contractor from DOT
 - 3.1.8.3 The contractor shall confirm with DOT in writing that all items in this section have been processed and that no copies are maintained with the contractor on any media.
 - 3.1.9 The contractor shall surrender access badges, keys, cards, passwords, and security codes.
 - 3.1.10 The contractor shall participate in knowledge transfer sessions.
 - 3.1.11 The contractor shall respond to DOT and any new support group questions related to the CCoE .
 - 3.1.12 The contractor shall only release data on approval by DOT and for lawful purposes with consultation with and upon written approval from DOT council.

Accessibility Requirements

In support of executing the contract, the Contractor shall comply with Section 508 of the Rehabilitation Act. Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All deliverables shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt

Breach Response - The Contractor agrees that in the event of any actual or suspected breach of Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the contracting officer, the Contracting Officer's Representative (COR), and the DOT Privacy Officer (DOTsecurity@dot.gov). The Contractor is responsible for positively verifying that notification is

received and acknowledged by at least one of the foregoing DOT parties.

Personally Identifiable Information Notification Requirement - The Contractor has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the Contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by DOT in accordance with DOT Privacy Incident Handling Guidance. Notification shall not proceed unless DOT has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to Government analysis of the breach and the terms of its instructions to the Contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by DOT. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

In the event that a Sensitive PII breach occurs as a result of the violation by the Contractor or its employees, the Contractor shall, as directed by the contracting officer and at no cost to DOT, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should DOT elect to provide and/or procure notification or identity protection services in response to a breach, the Contractor will be responsible for reimbursing DOT for those expenses.

E-Discovery- DOT's document retention management plan shall apply to DOT's data stored in the cloud. In the case of a litigation hold, the Contractor shall work with DOT to ensure destruction of data does not occur.

Indemnities – The contractor shall defend and indemnify DOT against any “Indemnified Claim,” meaning any third party claim, suit or proceeding arising out of, or alleging:

(i) infringement of any patent, copyright, trade secret or other intellectual property right by the System; (ii) injury to or death of any individual, or any loss of or damage to real or tangible personal property, caused by the act or omission of the Contractor or any of its agents, subcontractors or employees; or (iii) disclosure or exposure of personally identifiable information or other private information caused by the act or omission of the Contractor or any of its agents, subcontractors or employees.

Non-Disclosure Agreements - The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.

Protection of Information - The government will retain unrestricted rights to government data. The Government retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

Government data loaded into or processed by the cloud services shall be protected against

unauthorized access, disclosure or modification, theft, or destruction. The Contractor shall ensure that the facilities that house the network infrastructure are physically secure.

Availability - The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no additional cost to the government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

Security Classification - The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level.

Disclosure of Information - Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

2.0 Period of Performance

The period of performance shall be for one (1) 5 Month Base period of five (5) 12 Months option periods The Period of Performance reads as follows:

Base Period - 12 Months
Option Period 1 – 12 Months
Option Period 2 – 12 Months
Option Period 3 – 12 Months
Option Period 4 – 12 Months
Option Period 5 – 12 Months

3.0 General (Note: This section applies to a Performance Work Statement, enter “N/A” if using this format for a Statement of Work

The Contractor shall develop and maintain an effective Quality Control Plan (QCP to ensure services are performed in accordance with this SOW. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's QCP is the means by which he/her assures that his/her work complies with the requirement of the contract. The QCP is to be delivered 30 days after contract award. After government acceptance of the QCP, the Contractor shall receive the Contract Officer's (CO) acceptance in writing of any proposed change to the government accepted QCP.

3.1 Hours of Operation (Note: This section applies to work conducted at a Government Facility, enter “N/A” if place of performance is at the contractor's facility

Under this contract, the Contractor is responsible for conducting business, between the hours of

8:00AM through 5:00PM EST Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor at all times must maintain an adequate workforce for the uninterrupted performance of all tasks defined within this SOW when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

3.2 Place of Performance

The work to be performed under this contract shall be performed at 1200 New Jersey Avenue, SE, Washington, DC 20590 or Contractor facility.

3.3 Physical Security

The Contractor shall be responsible for safeguarding all government equipment, information, and property provided for Contractor use. If performing in a government facility At the close of each work period, government facilities, equipment, and materials shall be secured.

3.4 Special Qualifications

The Contractor is responsible for ensuring all employees working on this project possess and maintain current professional AWS certification during the execution.

3.5 Periodic Progress Meetings

The contractor agrees to attend progress meetings. The Contracting Officer or Contracting Officer's Representative (COR), and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings, the CO will apprise the Contractor of how the government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

3.6 Identification of Contractor Employees

All contractor personnel attending meetings, answering Government telephones, and working in other situations where their Contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by Contractors are suitably marked as Contractor products or that Contractor participation is appropriately disclosed. Contractor personnel will be required to obtain and wear badges in the performance of this service.

3.7 Contractor Travel

Contractor may be required to travel throughout CONUS during the performance of this contract to attend meetings, conferences, and training. The Contractor may be required to travel to off-site training locations and to ship training aids to these locations in support of this SOW." All travel requires Government approval/authorization and notification to the COR.

3.8 Materials

Training materials may be required. These costs must be preapproved by the contracting officer. Material costs are not typically used in FFP unless there are substantial direct costs for materials involved or the cost of the materials is subject to change based on fluctuating market conditions.

3.9 Organizational Conflict of Interest

Contractor and subcontract personnel performing work under this award may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the CO immediately whenever he/she becomes aware that such access or participation may result in any actual or potential OCI, and may merit the submittal of a plan to the CO to avoid or mitigate any such OCI. This mitigation plan would be determined to be acceptable solely at the discretion of the CO, and in the event the CO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may effect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

3.10 Phase In /Phase out Period

To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the thirty (30) days phase in/ phase out periods. During the phase in period, the Contractor shall become familiar with performance requirements to commence full performance of services on the start date.

4.0 Government Furnished Equipment and Services

4.1 Services

The Government will provide personnel to support this Agile process.

4.2 Facilities

The Government will provide *workspace for the Contractor staff to include desk space, telephones, computers, and other items necessary to maintain an office environment.*

4.3 Materials

The Government will provide Standard Operating Procedures and Policies for the appropriate sections of the contract.

5.0 Applicable Publications (Current Editions)

The Contractor must abide by the following regulations, publications, manuals, and local policies and procedures. NA

5.1 Applicable Clauses

52.217-8 Option to Extend Services

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within the contract period.

52.217-9 Option to Extend the Term of the Contract

(a) The Government may extend the term of this contract by written notice to the Contractor any time prior to contract expiration, provided that the Government gives the Contractor a preliminary written notice of its intent to extend any time before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **[18]** months.

6.0 Attachment/Exhibit List

6.1 Exhibit 1

Performance Requirements Summary

6.2 Exhibit 2

Deliverables Schedule

6.3 Exhibit 3

Schedule of Services (To be included at award)

TECHNICAL EXHIBIT 1

PERFORMANCE REQUIREMENTS SUMMARY

The Contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective (The Service required—usually a shall statement)	Performance Standard	Performance Threshold (This is the maximum error rate.)	Method of Surveillance
PRS # 1. The Contractor shall provide Meeting minutes (including comments on external meeting minutes) Conduct and/or attend all working group meetings on schedule.	The Contractor provided meeting minutes delivered within 2 working days after the meeting.	90% acceptable on first submission to Government 100% acceptable on subsequent submission to Government Deliver minutes and comments by 2 working days after meeting.	Reviewed by Program Technical Assistant (TA)

TECHNICAL EXHIBIT 2

DELIVERABLES SCHEDULE

This technical exhibit lists any reports or documentation that is required as a deliverable to include the frequency, # of copies, medium/format and who/where it is to be submitted. A deliverable is anything that can be physically delivered but may include non-physical things such as meeting minutes.

<u>Deliverable</u>	<u>508 Compliant</u>	<u>Frequency</u>	<u># of Copies</u>	<u>Medium/Format</u>	<u>Submit To</u>
Kickoff meeting agenda Subtask 1.1	No	One time	One for every attendee	PowerPoint	COR
Management Plan	No	Living document updated as necessary	One	MS Word, MS Project	SharePoint site, and COR
Monthly Report	No	Monthly	One	MS Word	SharePoint site, and COR

Meeting record minutes with action items	No	1 day after meeting	One	MS Word	SharePoint site, and COR
Monthly Invoice	No	By the 10 th of every month	One	MS Word/Excel	<u>9-AMC-AMZ-NHTSA-Invoices@faa.gov</u> , COR
Task 2 Ordering					
Consumption Report	No	Monthly	One	Excel	SharePoint and COR
Task 3 Transition-Out Planning					
Documentation	No	One Time	One	MS Word and Visio	SharePoint and COR