safe drivers
safe vehicles
secure identities
saving lives!

AAMVA

REQUEST FOR PROPOSAL

No. FY20-21514

Managed Services Provider for Silver Peak Software Designed Networking (SD-WAN)

December, 2019

AAMVA - Official Use Only

American Association of Motor Vehicle Administrators

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.

CONTENTS

1 INTRODUCTION

1.1 PURPOSE

The American Association of Motor Vehicle Administrators, hereafter "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.

AAMVA is currently in the process of migrating core business applications and central databases from traditional data centers to the Azure Government and Commercial cloud environments; and as a result, selected Silver Peak Software-Defined Wide Area Networking, hereafter "SD-WAN", to modernize AAMVA's external network access provided primarily through a private MPLS network, hereafter "AAMVAnet". Additional forms of external access to these core applications and services include public Internet based point-to-site VPN and web services directly to the servicing data centers.

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

1. Managed services for Silver Peak SD-WAN — Required
2. Provide professional services for Silver Peak SD-WAN — Required
3. Sell Silver Peak SD-WAN hardware - Required

Organizations responding should have extensive experience with Silver Peak SD-WAN Solution in the following areas but not limited to:

1. Design and implementation in traditional on premise data centers as well as Azure government and commercial clouds.
2. Integration of MPLS networks and Azure cloud (Government & Commercial) access technologies/solutions.
3. Managed network services support for Silver Peak SD-WAN.
4. Proven record of successful Silver Peak SD-WAN implementations.

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 who 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.

AAMVAnet is a fully managed, private network environment built upon Verizon Business Solutions' Private IP (PIP) MPLS core network service. External access to AAMVAnet is primarily via private leased line circuits procured from Verizon by AAMVA on behalf of AAMVA's contracted subscribers, partners and service providers. AAMVAnet is also interconnected to some service provider and partner networks through network-to-network interfaces or partner provided private leased lines.

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.

On an average day, some systems process over 4 million transactions. Some of the databases hold over 1 billion records and exceed 1 TB of data. The infrastructure supporting those systems across their lifecycle exceed 200 servers spread across six data centers managed by different content security policies (CSP). The connectivity is accomplished, for the most part, through a private nationwide multiprotocol label switching (MPLS) network, and through Internet access.

All of AAMVA critical systems are developed in house using Microsoft technologies, mainly Microsoft .NET and SQL Server. The servers' operating systems range from Windows Server 2003 to Windows 2012. More than 70% of the servers are virtualized.

In addition to the critical applications, AAMVA also operates many systems typical of an association such as email, 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.

1.2.2 AAMVA Capabilities

AAMVA has highly technical and competent staff that consists of approximately 100 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 is capable of deploying servers, managing data centers, and developing and supporting applications.
The AAMVA teams involved with data center operations are organized as follows:

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

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.

1.3 Minimum Qualifications

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

1.4 Period of Performance

The performance period for the anticipated contract:

Contract Period	Start	End
Base Contract	Contract Award	September 30, 2020
Option Year 1	October 1, 2020	September 30, 2021
Option Year 2	October 1, 2021	September 30, 2022

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	Siedah Ross, Procurement Specialist
Address	4401 Wilson Boulevard, Suite 700
City, State, Zip Code	Arlington, Virginia 22203
Phone Number	703-908-2861
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 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	Dec 6, 2019
Written Intent to Bid Due	Dec 13, 2019
Written Questions Due From Vendors About Scope Or Approach	Dec 15, 2019
Pre-Proposal Conference	Jan 16, 2020
Proposals Due	Jan 27, 2020
Evaluate Proposal	Jan 28 – Feb 4, 2020
Finalist Presentations and Site Walkthroughs	Feb 10 – Feb 14, 2020
Announce “Apparent Successful Contractor”	Feb 17 , 2020
Contract negotiations	Feb 18 – Feb 28, 2020
Contract presented to AAMVA Board for approval	April 2020

Activity	Date
Contract execution	Post AAMVA board meeting in April 2020

AAMVA reserves the right to revise this schedule.

2.3 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 (FY18-012) to the attention of the RFP Coordinator, Wesley Day.
- 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 FYXX-XXX by <company name>.pdf"
  - **File 2:** Shall include Volume IV Price proposal response labeled "Price proposal response for RFP FYXX-XXX by <company name>.pdf". Please also include the signed Exhibits A and B.

2.4 Acceptance Period

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

2.5 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.

2.6 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.

2.7 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 *§5.1 Exhibit A: Certifications and Assurances* to this solicitation. AAMVA will review requested exceptions and will accept or reject them at its sole discretion.

2.8 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.

2.9 No Obligation to Contract

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

2.10 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

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

1. Managed Services for Silver Peak SD-WAN (Required)
2. Professional services for designing and implementing Silver Peak SD-WAN (Required)
3. Resell Silver Peak SD-WAN hardware (Required)

3.1 Managed Services For SD-WAN Services (Required)

3.1.1 Managed Services

3.1.1.1 Network Operations Center

The provider must provide a continual, around the clock (24 hours, 7 days a week, 365 days a year) manned network operating center (NOC) support and monitoring. This includes, but is not limited to network monitoring and health performance, network availability, and network security reporting. These services must be offered within the continental United States.

This support will be required for all of AAMVA's Silver Peak SD-WAN deployment sites. The list of sites is located in appendix 1 of the RFP.

3.1.1.2 On-Site Support

The provider must provide a continual, around the clock (24 hours, 7 days a week, 365 days a year) support for hardware and software related issues. This includes but not limited to, the provider or a representative replacing faulty parts, upgrading the Silver Peak SD-WAN device and deploying new SD-WAN devices. These services apply to all AAMVA hub sites and customers sites.

3.1.1.3 Issue Tracking

The provider shall use an industry standard tracking system to thoroughly documents issues and requests for AAMVA. The provider shall facilitate a customer portal for AAMVA to track help desk ticketing and incident resolution, contact information, as well as storage of the customer solution/design for continuity among support staff. Details of AAMVA's environment within the custody of the provider must be readily available to any authorized personnel of the provider, including, but not limited to, architecture diagrams, network connectivity diagrams, service level agreements (SLA), contacts, network configurations, and monitoring alerts.

3.1.1.4 Service Level Requirements

The provider shall follow the problem severity guidelines specified in Table 1 for assigning severity levels for incident creation.

Severity	Criteria	Response Time (Guarantee)	Resolution Time (Target)
Urgent (Sev1, Sev1.5)	*Critical Event*: Central Site outage and/or state outage (either PROD or CERT (AAMVA's state testing environment)) that impact one or more states/members.	1 Support hour	2 Support hours
High (Sev2)	*Significant Event*: That can impact AAMVA members in production or test regions.	2 Business hours	8 Business hours
Medium (Sev3)	Requests and Compliance issues, not deemed critical enough to be a SEV1 or SEV2	8 Business hours	48 Business hours
Low (Sev4)	Reserved for user requests, investigations, research, etc.	24 Business hours	10 Business days

Table 1: Severity Level Guidelines

AAMVA requires notifications of service outages or degraded performance. The provider shall communicate notifications via a support ticket, email, telephone call, automated phone calling for sev 1 events or all of the above methods, depending upon the severity of the situation. Protocols would need to be in place before vendor selection is finalized. 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 provide root-cause analysis notifications within two business days of the incident.

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.

3.1.1.5 Systems Monitoring

AAMVA requires monitoring services which must cover all the services provided by the provider, including but not limited to:

- Network connectivity (i.e., whether the network is up or down, and real-time bandwidth usage.)
- Full stack network monitoring
- Performance indicator
- Network latency
- Network Utilization (e.g., memory, disk usage, bandwidth)
- Trending (for minimum of one year)
- Sharing of the monitored data with AAMVA through a portal
- High Availability—provider must have capabilities to detect failover between AAMVA's MPLS infrastructure and SD-WAN in the event of workload and services failover.

3.1.1.6 Troubleshooting Tools

The provider must be able to provide tools and systems to accommodate a structure whereby AAMVA can access all customer resources. AAMVA must have "master" access to all customer equipment via a streamlined single login.

3.1.1.7 Carrier Escalation Management

The provider will be required to serve as the first point of contact for contacting and resolving issues with transport carriers supporting the SD-WAN solution. This includes the provider initialing and resolving issues with AAMVA's MPLS provide, Verizon, as well as additional forms of transport such as internet.

Additionally the provider will also be responsible for configuring new devices to account for all forms of transport as well.

3.1.1.8 Backup Services

The provider must be able to configure, schedule, and manage backups for all the SD-WAN devices configurations. The provider must encrypt all backup files and data, and must manage encryption keys.

3.1.1.9 Patching

The provider must provide capabilities to deploy and install patches as made available by the SD-WAN provider. From time to time, AAMVA may request that specific patches be performed. The provider must be capable to support these out-of-cycle requests.

The provider shall have processes in place to support AAMVA's network operations. These processes must (but must not limited to):

- Support established provider policies
- Be thoroughly documented
- Be reviewed and adjusted, as necessary, at least annually by the provider
- Be reviewed with AAMVA on a recurring basis

3.1.1.10 Billing

The provider must be able to provide AAMVA with an invoice consisting of but not limited to:

- AAMVA Customer location
- AAMVA internal project numbers

Additionally the provider must be able to integrate their invoicing into AAMVA's current electronic billing process.

3.1.2 Account Management

AAMVA requires a primary and backup account representative who is responsible for ensuring that all provider SLAs are met. The account representative must communicate all service outages or degraded performance in a recurring performance report and on a weekly basis via a recurring 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. Please provide location and hours of operation of the account management team and technical staff.

The provider must be able to provide a project management team for new installations as well as existing service changes.

3.1.3 Dedicated Engineering Staff

The provider must assign dedicated staff as an engineering support team. The dedicated staff is not expected to provide immediate, around-the-clock (24 hours a day, 7 days a week) support, but rather must be capable of acting as an advocate for AAMVA during outage events. The provider must make these staff persons accessible at all times, or must 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 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

In addition, the Provider shall comply with the Service Provider Information Security Requirements defined in Exhibit C.

3.1.5 Cost Optimization

The Provider must have in place the tools and processes that will allow AAMVA to best optimize AAMVA's SD-WAN resources and services in on premise data centers, customer sites and Azure cloud to reduce costs and gain efficiencies.

3.1.6 Reporting

AAMVA requires a 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
Mean Time to Repair Intervals	Monthly
Tickets that Missed SLA Intervals	Weekly
List of Chronic Issues	Bi-Weekly
Network Availability	Monthly
Backups Success	Daily
Capacity Projections	Quarterly
NOC Incident Response Call Tree	Quarterly
Monitoring Thresholds	Quarterly

3.1.7 Site On-Boarding Schedule

Below is AAMVA's proposed schedule for deployment of the SD-WAN solution. The schedule takes into account the Period of Performance in section 1.4.

Activity	Time Frame
Contract presented to AAMVA Board for approval	April 2019
Contract execution	Post AAMVA board meeting in April 2019
Design and deployment of SD-WAN solution in AAMVA hub sites*	Base Contract Year (6-9 months)
Purchase and deployment of SD-WAN devices to customer sites*	Year 2 and 3

Deployment of the SD-WAN devices to customer sites will be dependent on customer's decision to install the SD-WAN technology.

**List of hub and customer sites are in Appendix 1*

3.2 PROFESSIONAL SERVICES (REQUIRED)

The Provider must be able to provide professional services for all Silver Peak SD-WAN solutions. This includes but not limited to designing, installation and implementing Silver Peak SD-WAN solutions in AAMVA's on premise data centers, Azure Cloud (Government & Commercial) and all of AAMVA's customers in the United States. Please provide examples of prior engagements of this nature.

The provider will be required to work with AAMVA and its Managed Services Provider for Azure Cloud to design and implement the Silver Peak SD-WAN solution for Azure deployments.

3.3SILVER PEAK HARDWARE (REQUIRED)

3.3.1 Hardware

The vendor must be able to quote and sell Silver Peak SD-WAN hardware devices listed in Appendix 2.

3.3.2 Maintenance

All hardware must be quoted for 3 years of hardware and software maintenance.

3.3.3 Pricing

Vendor must provide flexible pricing options for all hardware including CapEx pricing options.

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 boiler plate information in your response.***

- ✓ **Volume I Corporate Information**-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 brief summary of the financial strength of the company.

- ✓ **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.

- ✓ **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 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.

- ✓ **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. Identify any assumptions made to create the Price Proposal. Please include pricing for travel, other direct cost, and any optional services that may be relevant to this RFP.

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. Table 3 indicates how AAMVA will score each Proposal it evaluates.

Table 3: Proposal Scoring

Technical Proposal Evaluation			
ID	Description	Weight	Score
1	Management Proposal	15%	
	i. Account Team/Oral Presentations	5%	
	ii. Corporate Qualifications	5%	
	iii. Corporate Experience	5%	
2	Technical Proposal	50%	
Cost Proposal Evaluation			
3	Cost Proposal	35%	
	i. Terms and Conditions	5%	
	ii. Pricing	30%	
Total Possible Points		100	

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

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.

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

5.3 EXHIBIT C – SERVICE PROVIDER INFORMATION SECURITY REQUIREMENTS

1.1. Standard of Care.

1.1.1. In the course of providing the services, the Service Provider may create, receive, or have access to AAMVA information categorized as confidential or official use only, labeled herein as Protected Information. The Service Provider shall comply with the requirements defined in this document in the creation, collection, receipt, transmission, storage, disposal, use, and disclosure of the Protected Information. The Service Provider shall also be responsible for any unauthorized transmission, access, storage, disposal, use, or disclosure of any Protected Information under its control.

1.1.2. In recognition of the foregoing, the Service Provider shall:

1.1.2.1. Keep and maintain all Protected Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure;

1.1.2.2. Not, directly or indirectly, disclose Protected Information to any person other than employees, or contractors working on behalf of the Service Provider, with a need to access the Protected Information in order to provide the services to AAMVA, and who have been made are of the obligations defined through those requirements (Authorized Persons).

1.1.2.3. Not create, collect, receive, access, or use Protected Information in violation of any law(s), including state, federal, and international law(s) or conventions;

1.2. Information Security.

1.2.1. The Service Provider shall implement and maintain a written information security program including appropriate policies, procedures and risk assessments to maintain the confidentiality and integrity of the Protected Information and the availability of the services provided to AAMVA. The Service Provider shall review the program and the associated documents at least annually.

1.2.2. Without limiting Service Provider's obligations, the Service Provider shall implement security controls that are no less rigorous than those defined in recognized industry best practices, including the International Organization for

Standardization's standards: ISO/IEC 27001 – Information Security Management Systems – Requirements and ISO/IEC 27002 – Code of Practice for International Security Management, the National Institute of Standards and Technology (NIST), and the Cybersecurity Framework or Center for Internet Security, Critical Security Controls (CSC-20).

1.2.3. At a minimum, the Service Provider's safeguards for the protection of the Protected Information shall include: (i) limiting access to Authorized Persons; (ii) securing, both physically and technologically, business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, application, database, and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) encrypting all confidential information stored on any media; (vii) encrypting confidential information transmitted over public or wireless networks; (viii) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Service Provider's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing; (ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (x) providing appropriate privacy and information security training to Service Provider's employees.

1.2.4. During the term of each Authorized Person's employment or retention through subcontract by the Service Provider, the Service Provider shall at all times cause such Authorized Persons to abide strictly by AAMVA security requirements. The Service Provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use, or disclosure of Protected Information by any of Service Provider's officers, partners, principals, employees, agents, or contractors.

1.2.5. At least 15 days prior to making any material changes to the Service Provider's security program or controls, the Service Provider shall notify AAMVA of the change in writing.

1.2.6. Upon AAMVA's written request, Service Provider shall provide AAMVA with a network diagram that outlines Service Provider's information technology network infrastructure and all equipment used in relation to fulfilling its obligations under this contract, including, without limitation: (i) connectivity to AAMVA and AAMVA managed equipment, and all third parties who may access Service Provider's network to the extent the network contains Protected

Information; (ii) all network connections, including remote access services and wireless connectivity; (iii) all access control measures (for example, firewalls, packet filters, intrusion detection and prevention services, and access-list-controlled routers).

1.3. Security Incident Procedures.

1.3.1. For purposes of this Section 1.3, Security Incident means the acquisition, access, use, or disclosure of Protected Information in a manner not permitted under these requirements which compromises the security of the Protected Information, or unauthorized access to services or equipment that create a risk to AAMVA.

1.3.2. The Service Provider shall:

1.3.2.1. Upon execution of the contract, provide AAMVA with the name and contact information for an employee of the Service Provider who shall serve as AAMVA's primary security contact and shall be available to assist AAMVA twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a security incident;

1.3.2.2. Notify AAMVA by phone and by email of a security incident as soon as practicable, but no later than eight (8) hours after the Service Provider confirms the security incident involves any Protected Information;

1.3.2.3. Service Provider shall, at its own expense, use best efforts to immediately contain and remedy any security incident and prevent any further security incident;

1.3.2.4. Submit a written report of the incident via email to security@aamva.org within forty-eight (48) hours; providing reasonable detail concerning the incident, including (a) the nature and impact of the incident, (b) an assessment of immediate risks, (c) corrective actions already taken, and (d) corrective actions to be taken;

1.3.2.5. To the extent the security incident includes personal identifiable information, (a) cooperate with regulators and law enforcement, in addition to AAMVA, to prevent any further unauthorized use and to notify affected individuals,(b) as required by applicable law; bear the costs associated with compliance with applicable breach notification laws;

1.3.2.6. Agree that it shall not inform any third party of any security incident involving the Protected Information without first obtaining AAMVA's prior written consent, other than to inform a complaining AAMVA customer that the matter has been forwarded to AAMVA.

1.3.2.7. Agree to maintain and preserve all documents, records, and other data related to any security incident.

1.4. Oversight of Security Compliance.

1.4.1. Upon AAMVA's written request, the Service Provider shall make available to AAMVA for review all of the following, as applicable: Service Organization Controls (SOC) Type 2, or 3 audit reports, vulnerability assessment and penetration test pertaining to the infrastructure used by the service provider to provide the services to AAMVA, and any reports relating to its ISO/IEC 27001 or NIST certification.

1.4.2. The Service Provider will promptly address any exceptions noted on the SOC reports, or other audit reports, with the development and implementation of a corrective action plan by Service Provider's management.

1.4.3. Upon AAMVA's written request, the Service Provider shall promptly and accurately complete a written information security questionnaire provided by AAMVA, or a third party on AAMVA's behalf, regarding Service Provider's business practices and information technology environment in relation to all Protected Information being handled and/or services being provided by Service Provider to AAMVA pursuant to this contract.

1.5. Return or Destruction of Protected Information.

At the term of this contract, at AAMVA's written request, the Service Provider shall comply with all directions provided by AAMVA with respect to the return or disposal of AAMVA's Protected Information.

6 APPENDIX

6.1 APPENDIX 1: LIST OF AAMVA SITES

AAMVAnet Sites and Addresses.xlsx

6.2 APPENDIX 2: AAMVA SILVER PEAK BOM

AAMVA Silver Peak BOM.xlsx