REQUEST FOR PROPOSAL

No. FY26-1353

Azure Managed Services Provider

May 2026

AAMVA - Official Use Only

The American Association of Motor Vehicle Administrators (AAMVA) is a non-profit organization, representing the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws.

1 INTRODUCTION

1.1 PURPOSE

The American Association of Motor Vehicle Administrators (referred to here as "AAMVA") releases this request for proposal (RFP) to solicit proposals from qualified firms interested in participating in the bidding process.

AAMVA runs a large-scale IT infrastructure for exchanging information pertaining to driver licensing and vehicle registration among the motor vehicle agencies in all 50 U.S. states, the District of Columbia, several federal agencies, private sector organizations, and the provinces of Canada.

At present over 95% of the AAMVA's infrastructure is already hosted in Azure.

The purpose of this RFP is to select a vendor who can provide the following services:

- Provide Managed Services for Infrastructure, Services and Applications hosted in Azure Public and Government Cloud – (Required)
- Based on AAMVA's applications portfolio, AAMVA's current data hosting requirements are and will continue to be organized into two cloud deployment models:
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS) – including services like AKS, Managed SQL, Redis, Cosmos DB, Open Search, App Services, Event Hubs

In addition, AAMVA will continue to seek the transformation and modernization of its application portfolio to further leverage cloud native solutions and incorporate newly released Azure based solutions.

1.2 BACKGROUND

AAMVA is a tax-exempt, nonprofit organization that develops and supports model programs in motor vehicle administration, law enforcement, and highway safety. The association also serves as an information clearinghouse in these areas and acts as the international spokesman for these interests.

Founded in 1933, AAMVA represents the state and provincial and territorial officials in the United States and Canada that administer and enforce motor vehicle laws. AAMVA's programs encourage uniformity and reciprocity among the states and provinces. The association also serves as a liaison with other levels of government and the private sector. Its development and research activities provide guidelines for more effective public service. AAMVA's membership includes associations, organizations and businesses that share an interest in the association's goals.

1.2.1 AAMVA Environments, Systems and Applications

The exchange of information for AAMVA occurs through a combination of real-time system-to-system messaging (e.g., web services), batch processing (e.g., files), or through web user interfaces. The systems supporting the exchange of information are critical to AAMVA and its customers, as they have a direct impact on the motor vehicle agencies' ability to conduct their business operations.

On an average day, some systems process over 10 million transactions. Some of the databases hold over 1 billion records and exceed 1 TB of data. Legacy on-prem DCs are fully integrated with two Azure Gov hosted sites and two Azure Commercial hosted sites. The connectivity between on-prem and cloud sites is enabled through Express Routes, backed up by VPN circuits. AAMVANet – AAMVA's private nationwide network – utilizes SD-WAN, MPLS, and Secure Cloud Interconnect (SCI) services to provide connectivity between the core network and cloud sites.

All AAMVA critical systems are developed in house using Microsoft technologies, mainly Microsoft .NET and SQL Server, and are on a continuous modernization improvement trajectory. All servers are virtualized. The servers' operating systems are Windows Server 2019, with an active migration path to Windows Server 2025. AAMVA is actively transitioning workloads from IaaS to PaaS services — including Azure Kubernetes Service (AKS) and Azure App Service Plans — as part of its cloud modernization strategy. Please refer to §5.1 Exhibit A: Azure Services in-use or Under Consideration, for a more detailed look at the level of cloud adoption already achieved and the technologies currently considered.

In addition to the critical applications, AAMVA also operates many systems typical of an association such as email (i.e., O365), customer relationship management, productivity and collaboration, and financial applications.

AAMVA prides itself in providing its external and internal customers with outstanding services, which are made possible through devoted management of its infrastructure and service level objectives by dedicated staff complemented with external vendors and third-party service providers. AAMVA is currently on a transformation path that seeks to increase the overall Application availability from 99.5% to 99.95%.

1.2.2 AAMVA Capabilities

AAMVA has highly technical and competent staff that consists of approximately 120 IT professionals who support all phases of a system's lifecycle. The IT staff supports data center operations at the application, operating system, and infrastructure layers. The staff has the capability to deploy cloud resources, manage data centers, develop, and support applications, practice Continuous Integration (CI) and Continuous Delivery (CD) in a DevSecOps, ITIL v4, driven culture.

The AAMVA teams involved with cloud and on-prem data center operations are organized as follows:

- Application development and support
- Infrastructure, data center, and network support
- Quality assurance
- Help desk operations
- Network and Security infrastructure support

The existing Azure footprint spans both Production and Disaster Recovery environments across Azure Government and Azure Commercial. A part of this is currently operationally supported by a single Third-Party Provider. The Provider delivers the following services under multiple engagement:

- 24×7 monitoring with Level 1 and Level 2 incident response across both Production and DR in Azure Government
- Proactive capacity management, including trend analysis and resource forecasting across the Azure Government environment
- Backup administration and recovery validation across all Production and DR environments
- Patch management for all in-scope systems across both Production and DR in Azure Government
- Security Operations Center (SOC) services, including managed detection and response

  Level 1 and Level 2 Incident response includes but is not limited to:

  - **L1 (Triage & Initial Response):** Alert acknowledgment, initial diagnosis, runbook execution, basic remediation, ticket creation and classification
  - **L2 (Advanced Troubleshooting):** Deep technical investigation, configuration changes, coordination with AAMVA Support and Microsoft support, root cause analysis

Issues that exceed the Provider's L2 resolution capability are escalated to AAMVA's internal engineering teams or to Microsoft support as appropriate. The Provider is responsible for ticket continuity, status communication, and coordination throughout the escalation.

At present, L1 and L2 operational support is concentrated on the Production environments hosted in Azure Government, which carry the highest transaction volumes and the most stringent service level expectations. DR environments are monitored and maintained but operate under lower response thresholds consistent with their standby role.

This operational footprint is expected to shift as AAMVA advances its architectural transformation. AAMVA is actively moving from an active/stand-by regional model toward a high-availability, active/active deployment model. As that transition progresses, dedicated DR environments will be reduced in scope and replaced by production-grade active/active configurations. Concurrently, a growing share of production workloads will be deployed into Azure Commercial alongside the existing Azure Government footprint. Providers responding to this RFP should anticipate that the managed services scope will evolve accordingly, with an increasing number of production-tier environments in Azure Commercial requiring the same depth of L1/L2 support currently concentrated in Azure Government.

1.3 MINIMUM QUALIFICATIONS

The vendor must have a minimum of five years demonstrated experience in the commodities or services listed in this RFP.

The provider(s) must be a Microsoft Solutions Partner for Microsoft Cloud and currently have ongoing engagements for services similar to the ones requested in this RFP. The provider(s) must detail the list of all services that they are certified for with Microsoft.

The provider must be able to deliver technical assistance in the following areas:

- Managed Services for Azure Public and Government Cloud – (Required)
- Professional services in support of Azure transformational activities (list if available but not required)
- SOC support capabilities (list if available but not required). Please note that this is for informational purposes only, at this time AAMVA has no intention to replace its SOC Services provider.

In addition, the Provider:

- Must be able to share with AAMVA a current Standard Operational Classification (SOC) 2 Type II report, or the equivalent, such as relevant ISO certifications. For SOC 2, each of the Trust Service Principles must be addressed. These include Security, Availability, Processing Integrity, Confidentiality, and Privacy
- Must be able to support audits from independent third-party auditors, working on behalf of AAMVA, to assess the pertinent compliance level of AAMVA systems and operations

1.4 Period of Performance

The performance period for the anticipated contract:

Contract Period	Start	End
Base Contract	Contract Award	12-month base period from date of award.
Option Year 1	Following base contract	13 months from date of award; 12-month period.
Option Year 2	Following option year 1	25 months from the date of award; 12-month period.

2 GENERAL INFORMATION

2.1 RFP COORDINATOR

The RFP Coordinator is the sole point of contact at AAMVA for this procurement. All communication between the Offeror and AAMVA upon receipt of this RFP shall be with the RFP Coordinator, as follows:

Name, Title	**AAMVA Procurement**
Address	4250 N. Fairfax Drive, Suite 1000
City, State, Zip Code	Arlington, Virginia 22203
Phone Number	703.908.5877
E-Mail Address	procurement@aamva.org

AAMVA will consider any other communication as unofficial and non-binding on AAMVA. Communication directed to parties other than the RFP Coordinator, as related to the scope of the RFP, may result in disqualification of the Proposal.

2.2 Estimated Schedule of Procurement Activities

The estimated procurement schedule of activities for this RFP is as follows:

Activity	Date
Issue RFP	5/21/2026
Written Intent to Bid Due	5/28/2026
Written Questions Due from Vendors About Scope Or Approach	6/4/2026
Pre-Proposal Conference (Optional element)	6/8/2026 - 6/12/2026
Proposals Due	6/30/2026
Evaluate Proposal	7/01/2026 - 7/15/2026
Finalist Presentations for short-listed vendors (date/time TBD)	7/19/2026 - 7/25/2026
Announce “Apparent Successful Contractor”	One week following presentations

AAMVA reserves the right to revise this schedule.

2.3 Acceptance Period

The Proposal must provide 120 days for acceptance by AAMVA from the date of submission.

2.4 Responsiveness

The RFP Coordinator will review the Proposal to determine compliance with administrative requirements and instructions specified in this RFP. The contractor is specifically notified that failure to comply with any part of the RFP may result in rejection of the Proposal as non-responsive.

AAMVA also reserves the right, at its sole discretion, to waive minor administrative irregularities.

2.5 Most Favorable Terms

AAMVA reserves the right to make an award without further discussion of the Proposal submitted. Therefore, the Proposal should be submitted initially with the most favorable terms that the contractor can propose. AAMVA also reserves the right to contact a contractor for clarification of its Proposal and request a face-to-face meeting.

The contractor must be prepared to accept this RFP for incorporation into a contract resulting from this RFP. It is understood that the Proposal will become a part of the procurement file on this matter without obligation to AAMVA.

2.6 General Terms and Conditions

The apparent successful contractor will be expected to enter into a contract or purchase order with general terms and conditions agreeable to both parties. In no event is a contractor to submit its own standard contract terms and conditions in response to this solicitation. The contractor may submit exceptions as allowed in §5.2 Exhibit B: Certifications and Assurances to this solicitation. AAMVA will review requested exceptions and will accept or reject them at its sole discretion.

2.7 Costs to Propose

AAMVA will not be liable for any costs incurred by the Offeror in preparing a Proposal submitted in response to this RFP, or in performing any other activities related to responding to this RFP.

2.8 No Obligation to Contract

This RFP does not obligate AAMVA to contract for the commodities specified herein.

2.9 Rejection of Proposal

AAMVA reserves the right at its sole discretion, and without penalty, to reject any and all proposals received and not to issue a contract as a result of this RFP.

3 SCOPE OF SERVICES AND STATEMENT OF WORK

3.1 MANAGED SERVICES FOR AZURE CLOUD SERVICES (REQUIRED)

3.1.1 Managed Services

3.1.1.1 Network Operations Center

The Provider shall maintain a fully staffed Network Operations Center (NOC) operating continuously, twenty-four (24) hours a day, seven (7) days a week, and three hundred sixty-five (365) days a year, including holidays. The NOC shall serve as the primary point of operational oversight for all services delivered under this contract and must be physically located within the continental United States (CONUS) with staff located in CONUS.

The Provider shall ensure continuous eyes-on-glass monitoring by qualified NOC personnel at all times. Automated alerting alone does not satisfy this requirement — staff shall be actively engaged with live monitoring dashboards and tooling to enable rapid detection of and response to network events without reliance solely on automated notification systems.

NOC responsibilities shall include, at a minimum:

- Network Monitoring & Performance – Continuous real-time, eyes-on-glass monitoring of network health, availability, throughput, and latency across all in-scope infrastructure and circuits. NOC staff shall be positioned to detect and act on anomalies immediately upon alert generation.
- Operating System Support – Proactive and reactive support for operating system-level events, including patch status awareness, service failures, and system resource thresholds.
- Incident Detection & Response – Identification, escalation, and coordination of response activities for all network incidents in accordance with established severity and escalation procedures. Escalation Gates vary based on environments, services and applications and will be provided as part of the onboarding process. They fall within the Severity Level Guidelines and Communication Method specified in Table 1 below.
- Availability Reporting – Generation and delivery of network availability and performance reports on a schedule defined by the contracting agency.

3.1.1.2 Issue Tracking and Management

The Provider shall utilize an industry-standard issue tracking and management system to document, track, and manage all issues, requests, and incidents initiated by or on behalf of AAMVA. The system shall maintain complete and auditable records throughout the full lifecycle of each ticket, from initial submission through resolution and closure.

The Provider's ticketing system shall be capable of receiving and automatically ingesting email-based alerts from external monitoring and cloud platforms — including but not limited to Microsoft Azure, AAMVA health check systems, and third-party vendor alerting tools — and converting those alerts into managed incidents. Each ingested alert shall be tracked through its full incident lifecycle, including triage, assignment, status updates, escalation as warranted, and formal closure with documented resolution.

The Provider shall make available a self-service customer portal accessible to authorized AAMVA personnel at all times. The portal shall support, at a minimum:

- Help Desk & Incident Ticketing – Submission, tracking, and status visibility for all open and historical tickets and incident records.
- Incident Resolution Tracking – Real-time status updates and resolution documentation for all active incidents.
- Contact Directory – Current escalation contacts and support personnel information.
- Environment Documentation – Centralized, up-to-date storage of AAMVA's solution and environment design documentation to ensure continuity across Provider support staff.

All details pertaining to AAMVA's environment within the custody of the Provider shall be maintained and readily accessible to any authorized Provider personnel. This documentation shall include, but is not limited to:

- Architecture and network connectivity diagrams
- Service Level Agreements (SLAs)
- Escalation and support contacts
- Backup schedules and retention records
- Monitoring alert configurations and thresholds

The Provider shall conduct a weekly review with AAMVA covering all active and recently resolved incidents, ongoing issues, and identified trends. This review shall be delivered in a format and schedule mutually agreed upon by both parties.

3.1.1.3 Service Level Requirements

The provider shall be able to support and follow the problem severity guidelines specified in Table 1 for assigning severity levels for incident creation.

Table 1: Severity Level Guidelines and Communication Method

Severity*	Characteristics	Response Target	Communication Method
1 – Severe	Critical infrastructure component, critical system, network, or key application outage with critical impact on service delivery Total loss of production service to entire customer set One or more service level commitments impacted Revenue or delivery schedule impacted	5 minutes (7/24)	OmniAlert, Email, Phone, Text
2 – Major	Key component, application, critical end user machine or network is down, degraded, or unusable Service performance degradation, service delivery impacted; or, Partial customer set affected	30 minutes (7/24)	Email, Phone, Text
3 – Minor	Component, minor application or procedure is down, degraded, or difficult to use Some operational impact, but no immediate impact on service delivery Service outage, but alternative workaround available	2 hours (7/24)	Email

**1 indicates highest severity; 3 indicates lowest severity.*

AAMVA's production environments include DR components that while considered live production will have overall lower target response timeframe requirements.

AAMVA requires notifications of service outages or degraded performance. The provider shall communicate notifications via a support ticket, email, telephone call, or by all three methods, depending upon the severity of the situation as specified in Table 1. Upon service restoration, the provider shall provide fault isolation and root-cause analysis findings in restoration notices to AAMVA points of contact. AAMVA requests that the Provider provides root-cause analysis notifications within two business days of the incident. The provider shall work directly with Microsoft on behalf of AAMVA to manage tickets and problem resolution for any Azure platform related components.

The provider must have proven technology, processes, and procedures to escalate problems to AAMVA points of contact via a call tree-based solution, depending on the severity and type of issue.

SLA Metrics and Penalties

The provider must demonstrate a mature KPI management system including a service credit or remediation methodology designed to ensure SLAs are not missed:

- Resolution time targets, not just response time, per severity
- Provider NOC availability SLA (e.g. 99.99% uptime for monitoring platform)
- Service credit or remediation framework for SLA misses
- Weekly SLA attainment review as a contract governance mechanism

3.1.1.4 Systems and Application Monitoring

AAMVA requires proactive and reactive monitoring services which must cover all the services provided by the Azure Cloud provider and implemented by AAMVA, including but not limited to:

- Network resources – setup KPIs, proactively monitor, and report on performance and availability of all Cloud based network components deployed and leveraged by AAMVA. KPI and components monitored must include but not be limited to availability, latency, packet loss, jitter and utilization of Express Routes, VPN Circuits, SCI links, SD-WAN and NVAs.
- Services running on the operating systems – setup KPIs, proactively monitor, and report on performance and availability of OS level services.
- VM Utilization – setup KPIs, proactively monitor, and report on performance and availability of VMs including Utilization (e.g., memory, disk usage, I/O throughput).

- Full stack application monitoring – setup monitoring for and respond to application-level alarms as provided by AAMVA. Execute runbooks for specific alarms as provided by Application Development team.
- AKS Services – setup KPIs, proactively monitor, and report on performance and availability of multiple AKS Clusters and Applications.
- PaaS Services – setup KPIs, proactively monitor, and report on performance and availability of PaaS services deployed and in use by AAMVA.
- Backups – setup KPIs, monitor and report on the completion/failure of backups.
- Trending (for minimum of one year) with quarterly reporting checkpoints.
- High Availability — provider must have capabilities to detect failover to another region or availability zone in the event AAMVA's workload and services failover.
- Custom Monitoring — AAMVA's suite of services includes custom developed applications, commercial off-the-shelf (COTS) software, and custom synthetic monitoring transactions developed to monitor end user experience and response times. The provider will be required to use AAMVA's monitoring tools and services to further diagnose, troubleshoot, and resolve the issue as alerts are triggered. The provider will also be required to leverage Azure native machine learning capabilities to further enhance the proactive monitoring capabilities of the managed environment.
- External and Internal URL Monitoring (e.g., application health probes) — provider must be able to monitor and alert AAMVA's websites from an external internet connection at rates requested by AAMVA ranging from 15s to 1min, based on the use case.

Provider must supply detailed examples of how it will integrate alerts triggered by AAMVA's monitoring technologies into their support processes.

3.1.1.5 Backup Services

The provider must be able to configure, schedule, and manage backups of all the data including, but not limited to files, folders, images, system state, databases, and enterprise applications. The provider must provide cloud native backup options. The provider must encrypt all backup files and data and must manage encryption keys. The backup options must encompass a strategy of daily incremental and weekly full backups, at a minimum. All cloud instances must include options for snapshots and backups of snapshots. The encrypted backup should be moved to another geographical cloud region. Regardless of the method of backup, weekly full backups must include system state information. AAMVA's retention requirement for backups varies by application. Backup retrieval must be started within two hours of notification from AAMVA. The Provider must monitor all disaster recovery instances, including replication and instance performances.

3.1.1.6 Patching

The provider must provide patching capabilities for all AAMVA systems. Patching must cover all Microsoft and non-Microsoft vulnerabilities. The provider must manage deployment of new patches in AAMVA's environment before production deployment and must be capable of excluding patches from normal patching based on requests from AAMVA. This may include service packs and other application-specific patches. The provider must provide AAMVA with a list of patches to be applied before each patching event. From time to time, AAMVA may request that specific patches be performed outside of the normal monthly patching cycle. The provider must be capable of supporting these out-of-cycle patch requests. AAMVA plans to address patching via different approaches based on maturity:

- The Provider will be required to test new patch deployments in the DR designated environment before they are applied to Production designated environments.
- AAMVA plans to transition from IaaS to PaaS and from active/passive regional architecture to active/active regions over the next two years. The Provider must have proven capabilities supporting PaaS-based environments and active/active deployment models and must provide examples that demonstrate those capabilities.
- The Provider shall document the division of patching responsibilities across Microsoft (platform-managed updates), the Provider (OS, middleware, container images, AKS node pools), and AAMVA (application code and deployment pipelines).

3.1.1.7 Processes

The provider shall have processes in place to support AAMVA's IT operations. These processes must include but will not be limited to:

- Support for and integrate with established Cloud provider policies and practices
- Support for critical deployments
- Support for periodic DR exercises
- Support for AAMVA's Change Management requirements (CAB participation, change classification, emergency change procedures, RCAs)

The provider's processes must be:

- Thoroughly documented
- Reviewed and adjusted, as necessary, and reviewed at minimum annually

3.1.1.8 Security Operations Center Integration

The provider shall have processes in place to support integration with AAMVA's Security Operations Center – supported by a Security Managed Services Provider

- Integrate monitoring telemetry with AAMVA's SIEM platform (e.g., Microsoft Sentinel)
- Forward security-relevant alerts to the SOC in near-real-time
- Participate in joint incident response procedures for security events
- Support SOC-directed threat hunting and forensic investigations
- Establish clear swim lanes between the NOC (availability/performance) and the SOC (security)

NOC personnel shall maintain operational awareness that encompasses both infrastructure performance and security posture.

The Provider shall describe how its NOC operational model ensures integration with a SOC function for coordinated responses.

3.1.1.9 AAMVA Operations Center Integration

The provider shall establish and support process and system integration with AAMVA's Internal Operation Center. Consideration will be given to the capabilities available to:

- Implement bi-directional ticket integration between the Provider's ITSM system and AAMVA's internal ticketing system
- Define hand-off and escalation procedures between the Provider's NOC and AAMVA's internal Operations Center
- Develop joint runbooks for scenarios requiring coordinated response
- Support regular joint exercises or tabletop drill

3.1.2 Account Management

AAMVA requires a primary and backup account representative responsible for ensuring that all provider SLAs and deliverables are met. The account representative must communicate all service outages or degraded performance in a recurring performance report and weekly via a regularly scheduled meeting. The account management team must be within the continental United States.

AAMVA's hours of operations are Monday to Friday, 8 a.m. – 5 p.m. Eastern Time. AAMVA staff is available after hours and weekends as needed using an on-call rotation system. Please provide the location and hours of operation of the account management team and technical staff.

3.1.3 Dedicated Support Staff

The provider must assign dedicated staff as a technical support team. The dedicated staff is expected to provide immediate, around-the-clock (24 hours a day, seven days a week) support. It must be capable of acting as an advocate for AAMVA during outage events. The provider must make the identified staff accessible at all times or provide alternative backup contacts that are equally capable of understanding and supporting AAMVA's technical configuration.

The provider must provide processes for training new staff and provide detailed examples of how they will train new staff (technical and account management) to support AAMVA when they are assigned to AAMVA's account, or when there is staff turnover.

3.1.4 Governance, Risk Management and Compliance

Certain AAMVA systems must comply with the security and privacy requirements of the Federal Information Security Management Act (FISMA). These systems are either FISMA-classified as "Moderate," or must conform with the Payment Card Industry Data Security Standard (PCI DSS). As a result, the Provider must conform to the relevant FISMA or PCI controls. These include, but are not limited to:

- Access controls (logical and physical protections)
- Personnel security (e.g., background screening)
- Network and system protections (e.g., firewalls, malware protection)
- Security and privacy policies and procedures
- Security awareness training
- SOC 2, Type II

3.1.5 Azure Offerings

The Provider must have in place and explain its processes for bringing new Azure service offerings into operation. This must include development processes, procedures, and SLAs and must include examples for supporting Azure Kubernetes Cluster (AKS) and other PaaS Services.

The Provider must demonstrate that it has the processes to adopt and support recently released Azure Technologies (e.g., made GA by Microsoft within the previous six months) when AAMVA requests these. The Provider will be required to build the capability and capacity to support such services with no additional cost to AAMVA until turned into operations. Such agility is necessary to support changes to the AAMVA technology roadmap to take advantage of recently released products and feature sets.

3.1.6 Cost Optimization

The Provider must have in place the tools and processes that will allow AAMVA to optimize AAMVA's cloud resources best to reduce costs and gain efficiencies.

The Provider must provide examples of how they currently manage cost optimization for their customers, including tools, AI, processes improvements, and techniques.

3.1.7 Reporting

AAMVA requires a minimum number of reports on a recurring basis. Table 2 provides an example of reports needed. Additional reports may be added as needed.

Table 2: Reporting Requirements

Report Name	Frequency
Weekly Incident Status – Open, Close, In Progress	Weekly
Mean Time to Repair Intervals	Weekly
Tickets that Missed SLA Intervals	Weekly
List of Chronic Issues	Bi-Weekly
Network Availability	Monthly
Patches Applied	Each patching cycle
Backups Success	Daily
Capacity Projections	Quarterly
NOC Incident Response Call Tree	Quarterly
Monitoring Thresholds	Quarterly

3.1.8 Onboarding / Transition Services

The Provider must demonstrate expertise onboarding customers to Azure-based cloud managed services from other third parties to its existing portfolio. The provider must detail the approach, type of artifacts required and applicable pricing (if any), and the general timeframes anticipated to take over operations of the existing environment.

4 PROPOSAL INSTRUCTIONS AND EVALUATION PROCEDURE

4.1 PROPOSAL CONTENT

The proposal shall be comprised of the following four (4) volumes, numbered Volumes I, II, III, and IV. All text shall be twelve (12) point font, and page limits shall be as indicated. Please do not include corporate marketing material or boilerplate information in your response.

- **Volume I – Corporate Experience**

Limit to two (2) single-spaced pages. Vendor(s) shall provide a summary of any corporate information relevant to this RFP, which should include, at minimum: Length of time providing managed services, experience handling the same level of services as AAMVA needs in this RFP, and summary of the financial strength of the company.

Please include any Microsoft Partnership Certifications currently held. If the Azure Migrate and Modernize partner designation is not achieved but actively pursued, please specify that.

- **Volume II – Technical Solution and Approach**

Limit to twenty-five (25) single spaced pages including graphics. Please format your response in the same outline as Section 3 of this RFP. Please address each paragraph and capture how your organization's capability and capacity meet these requirements.

- **Volume III – Past Performance**

Limit to eight (8) single spaced pages. Vendor(s) shall describe three (3) to five (5) examples of similar managed services support services that vendor has provided of comparable size in the past three (3) years. For each example include contact information, project scope, relevance to this solicitation, timeline/dedicated hours, and written permission for a reference to discuss its performance with AAMVA.

- **Volume IV – Price Proposal**

Limit to ten (10) single spaced pages. Vendor(s) shall provide the best financial proposal to complete the work for the duration of the contract term.

The pricing proposal must demonstrate a model that is flexible and accounts for:

- The type of environments supported (e.g., Production, DR, Test, Development).

- The dynamic nature of the environment supported where volumes can increase or decrease from year to year, and the economies of scale that such changes would trigger.
- Process and technology improvements achieved with AI technologies.
- The types of SLAs required for various environments.

Please specify how discounts are applied based on the changes in the managed base.

Pricing for other direct costs, and any optional services relevant to this RFP must be included.

The AAMVA RFP Coordinator will review all Proposals to determine compliance with administrative requirements and instructions specified in this RFP. The RFP Coordinator will only forward responsive proposals that meet the minimum requirements to the evaluation team for further review.

AAMVA will evaluate responsive Proposals forwarded by the RFP Coordinator in accordance with the specifications stated in this solicitation and any issued addendums. AAMVA will award the contract to the vendor that provides the best overall value to AAMVA, according to the Proposal.

4.2 PROPOSAL SUBMISSION

Proposal must be submitted in soft copy (Adobe PDF format) as set forth below.

- The Proposal is to be sent to the RFP Coordinator at the email address noted in §2.1 RFP Coordinator. The email must be clearly marked with the RFP number to the attention of the RFP Coordinator,.
- Any modifications to a Proposal in response to this RFP will be subject to these same conditions. The Proposal must respond to the procurement requirements. Do not respond by referring to material presented elsewhere. The Proposal must be complete and must stand on its own merits. Failure to respond to any portion of the procurement document may result in rejection of the Proposal as non-responsive. All Proposals and any accompanying documentation become the property of AAMVA and will not be returned.
- Proposals must be submitted as two separate files in your response as follows:
  - File 1: Shall include Volumes I, II, and III labeled “Technical Proposal Response for RFP FY26-1353 by <company name>.pdf”
  - File 2: Shall include Volume IV Price proposal response labeled “Price proposal response for RFP FY26-1353 by <company name>.pdf”. Please also include the signed Exhibits A and B.

4.3 EVALUATION PROCEDURE

Response to proposals will be evaluated in accordance with the specifications stated in this solicitation and any addendum issued. Award will be made to the vendor that provides the best overall value to AAMVA.

Eval No.	Description	Possible Points
1.1	Reputable and established organization – Past Performance and Microsoft Partner Certification Levels is reviewed	10
	Total Possible Corporate Experience Points	**10**
2.1	Managed Services – Onboarding methodology	10
2.2	Managed Services – Technical monitoring and execution capability	30
2.3	Managed Services – AAMVA Operations Center Integration	10
2.4	Managed Services – Security Operations Center Integration	10
	Total Possible Technical Points	**60**
3.1	Pricing Model and Flexibility	30
	Total Possible Price Points	**30**
	Grand Total Possible Points	**100**

5 RFP EXHIBITS

5.1 EXHIBIT A: AZURE SERVICES IN-USE OR UNDER CONSIDERATION

Exhibit A provides a representative inventory of Azure services currently deployed or under active evaluation. Providers should use this inventory alongside the resource summary below to estimate the scale and complexity of the managed services engagement.

AAMVA's infrastructure currently spans six sites across two Azure cloud tenants and two co-location facilities:

- **Azure Government** — Two tenants (Virginia and Texas). These host the majority of production workloads today, including all mission-critical transaction processing systems. This is the primary focus of the current managed services engagement.
- **Azure Commercial** — Two tenants (EastUS2 and Central US). These currently host non-production workloads. As AAMVA transitions to an active/active high-availability model (described in §1.2.2), an increasing share of production workloads will be deployed here, and the managed services scope will expand accordingly.
- **Co-Location Facilities** — Two data centers (Ashburn, VA and Chicago, IL) supporting legacy on-premises infrastructure. These facilities are connected to the Azure environments via ExpressRoute, VPN, and SD-WAN/SCI circuits. AAMVA is executing a planned exit from on-premises hosting; as that effort concludes, the co-location footprint and associated interconnection services will be decommissioned. Providers are not required to assume any on-premises management responsibilities but should be prepared to support interconnecting Express Routes and Connections and the transition period.

For reference, the Production/DR Environment in scope supporting ~12 major external-facing customer application, is currently included the following technologies and approximate counts:

- ~536 VMs
- ~8 AKS Custers
- ~100 DB PaaS
- ~200 Compute PaaS
- ~ 80 Network PaaS
- ~ 600 Backup Items

5.2 EXHIBIT B: CERTIFICATIONS AND ASSURANCES

I/we make the following certifications and assurances as a required element of the proposal to which this Exhibit B is attached, understanding that the truthfulness of the facts affirmed herein and the continuing compliance with these requirements are conditions precedent to the award or continuation of the related contracts:

- I/we declare that all answers and statements made in the proposal are true and correct.
- The prices and/or cost data have been determined independently, without consultation, communication, or agreement with others for the purpose of restricting competition. However, I/we may freely join with other persons or organizations for the purpose of presenting a single proposal.
- The attached proposal is a firm offer for a period of 120 days following the due date for receipt of proposals, and it may be accepted by AAMVA without further negotiation (except where obviously required by lack of certainty in key terms) at any time within the 120-day period.
- In preparing this proposal, I/we have not been assisted by any current or former employee of AAMVA whose duties relate (or did relate) to this proposal or prospective contract, and who was assisting in other than his or her official capacity. Any exceptions to these assurances are described in full detail on a separate page and attached to this document.
- I/we understand that AAMVA will not reimburse any costs incurred in the preparation of this proposal. All proposals become the property of AAMVA and I/we claim no proprietary right to the ideas, writings, items, or samples presented in the proposal, unless so stated in the proposal.
- Unless otherwise required by law, the prices and/or cost data which have been submitted have not been knowingly disclosed by the consultant and will not knowingly be disclosed by him/her prior to opening, directly or indirectly, to any other consultant or to any competitor.
- I/we agree that submission of the attached proposal constitutes acceptance of the solicitation contents and the attached general terms and conditions. If there are any exceptions to these terms, I/we have described those exceptions in detail on a page attached to this document.
- No attempt has been made or will be made by the consultant to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.

_____

_____

Signature of Offeror Printed Name, Title and Date

5.3 EXHIBIT C: CERTIFICATION REGARDING DEBARMENT, SUSPENSION, AND OTHER RESPONSIBILITY MATTERS

The prospective vendor certifies to the best of its knowledge and belief that it and its principals:

- Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;
- Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any department or agency of the Commonwealth of Virginia or any of the jurisdictions comprising the membership of the American Association of Motor Vehicle Administrators (AAMVA);
- Have not within a three year period preceding this date been convicted of or had a civil judgment rendered against them for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
- Are not presently indicted for or otherwise criminally or civilly charged by a government entity (Federal, State or local) with commission of any of the offenses enumerated above of this certification; and
- Have not within a three-year period preceding this date had one or more public transactions (Federal, State or local) terminated for cause or default. Vendor understands that a false statement on this certification may be grounds for rejection of any submitted proposal or quotation or termination of any award. In addition, under 18 USC Sec. 1001, a false statement may result in a fine of up to $10,000 or imprisonment for up to 5 years, or both if federal funds are being used to support the procurement.

_____

Printed Name of Vendor

_____

Printed Name and Title of Authorized Representative

_____

Signature of Authorized Representative