American Association of
Motor Vehicle Administrators

OUR MISSION

Serve North American motor vehicle and law enforcement agencies to accomplish their missions.

OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

REQUEST FOR PROPOSAL

No. FY24-34677

Managed Detection & Response (MDR)

April 2024

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.

CONTENT

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.

The purpose for this RFP is to select a single service provider who can provide:

- 24x7x365 Managed Detection and Response (MDR) solution to support AAMVA' security operations that leverages AAMVA existing investments in the Microsoft Azure technologies.
- Support AAMVA's enhancement of its Security Operations Center (SOC) capabilities.

1.2 ENTITY 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 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.

AAMVA's AAMVAnet network processes more than 2.4 billion messages a year. Some of the databases hold over 2 billion records and exceed 1 TB of data. The infrastructure supporting those systems across their lifecycle exceeds 200 servers spread across three on-prem data centers, 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.

AAMVA currently provides application solutions and network services to its subscribers. Network services include a nationwide telecommunications network (AAMVAnet) that facilitates the exchange of information among government agencies and their private-sector trading partners. AAMVAnet is an external customer network separate from AAMVA's internal network.

AAMVAnet is a fully managed, private network environment built upon Verizon Business Solutions' Private IP (PIP) multiprotocol label switching (MPLS) core network service. AAMVA is in the process of rolling out SD-WAN technology to enable better routing performance, security and transport/provider diversity.

All AAMVA critical systems are developed in house using Microsoft technologies and are on a continuous modernization improvement trajectory that focuses on cloud native technology, and micro-services.

In addition to the critical applications that AAMVA operates to serves its members and customers, AAMVA also operates many systems typical of an association such as email (i.e., M365), 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 levels objectives by dedicated staff complemented with external offerors and third-party service providers.

A detailed inventory of the information assets in scope for this RFP will be provided under NDA and once AAMVA receives an intent to bid.

1.2.2 AAMVA Capabilities

AAMVA has approximately 210-225 personnel supporting the organization; among those, AAMVA benefits from a highly technical and competent IT professionals consisting of approximately 140-155 staff members who support all phases of a system's lifecycle, from business requirements to operations.

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

- Application development and tiers 3 support;
- Infrastructure, data center, and network operations and engineering;
- Quality assurance;
- Help desk operations; and,
- Security operations and engineering.

The IT staff supports data center operations at the application, operating system, and infrastructure layers. The staff has the capability to deploy servers, manage data centers, develop, and support applications, practice Continuous Integration (CI) and Continuous Delivery (CD) in a DevSecOps driven culture.

A third-party managed services provider oversees the continuous (24x7x365) monitoring of health and capacity of the Azure government regions, as well as provide backup and patch management of resources currently in production.

AAMVA boasts a mature Cyber Security operation, incorporating standard enterprise security practices such as Logging and Monitoring, Identity and Access Management (including Privileged Identity Management), in-house Managed Detection & Response (MDR), Cryptography, Network Access (including Privileged Access Management), Business Continuity/Disaster Recovery, and Endpoint Protection, among others.

While the majority of AAMVA staff is located within the metropolitan DC, MD, and VA area, AAMVA is a "remote organization", whereby all its personnel is working remotely.

1.2.3 AAMVA Compliance Requirements

As part of AAMVA's key organizational objectives, AAMVA strives to enhance compliance and transparency. To that effect, AAMVA is currently supporting the following practices:

- SOC2 Type II
- FISMA – NIST SP800-53 Rev 5
- FedRAMP Moderate

1.3 Service Provider Minimum Qualifications

1.3.1 Entity/Personnel Specific

1.3.1.1 Location requirements:

All services under this RFP must be provided using US-based resources: including systems, networks, data, and personnel.

1.3.1.2 Industry/Service requirements:

The service provider must have demonstrated experience in the commodities or services listed in this RFP for organizations with IT footprints comparable to AAMVA. Additionally, the provider should be experienced supporting organizations and IT operations similar in size and complexity as AAMVA.

The services consist of providing a cloud based, 24x7x365 MDR solution to support AAMVA' security operations that leverages AAMVA existing investments in the Microsoft Azure technologies; and to assist AAMVA is strengthening its SOC maturity.

1.3.1.3 Organizational Accreditations/Certifications:

The Provider must be able to share with AAMVA a current Service Organization Control (SOC) 2 Type II report, or the equivalent, such as relevant ISO certifications (27001). For SOC 2, the Security and Confidentiality Trust Service Principles must be addressed. Absent of the SOC2 Type II, or ISO certifications, the offeror must clearly spell out the measures taken to protect AAMVA sensitive information and assets related to the types of services provided to AAMVA. In addition, the service provider must be experienced and demonstrate capabilities to support AAMVA compliance requirements, including FISMA, FedRAMP and SOC2 Type II.

1.3.1.4 Environment requirements:

The provider must demonstrate proficiency in effectively managing multiple Azure tenancies and on-premises datacenters. This includes ensuring streamlined access control, efficient monitoring, and seamless management across diverse Azure environments.

The provider should be well versed in secure operations with the latest Microsoft technologies, whether it is on the Microsoft Azure clouds (Government and Commercial) or the M365 platform. Members of the team supporting AAMVA shall hold pertinent certifications and demonstrate a level of seniority and experience that is commensurate with their role.

1.3.1.5 Personnel Certifications/Skills:

All the provider resources assigned to this engagement must have at least five of relevant security operations and threat hunting experience, and maintain in good standing relevant professional certifications such as CEH, GIAC etc.

The provider should also assign a primary resource to provide oversight of all the technical aspects of this engagement. This resource should be self-directed, ideally with demonstrated leadership experience in the subject matter.

The provider must clearly state during the RFP process the qualifications of the resources assigned to this engagement and their associated responsibilities. The quality and experience of the resources assigned to this engagement will be a key factor in AAMVA's selection process.

Lastly, the provider should disclose current turnover ratio for the main resources assigned to this engagement.

1.3.1.6 Other Vendor Experience

In the response to this RFP, the service provider is expected to speak to the following:

- Expertise with SIEM solutions, including Microsoft Sentinel
- Expertise with Microsoft Azure and any Microsoft partner status
- Experience and in-depth knowledge around complex compliance regulations, including Federal security compliance requirements
- Expertise around management and monitoring of third-party risks
- Capabilities with regards to threat intelligence
- Catalogue of alerts, reports and runbooks
- Key performance indicators such as, but not limited to, Mean Time to Response, Mean Time to Closure.

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 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	AAMVA Procurement
Address	4401 Wilson Boulevard, Suite 700
City, State, Zip Code	Arlington, Virginia 22203
Phone Number	703.908.2861
Coordinator	Khalid Rahimi
Title	Senior Procurement Manager
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	04/12/2024
Written Intent to Bid Due	04/19/2024
Written Questions Due from Offerors About Scope or Approach	04/23/2024
Pre-bid proposal teleconference (date/time TBD)	04/25-30 2024
Proposals Due	05/20/2024
Evaluate Written Proposal	05/24/2024
Finalist Presentations for short-listed vendors (date/time TBD)	05/27-6/05 2024
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

AAMVA is soliciting experienced and qualified service provider(s) who can provide the following services:

- 24x7x365 Managed Detection & Response (MDR) solution to support AAMVA' security operations that leverages AAMVA existing investments in the Microsoft Azure technologies.
- Support AAMVA's enhancement of its Security Operations Center (SOC) capabilities.

Note: A detailed inventory of the information assets in scope for this RFP will be provided under NDA and once AAMVA receives an intent to bid.

Please review the information provided in section 1.2 & section 1.3 (and associated subsections) of this RFP, including the high level description of AAMVA's background, environments, capabilities, and the service provider minimal qualifications as those details will not be repeated in this section.

3.1 MANAGED DETECTION & RESPONSE (MDR) SERVICES

3.1.1 Security Information and Event Management (SIEM) requirements:

The AAMVA security team has significant experience deploying and operating Security Information and Event Management (SIEM) solutions and managing incident response in house. However, the SIEM team's time is shared with other corporate priorities, and the team is small enough that a 24x7x365 eyes on glass monitoring is not feasible.

AAMVA's SIEM solution is fully deployed using Microsoft native technology and provides broad coverage of AAMVA IT operations in Azure and on-premises.

AAMVA is not interested in deploying another redundant external SIEM solution. Instead, AAMVA wants to work with service providers who can leverage the existing SIEM solution. Service providers will be given and are encouraged to review the existing SIEM implementation to ensure that it is configured in such way that it will allow for effective delivery of MDR services.

The service providers must explain how their security operations center (SOC) operations will leverage AAMVA's SIEM solution, including aspects such as identity and access management.

If the vendor intends to manage the incidents generated by AAMVA SIEM into a platform other than AAMVA's, a detailed description of the platform and its interoperability requirements with AAMVA SIEM is expected.

Usage of any additional threat sources should be disclosed in the RFP response.

In all cases, the vendor shall clearly disclose the workflow associated with the incident response, whether that workflow varies based on incident criticality, and how they intent to escalate relevant issues to AAMVA.

3.1.2 Role and Responsibility requirements:

Given AAMVA existing capabilities and expertise operating its complex IT infrastructure, the service providers must describe how they will interact with AAMVA teams, and specifically, where the division of responsibilities lie between AAMVA's SIEM team and the providers team. That said, as the relationship between AAMVA and the service provider matures, it is AAMVA expectation that the service provider ability to conduct incident response will grow.

AAMVA is interested in understanding the details of the service provider onboarding process and the expected interactions and dependencies on AAMVA personnel.

AAMVA needs to understand the composition of the team responsible for the delivery of the services, the role of each member and their level of relevant expertise & certifications; and how the service provider will manage staffing turnover and knowledge transfer.

In addition, AAMVA needs details on how incidents will be transferred to its own team, and any escalation path the service provider is relying upon.

3.1.3 Monitoring / Service-level agreement (SLA) requirements:

AAMVA expects the service provider to provide eyes-on-glass 24x7x365; with the full awareness that not all incidents require the same level of urgency. AAMVA's target service-level agreement (SLA) for the MDR services are as follow:

Time	Criticality	Incident Acknowledgement	Incident Response
Core Business Hours **M-F 7AM-9PM EST**	Critical & High	30 min	1 hr.
	Others	2 hrs.	4 hrs.
Nights and Weekends	Critical & High	30 min	1 hr.
	Others	Next business day	Within 4 hrs. next business day

Should the service provider offer multiple tiers of SLA, details of those tiers MUST be fully disclosed in response to the bid solicitation; including but not limited to tier differences both operationally (in delivery to meeting AAMVA's requirements) and financially (cost to AAMVA).

The vendor must specify how incidents will be managed, including any use of an IT Service Management solution, the workflow(s) of each incident type, and how AAMVA may interact with the ITSM solution.

AAMVA requires weekly incidents and operations reviews, and quarterly account reviews. The weekly reviews objectives include reviews of notable incidents, reviews of key performance indicators and discussion of any impediment. The quarterly reviews objectives include detailing the current state of AAMVA cyber maturity, its target state and the specific actions that can be taken to advance towards AAMVA's cyber maturity target state and any adjustments that can be made to the services delivered to AAMVA. The service provider is expected to detail the content and approach of each review and is encouraged to provide examples.

3.1.4 Access to AAMVA SIEM and Environments

The vendor must specify how they anticipate getting access to AAMVA SIEM and environments and whether any SSO or access broker solution, such as Azure LightHouse will be leveraged.

Furthermore, the vendor shall clearly denote the expectations in terms of permissions to the AAMVA Environment, whether it is on Azure or AAMVA active directory domain resources.

3.2 Security Operations Center (SOC) Services

In addition to providing services for managed detection and response, AAMVA is requesting the service provider to assist in further enhancing AAMVA's security operations center (SOC) maturity. Given that the vendor will rely on AAMVA's SIEM and work in tandem with AAMVA security personnel, it is imperative that both teams operate with the highest level of efficiency.

Potential areas of support that could benefit AAMVA:

- Review AAMVA incident response plan.
- Assist AAMVA in developing play books for common incident remediation.
- Assist AAMVA in automating incident remediation.
- Identify areas/use cases/incidents where the service provider could assume additional responsibilities.
- Assist AAMVA in enhancing advanced threat hunting capabilities.
- Suggest optimization of the monitoring platform from an effectiveness and costs standpoint.
- Assist AAMVA leverage the latest features and monitoring technologies as Microsoft solutions continue to evolve.

The service providers should describe their experience and approach in helping organization mature their internal SOC in a way that it supports the MDR services already offered.

3.3 Value Add Services

Aside from the MDR and SOC maturity services, AAMVA would like to understand what other related services the vendor has capabilities into. While having such capabilities is not a hard requirement, it can be a differentiator.

To that end, the service provider is encouraged to provide succinct information on value-add services. Example of such services may include:

- On-demand technical expertise on technologies relevant to AAMVA
- Virtual CISO support
- Review and optimization of AAMVA security policies and procedures
- AI and machine learning security
- Threat Intelligence data

4 PROPOSAL INSTRUCTIONS AND EVALUATION PROCEDURE

4.1 PROPOSAL CONTENT

The proposal shall comprise the following two (2) volumes, numbered Volumes 1 and 2.
All text shall be twelve (12) point font, and page limits shall be as indicated in the subsequent sections.

- Please limit the size of all email correspondences to 10 MB.
- ***Please do not include corporate marketing material or boilerplate information in your response.***

4.1.1 Volume 1

4.1.1.1 Volume 1.1 Corporate Information/Past Performance/Qualifications

Combined limit, eight (8) single spaced pages including graphics.

4.1.1.1.1 Corporate Information

Limit to two (2) single-spaced pages.

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

4.1.1.1.2 Past Performance

Limit to two (2) single-spaced pages.

Offeror(s) shall describe three (3) to five (5) examples of similar managed services support services that the offeror has provided of **similar size in the past three (3) years.** For each example, include contact information and written permission for a reference to discuss its performance with AAMVA.

4.1.1.1.3 Minimum Qualifications

Limit to two (2) single-spaced pages.

See *§ 1.3 Minimum Qualifications* for requirements.
Please describe how your firm meets all requirements; location, industry/service, compliance, and environment.

4.1.1.2 Volume 1.2 Technical Solution/Approach

Combined limit, twenty (20) single spaced pages including graphics.

Please format your response in the same outline as Section 3 of this RFP.

See *§ 3SCOPE OF SERVICES AND STATEMENT OF WORK* for requirements.

4.1.1.2.1 MANAGED DETECTION & RESPONSE (MDR) SERVICES

Limit to fifteen (10) single spaced pages including graphics.

Please describe how your firm meets all requirements of section 3.1 and associated subsections.

4.1.1.2.2 SECURITY OPERATIONS CENTER (SOC) SERVICES

Limit to ten (10) single-spaced pages, including graphics.

Please describe how your firm meets all requirements of section 3.2 and associated subsections.

4.1.2 Volume 2

4.1.2.1 Price Proposal

Limit to ten (10) single-spaced pages.

Offeror(s) shall provide the best financial proposal to complete the work for the duration of the contract term.

4.1.2.2 Volume 2.1 Professional Services

- Professional Services: Please provide a pricing catalog that covers ALL fees relevant to the type of engagements requested.
- Discounts: As applicable, please specify how discounts are calculated and applied.
- Assumptions: Identify any assumptions made to create the Price Proposal.
- Other: Please include pricing for travel, other direct costs, and any optional services that may be relevant to this RFP. Any other information as required.

4.1.2.3 Volume 2.2 Set Service Fees

If applicable, please provide fixed set fees for the subject services.

4.1.2.3.1 Setup Fees

One-time fees for initial setup, configuration, and deployment of SOC infrastructure and tools.

4.1.2.3.2 Monthly Subscription Fees

Recurring fees for ongoing monitoring, detection, and response services, based on the level of service and volume of data processed.

4.1.2.3.3 Incident Response Fees

Additional fees for incident response services, charged on a per-incident or hourly basis.

4.1.2.3.4 Compliance Reporting Fees

Fees for generating and delivering compliance reports, based on the frequency and complexity of reporting requirements.

4.1.2.3.5 Customization Fees

Fees for customizing the SOC environment, tools, and processes to meet the specific needs of AAMVA. State the service fees for creating or finetuning an Analytics rule.

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, Siedah Ross.
- 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, and II, and labeled “Corporate & Technical Proposal Response for RFP 34677 by <company name>.pdf”
  - **File 2:** Shall include Volume III, Price proposal response labeled “Price proposal response for RFP 34677 by <company name>.pdf”. Please also include the signed Exhibits B and C.

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 offeror that provides the best overall value to AAMVA.

Items	Description	Evaluation %
1	**Volume 1**	
1.1	**Volume 1.1 *(see section 4.1.1.1)***	
1.1.1	Corporate Information *(see section 4.1.1.1.1)*	5%
1.1.2	Past Performance *(see section 4.1.1.1.2)*	5%
1.1.3	Qualifications *(see section 4.1.1.1.3)*	5%
1.2	**Volume 1.2 *(see section 4.1.1.2)***	
1.2.1	MDR Services *(see section 4.1.1.2.1)*	20%
1.2.2	SOC Services *(see section 4.1.1.2.2*)	15%
2	**Volume 2**	
2.1	**Volume 2.1/2.2**	
2.1.1	Professional Services *(see section 4.1.2.2) / Set Service Fees (see section 4.1.2.3)*	20%
3	**Interviews***	
3.1	Presentations	30%

*Interviews will be held with down-selected offerors only based on their written responses to the RFP.

5 RFP EXHIBITS

5.1 EXHIBIT A: CERTIFICATIONS AND ASSURANCES

I/we make the following certifications and assurances as a required element of the proposal to which this Exhibit A 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:

1. I/we declare that all answers and statements made in the proposal are true and correct.
2. 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.
3. The attached proposal is a firm offer for a period of 90 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 60-day period.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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*

5.2 Exhibit B: Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The prospective offeror certifies to the best of its knowledge and belief that it and its principles:

1. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;
2. 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);
3. 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;
4. 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
5. 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.

Offeror 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 Offeror

_____

Printed Name and Title of Authorized Representative

_____

Signature of Authorized Representative

5.3 EXHIBIT C: AAMVA MUTUAL NONDISCLOSURE AGREEMENT

AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS

MUTUAL NONDISCLOSURE AGREEMENT

This Mutual Nondisclosure Agreement ("Agreement") is made as of _____, 20__ by and between the AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS, a District of Columbia nonprofit corporation ("AAMVA") and _____, a _____ corporation ("Company"). AAMVA and Company may be referred to individually as a "Party" or, collectively, as the "Parties".

Preliminary Statement

AAMVA and the Company are engaged in discussions regarding a possible business relationship pursuant to which each may disclose (as "Discloser") to the other (as "Recipient") certain Confidential Information (defined below). For the purpose of facilitating those discussions, AAMVA and the Company desire to enter into this Agreement.

Agreements

AAMVA and Company agree as follows:

1. **Confidential Information.**
   a. As used in this Agreement the term "Confidential Information" means all non-public business, technical, financial, marketing, or proprietary information disclosed to the Recipient by the Discloser orally, in writing, or in any other medium. Information generated by Recipient that contains, reflects, or is derived from information disclosed by either party to this Agreement shall constitute Confidential Information.
   b. Confidential Information does not include the following information:
      i. Information which is or becomes generally available to the public other than as a result of Recipient's breach of its obligations under this Agreement;
      ii. Information known to Recipient independently of its relationship with Discloser, including information learned by Recipient from a third party entitled to disclose it, or information known by Recipient prior to its relationship with Discloser; or
      iii. Information independently developed by Recipient without use of the Disclosing Party's Confidential Information.
2. **Treatment of Confidential Information.** The Parties agree that Confidential Information shall be treated as follows:

a. Recipient shall use Confidential Information only for the purpose stated above and for no other purposes.

b. Recipient shall not disclose, divulge, or transfer, either directly or indirectly, the Confidential Information to any third party without the written consent of Discloser.

c. Recipient shall maintain the confidentiality of the Confidential Information by using the same degree of care (which shall be no less than reasonable care) as Recipient uses to protect its own confidential information of a similar nature.

d. Recipient shall restrict its dissemination of Confidential Information to those of its employees, third-party contractors, advisors, and employees, third-party contractors, and advisors of Affiliates who have a need to know the Confidential Information and who are legally bound by confidentiality obligations at least as protective as those set forth in this Agreement. An "Affiliate," of the Company includes any corporation or other person or other entity that directly or indirectly controls, is controlled by, or is under common control with the Company. An ownership or similar interest representing 50% or more of the total interests then outstanding of the pertinent entity shall constitute "control" for the purposes of this definition.

e. Recipient shall promptly notify Discloser in writing of any unauthorized use or disclosure of Confidential Information, including a detailed description of the circumstances of the disclosure and the parties involved, and cooperate with the Discloser to remedy such unauthorized use or disclosure.

f. All Confidential Information shall remain the exclusive property of the Discloser. Recipient will do nothing to compromise or diminish Discloser's rights in any Confidential Information. At the conclusion of the relationship between the Parties, and promptly upon Discloser's written request, Recipient will return the Confidential Information to Discloser, or at Discloser's option, Recipient will destroy such Confidential Information and promptly provide Discloser with written confirmation of such destruction; *provided, however*, that Recipient may retain copies of Confidential Information for bona fide legal, financial, audit, or accounting purposes. The provisions of this Agreement shall, notwithstanding its expiration or termination, continue to apply to all Confidential Information so long as it is retained by the Recipient.

3. **Limitations on Recipient's Obligations.** If Recipient becomes legally compelled (by deposition, interrogatory, request for documents, subpoena, civil investigative demand or similar process by court order of a court of competent jurisdiction, or in order to comply with applicable requirements of any government department or agency or other regulatory authority) to disclose any of the Confidential Information provided by Discloser, Recipient shall provide Discloser with prompt written notice of such requirements so that the Discloser may seek a protective order or other appropriate remedy or waive compliance with the terms of this Agreement. If such protective order or other remedy is not obtained or Discloser waives compliance with the provisions of this Agreement, Recipient agrees to provide only that portion of the Confidential Information provided by the Discloser which is legally required

and to exercise its reasonable efforts to obtain assurances that confidential treatment will be afforded to such Confidential Information.

4. **Term, Termination and Survival.** This Agreement shall have a term of 2 years and may be terminated by either Party upon at least 30 calendar days prior written notice. Except as otherwise provided in this Agreement, the rights and obligations of the Parties under this Agreement with respect to any Confidential Information disclosed prior to expiration or termination of this Agreement shall survive such expiration or termination for a period of 2 years.
5. **Remedies.** The Recipient acknowledges and understands that the unauthorized use or disclosure of the Confidential Information may cause the Discloser irreparable damage. The Discloser shall have the right to seek equitable and injunctive relief to prevent such unauthorized use or disclosure and to recover the amount of all such damage to the Discloser in connection with such use or disclosure.
6. **Severability.** If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, the remaining provisions shall remain in full force and effect.
7. **Assignment.** This Agreement may not be assigned by either party without the prior written approval of the other party.
8. **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia, without regard to its principles of conflicts of laws.
9. **Entire Agreement.** This Agreement reflects the entire understanding of the parties relative to the subject matter hereof, and supersedes all prior representations and understandings, whether oral or written.
10. **Amendment.** This Agreement may not be modified except in a writing signed by both parties.

IN WITNESS WHEREOF, AAMVA and the Company, by their duly authorized representatives, have caused this Agreement to be executed and delivered.

AAMVA	**COMPANY**
By: _____	By: _____
Harold M. Gollos	Name
Director, Contracts Administration	Title