

AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS

SPEXS

STATE POINTER EXCHANGE SERVICES

PRIVACY IMPACT ASSESSMENT

6.0 | 2.0

System Release | Document Version




American Association of
Motor Vehicle Administrators


This document outlines the privacy impact assessment (PIA) for the State Pointer Exchange Services (SPEXS).


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



American Association of
Motor Vehicle Administrators

Address  AAMVA, Inc.
4401 Wilson Boulevard, Suite 700
Arlington, Virginia 22203

Telephone  1-703-522-4200

Fax  1-703-522-1553

E-mail : HelpDesk@aamva.org

Website  <http://www.aamva.org>

The American Association of Motor Vehicle Administrators (AAMVA) produced this document. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage or retrieval systems, for any purpose other than the intended use by AAMVA, without the express written permission of AAMVA.

© 2016 AAMVA. All rights reserved.

This document was prepared, at least in part, under a grant from the Federal Emergency Management Agency's (FEMA) Grant Programs Directorate (GPD) United States Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of FEMA/GPD or the US Department of Homeland Security.

The primary purpose of the State Pointer Exchange Services (SPEXS) is to provide information of use to state driver's license agencies in the issuance of driver's licenses. Participation in SPEXS is voluntary and is totally independent of a state's decision whether or not to seek compliance with the REAL ID Act. If a state chooses to pursue REAL ID compliance, SPEXS can be part of the state's overall compliance program. However, SPEXS is intended to be useful to any state, regardless of its decision to comply with REAL ID.

AAMVA – Official Use Only

Do not share with or forward to parties except as necessary to conduct the business for which this document was clearly intended. If in doubt, contact the originator for additional guidance. If you believe that you have received this document in error, please advise the sender, then delete or destroy the information.

CONTENTS

1	Introduction	1
1.1	Abstract.....	1
1.2	Overview	1
2	Characterization of the Information	3
2.1	types of Information.....	3
2.2	Sources of Information	3
2.3	Purpose Of Information	3
2.4	Collecting Information.....	4
2.5	Accuracy of Information.....	4
2.6	Legal Authority to Collect Information	5
2.7	Identified Privacy Risks and Mitigations.....	5
3	Information Usage.....	7
3.1	Description of Information Usage	7
3.2	Analysis of Information	7
3.3	Use of Commercial or Publicly-Available Data.....	8
3.4	Controls to Ensure Proper Information Handling.....	8
4	Information Retention	9
4.1	Retained Information.....	9
4.2	Length of Retention	9
4.3	Retention Schedule Approval.....	9
4.4	Information Retention Risks.....	9
5	Internal Sharing and Disclosure.....	11
5.1	Sharing Information Internally.....	11
5.2	Authorization for Internal Sharing.....	11
5.3	Security Controls for Internal Sharing and Transmission.....	11
5.4	Privacy Risk and Mitigation for Internal Sharing.....	11
6	External Sharing and Disclosure	12
6.1	Sharing Information Externally.....	12
6.2	Authorization for External Sharing.....	12
6.3	Security Controls for External Sharing.....	12
6.4	Privacy Risk and Mitigation for External Sharing.....	12
7	Notice	14
7.1	Providing Notice	14
7.2	User Right to Decline	14

- 7.3 User Right to Consent to Use 14
- 7.4 Privacy Risk and Mitigation 14
- 8 Access, Redress and Correction..... 15**
 - 8.1 Individual Access..... 15
 - 8.2 Correction of Information 15
 - 8.3 Notification of Procedures to Correct Information 15
 - 8.4 Alternatives to Formal Redress 15
 - 8.5 Privacy Risk and Mitigation 15
- 9 Technical Access and Security 17**
 - 9.1 Procedures for System Access 17
 - 9.2 Contractor Access 17
 - 9.3 Privacy Training 17
 - 9.4 Security Assessment and System Authorization 18
- 10 Technology 19**
 - 10.1 Project Type 19
 - 10.2 System Development Stage 19
 - 10.3 Technology Privacy Concerns 19
- Glossary of Acronyms 20**

1 INTRODUCTION

1.1 ABSTRACT

The availability of information, including personal information, is made all the easier today due to advancements in information sharing technologies, storage, networks, and the creation of new information systems. The E-Government Act of 2002 mandates an assessment of the privacy impact of any substantially revised or new information system, thus recognizing that these advances have important ramifications for the protection of personal information contained in such systems. The document that results from these mandated assessments is called a Privacy Impact Assessment (PIA).

This PIA also addresses a requirement of the contract between the Mississippi Department of Public Safety and AAMVA, for the development and pilot operations of the State Pointer Exchange Services (SPEXS)¹, as well as a requirement from the DIVS² (DL/ID Information Verification Systems) Privacy Policy for Vendors. The PIA is used to identify and mitigate privacy risks associated with the operation of the service.

1.2 OVERVIEW

The primary purpose of the State Pointer Exchange Services (SPEXS) is to provide information of use to State driver's license agencies (SDLAs) in the issuance of driver's licenses (DL) or ID cards. SPEXS fulfills all CDLIS (Commercial Driver's License Information System) requirements and supports the State-to-State Verification Service project within the DIVS initiative.

CDLIS was established under the Commercial Motor Vehicle Safety Act (CMVSA) of 1986³ and is based on the Federal Motor Carrier Safety Regulations (FMCSRs) in 49 CFR 383 and 384. CDLIS is a nationwide capability allowing the SDLAs to comply with the Federal requirement that each commercial driver, as defined in the Federal regulations, has only one US-issued driver's license and one complete driver record.

DIVS is a not-for-profit corporation formed by the State of Mississippi to organize, implement, and coordinate electronic information exchange between the SDLAs for the purpose of detecting and deterring driver license and identification card applicant fraud. The function of S2S is to provide an electronic tool for States to use to enforce their own laws regarding the issuance of driver licenses and ID cards. Specifically, all US SDLAs have existing laws that state that a person is not allowed to have more than one current US-issued driver's license. Some States have laws that go even further in that they don't allow a person to have more than one credential (i.e. they can have either a driver's license or an ID card, but not both). S2S provides a means for States to determine whether or not a credential applicant already holds a driver's license or identification card and then take whatever action is called for based on State law.

¹ Project Number 38394 – Software Development And Hosting Agreement Between the American Association of Motor Vehicle Administrators and the Mississippi Department of Information Technology Services as Contracting Agent for the Mississippi Department of Public Safety.

² DIVS is a not-for-profit corporation formed by the State of Mississippi to organize, implement, and coordinate the electronic information exchange between the SDLA for the purpose of verifying identification information provided by driver license and identification card applicants. The organizing Board of Directors of DIVS is comprised of representatives from the States of Mississippi, Indiana, Florida, Kentucky and Nevada.

³ <http://www.fmcsa.dot.gov/registration-licensing/cdl/cdl.htm>

SPEXS also supports the requirements of the REAL ID Act; however, participation in SPEXS is voluntary and is totally independent of a State’s decision whether or not to seek compliance with the REAL ID Act. SPEXS is intended to be useful to any State, regardless of its decision to comply with REAL ID.

SPEXS is comprised of the followings:

- A set of specifications and procedures that govern the information exchange between participating organizations
- Standardized system interfaces supporting the communications between those organizations’ systems
- The SDLA systems that hold detailed applicant information
- A pointer index operated by AAMVA, which identifies which State has the authoritative record for a credential holder (this State is also referred to as the State of Record or SOR).

For the purpose of this document, the scope is limited to the SPEXS pointer index.

2 CHARACTERIZATION OF THE INFORMATION

The following sub-sections are intended to provide answers to questions that define the scope of the information within the pointer index.

2.1 TYPES OF INFORMATION

The information in the pointer index is limited to what is directly relevant and necessary to accomplish its specified purpose(s) and consists of:

For all drivers that have a pointer within the index:

- Driver information such as the name(s), including former name(s), date of birth, gender and a portion of the social security number
- Credential information, including type of credential issued, credential number (e.g. driver license number), including past credential numbers

For only commercial drivers, as defined by Federal regulation:

- Full social security number

The system also stores meta-data information, such as date/time when a pointer is added or updated.

2.2 SOURCES OF INFORMATION

What are the sources of information in the system?

All PII comes from participating SDLAs'. The applicant provides the information to the SDLA when they apply for a credential.

Meta-data is generated by the SPEXS software.

SPEX does not require that any information be collected by the States beyond that which States already collect.

2.3 PURPOSE OF INFORMATION

Why is the information being collected, used, and disseminated?

The information is collected, used and disseminated in order to improve highway safety, homeland security, and identity security by:

- Detecting and deterring driver license and ID card fraud,
- Preventing a person from spreading driving convictions over multiple driving records,
- Inhibiting identity theft
- Inhibiting government benefits fraud

All States must address the following laws and regulations:

- Every State has laws that make it a crime for an individual to possess more than one US-issued driver's license

- Every State has laws that make it a crime to falsify information provided on an application for a driver's license or ID card
- All States must comply with the Commercial Motor Vehicle Safety Act (CMVSA) of 1986 and its subsequent laws and regulations

Some States have laws that make it a crime for an individual to possess more than one US-issued credential (i.e. they can possess a driver's license or and ID card, but not both).

In addition, States that choose to be REAL-ID compliant also must adhere to the Real ID Act of 2005 and its subsequent regulations.

The requirements that are the subject of this PIA come from two sources:

- The requirements documented by DIVS for the S2S project, that were given to AAMVA under the Mississippi contract, which address existing State law and REAL ID requirements, and
- Federal CDL legislation and regulation.

2.4 COLLECTING INFORMATION

How is information collected?

AAMVA does not collect any information from an individual.

The applicant applying for a credential, such as a driver's license, a commercial driver's license or an ID card, provides information to the SDLA.

S2S does not require that any information be collected by the States beyond that which States already collect as required by their state laws and regulations.

Collection of data related to S2S is determined by State law and regulation.

Collection of data related to CDLIS is determined by a combination of State and federal law and regulation.

The SDLA contributes the necessary applicant information to the pointer index through a combination of real-time information exchange (referred to as online transactions) and asynchronous batch processes (referred to as batch transactions).

2.5 ACCURACY OF INFORMATION

How is the information checked for accuracy?

The accuracy of the PII is the responsibility of the State that contributed the pointer. Each State has their own methods for checking the accuracy of the information.

In addition, each State conducts a Master Pointer Record (MPR) Data Quality Validation and Verification process, for pointers associated with commercial drivers, at least once a year. This process compares the State information stored in the pointer index with that of the SDLA database, and reports on any inaccuracies. Discrepancies are tracked through to resolution. The FMCSA monitors resolution of such discrepancies for all commercial records.

A similar process has been developed for non-commercial driver pointers. DIVS and AAMVA will be working with each S2S participant to develop a schedule and resolve any information discrepancies that are identified.

2.6 LEGAL AUTHORITY TO COLLECT INFORMATION

What specific legal authorities, arrangements, and/or agreements define the collection of information?

States have the authority to collect this information based on their individual State laws and regulations.

AAMVA is authorized to house this information based on:

- Individual User Agreements between AAMVA and the State pilot participants, related to operating S2S
- An agreement between FMCSA and AAMVA related to operating CDLIS, called the “CDLIS Cooperative Agreement between FMCSA and AAMVA – June 9, 2008”
- A contract between Mississippi and AAMVA related to non-CDL drivers and ID card holders

2.7 IDENTIFIED PRIVACY RISKS AND MITIGATIONS

Given the amount and type of data collected, what are the identified privacy risks and how are they mitigated?

Because the SPEXS pointer index contains PII, there are privacy risks that must be addressed. Access to the pointer index must be restricted to authorized users and any potential unauthorized access or misuse of the information must be detected and addressed.

It is important to understand the environment so that the assignment of privacy mitigation responsibilities can be understood. When the S2S project began, the first order of business was to determine the best design for the service. Therefore, prior to developing the pointer index, AAMVA through the State of Kentucky and in collaboration with 19 other States⁴, conducted a thorough analysis of various design models for S2S, ranging from a completely distributed solution across all the States, to one that would consist of having a large central database containing all the driver detail records. Privacy was one of the significant design criteria concerns. The conclusion⁵ was that a pointer index that contains the minimum amount of information necessary to locate the detail records stored within a State offered the best design, including the best privacy protection advantages. This design limits the potential exposure of PII while at the same time provides States with an effective, affordable service to detect and deter fraud.

Because of the design of S2S, States have a significant responsibility to address privacy risks since the detail regarding the individual is stored there. Each State has processes and procedures in place that address these concerns as they are already sharing similar information as part of CDLIS. The User Agreement that is signed by a State when it begins participation describes these responsibilities as they relate to S2S.

The privacy risks with the SPEXS pointer index are addressed through the following controls:

- Formally defined roles and obligations of each participating organization
- Assignment of oversight and compliance monitoring functions

⁴ California, Florida, Georgia, Idaho, Indiana, Iowa, Kentucky, Maryland, Massachusetts, Missouri, Montana, Nevada, New Jersey, North Carolina, South Carolina, South Dakota, Texas, Washington, Wisconsin

⁵ REAL ID State-to-State Verification Design Alternatives Analysis; November 2008

- Reducing the data elements maintained to the absolute minimum required to achieve the SPEXS purpose(s)
- Operating the pointer index in compliance with the Federal Information System Management Act (FISMA), and the security & privacy controls defined by the National Institute of Standards and Technology, including, but not limited to:
 - Implementing strong access controls to ensure that only authorized users/systems can contribute, access and update the information
 - Implementing the necessary audit trails to track changes to the information records
 - Implementing data quality checks and processes to periodically verify the quality and integrity of the information
 - Implementing a comprehensive backup strategy
 - Instituting a security incident response plan, including steps for handling and notification related to a breach of PII
 - For AAMVA employees and contractors, penalties for misuse of PII could include disciplinary action up to and including termination of employment or contract and/or civil and criminal prosecution, as appropriate.

3 INFORMATION USAGE

The following sub-sections are intended to clearly delineate the use of information and the accuracy of the data being used.

3.1 DESCRIPTION OF INFORMATION USAGE

How is the information used?

The information is used by the SDLAs to comply with the purposes specified in [2.3 Purpose of Information](#). Jurisdictions that do not participate in S2S only have access to CDLIS data.

Only SDLAs participating in S2S have access to non-commercial pointers. All SDLA's have access to pointers related to CDL holders. Access to SPEXS is limited to the purpose of processing an application for a State credential, except as shown below regarding the CDL portion of SPEX.

In accordance with Federal transportation regulations, and in support of the U.S. Department of Transportation's objective to make America's roads safer, access to CDL information in SPEXS is provided to support the following tasks related to commercial drivers:

- Federal Motor Carrier Safety Administration (FMCSA) for the monitoring of and overall compliance with the commercial driver's license CDL program
- Interprovincial reciprocal information exchange between the U.S. and Canada related to the operation of U.S. commercial drivers in Canada
- Law enforcement access, in relation to public safety operations, such as roadside inspections of commercial drivers
- Independent, private sector organizations providing background check services that include verification of a commercial driver status and history prior to, and during employment, subject to the driver's consent

Information system controls are used to prevent the above entities from accessing data that is not part of the CDL Program.

As the pointer index operator, AAMVA maintains agreements and detailed specifications and procedures for each type of allowable access to SPEXS.

Finally, authorized personnel from AAMVA may also use the information in SPEXS to provide support to the SDLA and the aforementioned organizations in accordance with defined policies and procedures.

3.2 ANALYSIS OF INFORMATION

What types of tools are used to analyze data and what type of data may be produced?

Data analysis is limited, and achieved through the use of reports or batch processes.

All data analysis is geared toward ensuring compliance with the system specifications and any associated regulations. The reporting feature enables authorized users to query and extract a predefined set of information from the pointer index, with data formatted into a report style meaningful to the requestor. The batch pro-

cesses are automated; the processes used to initiate a batch process and the data it produces are strictly controlled by the pointer index. The system also ensures that only the data relevant to, and authorized for, a particular user, SDLA, or inquirer is accessed or shared.

3.3 USE OF COMMERCIAL OR PUBLICLY-AVAILABLE DATA

Does the system use any commercial or publicly-available information or data? If so, explain why and how it is used.

The SPEXS pointer index does not rely on commercial or publicly available data in any way. The only sources of PII within SPEX are the SDLAs.

3.4 CONTROLS TO ENSURE PROPER INFORMATION HANDLING

Are there any controls in place to ensure that information is handled in accordance with the above described uses?

Each of the SPEXS participating organizations recognize the importance of, and advocate for, strong security and privacy controls. The oversight bodies, represented by the DIVS, AAMVA and FMCSA, play an essential role in specifying the minimum security and privacy requirements, and for monitoring ongoing compliance.

Proper information handling is addressed through the following controls:

- Formally defined the roles and obligations of each participating organization
- Assigned oversight and compliance monitoring functions
- Tightly control the organizations having access to the information to ensure it complies with the regulations and requirements for which SPEXS was instituted
- Operate the pointer index in compliance with the Federal Information System Management Act (FISMA), and the security & privacy controls defined by the National Institute of Standards and Technology, including, but not limited to:
 - Implement strong access controls to ensure that only authorized users/systems can contribute, access and update the information
 - Implement the necessary audit trails to track changes to the information records
 - For AAMVA employees and contractors, penalties for misuse of PII could include disciplinary action up to and including termination of employment or contract and/or civil and criminal prosecution, as appropriate.

4 INFORMATION RETENTION

The following sub-sections are intended to describe how long information will be retained after the initial collection.

4.1 RETAINED INFORMATION

What information is retained?

The SPEXS pointer index retains the information defined in the section 2.1 – Type of Information, as well as the audit trails associated with the addition, change or deletion of records.

The SPEXS information exchanged between two participating organizations is not retained, other than the meta-data supporting the exchange (i.e. origin, destination, date and time and type of the request etc.).

4.2 LENGTH OF RETENTION

How long is the information retained?

The regulations governing commercial driver's license (CDL) issuance specify how long a record and its history must be maintained before they can be deleted. This includes the retention periods for CDL convictions and withdrawals in accordance with the Non-Resident Violators Compact and Federal Regulations (49 CFR §384.231(d)). Therefore the retention of a CDLIS pointer is governed by these regulations. Essentially a CDLIS pointer may be deleted once the retention period has been satisfied based on the Federal regulations.

For other types of records, the States follow the SPEXS system requirements, which stipulate that the pointers must be deleted when the State deletes the associated record within their system.

4.3 RETENTION SCHEDULE APPROVAL

Has the retention schedule been approved?

The retention schedule for commercial pointers is defined and approved by Federal regulations.

The retention schedule for other pointers is referenced in 4.2 above and is based on State retention requirements.

A formal record retention schedule is maintained for system artifacts other than the pointers, such as reports, batch files etc. The schedule was reviewed and approved by the participating organizations and AAMVA's privacy officer.

4.4 INFORMATION RETENTION RISKS

What risks are associated with the length of time information is retained and how are those risks mitigated?

AAMVA minimized the data retained to what is necessary to ensure full compliance with the requirements, and to support the required ongoing compliance oversight. The risks are mitigated by:

- Development of a formal record retention schedule addressing all types of pointers

- Formally reviewing and approving the retention schedule
- Instituting periodic verification and validations to ensure record deletions occur in accordance with the retention schedule
- Implementing strong access controls to the stored data
- Encrypting all sensitive information, including PII data in the data store and in the backups
- Implementing a strong backup and disaster recovery strategy

5 INTERNAL SHARING AND DISCLOSURE

The following sub-sections are intended to define the scope of information sharing internally within AAMVA.

5.1 SHARING INFORMATION INTERNALLY

What information is shared internally and for what purpose?

Specific SPEXS pointer index information may be shared internally, within AAMVA, with the authorized personnel, in order to provide help-desk support to those using the SPEXS online and batch transactions. The information shared internally may consist of aggregate, non-identifiable dataset, or detailed record(s) based on the nature of the support requested.

5.2 AUTHORIZATION FOR INTERNAL SHARING

Is the sharing of PII inside AAMVA compatible with the original collection and purpose?

The internal sharing of information is compatible with the purpose for which it was collected. The internal information sharing at AAMVA is subject to AAMVA's privacy policy and conducted in accordance to well defined internal procedures. The procedures are updated, approved and communicated at least once a year.

5.3 SECURITY CONTROLS FOR INTERNAL SHARING AND TRANSMISSION

How is the information shared inside AAMVA and what security measures safeguard its transmission?

The information shared within AAMVA is encrypted while in transport or in storage.

5.4 PRIVACY RISK AND MITIGATION FOR INTERNAL SHARING

What is the privacy risk associated with internal sharing of information and how is the risk mitigated?

The risk of unauthorized disclosure associated with the internal sharing of information is mitigated by:

- Ensuring that all AAMVA personnel receive annual privacy awareness training
- Ensuring that AAMVA maintains a formal Privacy Policy
- Documenting and communicating the standards and procedures by which information can be shared; ensuring that such standards and procedures are reviewed and formally approved and that AAMVA personnel training occurs at least once a year.
- Ensuring that AAMVA personnel signs, on an annual basis, a Security and Confidentiality Agreement that denotes their responsibilities related to the protection of PII and the penalties for un-authorized use, which may include disciplinary action up to, and including, termination of employment or contract, and/or civil and criminal prosecution, as appropriate
- Develop and implement an incident response procedure with specific steps for the handling of a PII breach; including the breach notification requirements

6 EXTERNAL SHARING AND DISCLOSURE

The following sub-sections are intended to define the scope of information sharing outside of AAMVA.

6.1 SHARING INFORMATION EXTERNALLY

With which external organization(s) is the information shared?

Subject to the provision of the Privacy Act of 1974, the Driver Privacy Protection Act (DPPA), and specific State regulations, the SPEXS pointer index information is shared with the participating organizations described in 3.1 Description of Information Usage.

6.2 AUTHORIZATION FOR EXTERNAL SHARING

Is the sharing of personally identifiable information (PII) outside AAMVA compatible with the original collection? What legal mechanism allows the program or system to externally share the PII outside of AAMVA?

The external sharing of information is compatible with the purpose for which it was collected and necessary to address the State and Federal rules and regulations. The legal authority allowing for the sharing of PII is stated in [2.6 Legal Authority to Collect Information](#).

6.3 SECURITY CONTROLS FOR EXTERNAL SHARING

How is the information shared outside the system and what security measures safeguard its transmission?

To mitigate the risk associated with sharing PII externally, AAMVA implemented the following controls:

- Formally defined the roles and obligations of each participating organization
- Assigned oversight and compliance monitoring functions
- Defined and implemented communication standards and specifications
- Encrypted any PII while in transit using technologies that conform to the standards set by the National Institute of Standards and Technology, including the Federal Information Processing Standards.

6.4 PRIVACY RISK AND MITIGATION FOR EXTERNAL SHARING

What is the privacy risk associated with external sharing of information and how are they mitigated?

External sharing of information increases the risks of unauthorized disclosure and misuse. These risks are mitigated by:

- Developing a privacy framework that clearly states all the intended uses of the information, and specifies each user's and organization's responsibility in ensuring that the privacy of the information is maintained

- Communicating to the users their security and privacy obligations through formal contract or agreement, specifically for, or with explicit reference to, the information system
- Instituting penalties for the users that do not conform with the privacy protection requirements
- Maintaining a governance structure to review, approve and provide oversight over the purpose and participants of the program
- Ensuring that all sharing of information complies with the Driver Privacy Protection Act
- Restricting access to the information to those with a need to know
- Providing a point of contact for any privacy issues or breach
- Developing a comprehensive incident response plan with specific steps for the handling of a PII breach; including the breach notification requirements

7 NOTICE

The following sub-sections are intended to define the notice to the individual on the scope of information collected, the right to consent to usage of their information, and the right to decline to provide information.

7.1 PROVIDING NOTICE

Was notice provided to the individual prior to collection of information?

The participating States have the responsibility to provide notice to the applicant regarding the accuracy of the information the applicant is providing and the State's intent to detect and deter fraud related to the application for a credential.

7.2 USER RIGHT TO DECLINE

Do individuals have the opportunity and/or right to decline to provide information?

Existing State laws and regulations require the information to be collected in order to obtain a credential. The applicant's refusal to provide the necessary information would result in the State's inability to issue a credential.

7.3 USER RIGHT TO CONSENT TO USE

Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise that right?

The DPPA, along with other State-based legislation, primarily determine the use of information collected by SDLA's. Use of this information within SPEXS conforms to these laws.

7.4 PRIVACY RISK AND MITIGATION

Considering the notice, consent, and opportunities to decline to provide information, what are the identified privacy risks and how are they mitigated?

There is no confusion that the information provided by an applicant seeking a credential, such as a driver's license or an ID card, will be used for the purpose of issuing such credentials. There is also no confusion that this information may be verified later for the purposes outlined in the Driver Privacy Protection Act.

8 ACCESS, REDRESS AND CORRECTION

The following sub-sections are intended to define an individual's ability to ensure the accuracy of the information collected about them.

8.1 INDIVIDUAL ACCESS

What are the procedures that allow individuals to gain access to their information?

The SDLAs are the formal record holders of the information maintained in the SPEXS pointer index. The information in the SPEXS pointer index is a limited subset of the information in the SDLA database. AAMVA asserts no ownership of the information and cannot provide individuals direct access to their records.

An individual may request access to his or her information by contacting the SDLA that issued the credential they applied for. The SDLA may issue an inquiry to the SPEXS pointer index for the purpose of verifying that the information in the pointer index matches that in its own database.

SDLAs are public agencies and their contact information is readily available.

8.2 CORRECTION OF INFORMATION

What are the procedures for correcting inaccurate or erroneous information?

If an individual believes the information in the SPEXS pointer index is inaccurate, the individual is required to contact the SDLA that issued the credential associated with the pointer. Upon adjudication of the mistake, if necessary, the SDLA will issue an *Update* transaction to the SPEXS pointer index to update/correct the information.

8.3 NOTIFICATION OF PROCEDURES TO CORRECT INFORMATION

How are individuals notified of the procedures for correcting their information?

Individuals contacting AAMVA directly with requests to correct their personal information in the SPEXS pointer index will be directed to the SDLA that issued the credential in question.

Specific SDLA procedures supporting data correction are out of scope for this document and vary from State to State.

8.4 ALTERNATIVES TO FORMAL REDRESS

If no formal redress is provided, what alternatives are available to the individual?

If an individual is unable to resolve a data correction problem with the respective SDLA, he or she is encouraged to file a complaint with AAMVA's Privacy Officer by emailing Privacy@aamva.org or calling 703 522 4200.

8.5 PRIVACY RISK AND MITIGATION

What are the privacy risks associated with the redress available to individuals and how are those risks mitigated?

The main privacy risk associated with the SPEXS pointer index redress process relates to the fact that individuals may attempt to contact AAMVA instead of the SDLA that issued their credentials. The risk is mitigated by having well defined procedures allowing the AAMVA personnel to handle such requests in a very efficient manner, and by maintaining the contact list of all SDLAs, including the official Website or 800 number.

9 TECHNICAL ACCESS AND SECURITY

The following sub-sections are intended to describe technical safeguards and security measures.

9.1 PROCEDURES FOR SYSTEM ACCESS

What procedures are in place to determine which users may access the system? Are these procedures documented?

Access to the SPEXS pointer index information is provided to:

- **Authorized Jurisdiction Personnel** through their own SDLA system or through reports received from the pointer index, in accordance to each Jurisdiction acceptable use policy and, for the SPEXS participants, the requirements defined in the *DIVS Program – Pilot State to State Verification Service – Pilot Participant User Agreement*.
- **AAMVA SPEXS Support Personnel** including infrastructure, software, and Help Desk support. Access to computing support equipment (e.g., servers, databases) for infrastructure and application support is provisioned via the AAMVA Access Request System and must be approved by a designated SPEXS support manager. Access to AAMVA Help Desk support is limited to the internal (i.e., not Internet accessible) support web user interface and also managed through the AAMVA Access Request System.
- **Managed Data Center Support Personnel**, including facilities and operational support of the network and computing equipment and the associated operating systems. AAMVA infrastructure oversees the service provider's operational support and approves any changes including firewall policies, patching cycles, the commissioning / decommissioning of equipment.

9.2 CONTRACTOR ACCESS

Will contractors have access to the system?

In the capacity of acting as staff augmentation, contractors providing support services will have access to SPEXS as described in [9.1 Procedures for System Access](#).

As part of the managed services agreement with the data center managed service provider, system-level access is in place and is required by data center support in the capacity of providing operational services such as backups, patching, and general maintenance.

9.3 PRIVACY TRAINING

What privacy training is provided to users either generally or specifically relevant to the program or system?

As part of the AAMVA Security and Privacy program, all AAMVA staff, including staff equivalent contractors, are required to complete security and privacy training during the personnel on-boarding process, and annually thereafter. The training covers security and privacy matters.

9.4 SECURITY ASSESSMENT AND SYSTEM AUTHORIZATION

Has a formal security assessment and system authorization been completed for the system or systems supporting the program?

A formal security and privacy assessment leveraging the FISMA risk management framework was conducted in July 2015, prior to the launch of the SPEXS pointer index. Among others, the risk management framework complies with the NIST Security Special Publications and FIPS documentation, including:

- *NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations*
- *NIST SP 800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*
- *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*

In alignment with *NIST SP 800-37*, the risk management framework includes an analysis of the system impact level (“categorization”) which provides for the level of security and privacy controls. The risk management framework also includes a formal system security package, which is comprised of a security and privacy plan, privacy impact assessment, contingency plan, and a risk assessment report. For security reasons, the security package documentation is confidential.

10 TECHNOLOGY

The following sub-sections are intended to critically analyze the selection process for any technologies utilized by the system, including system hardware, software, and other technology.

10.1 PROJECT TYPE

What type of project is the program or system?

This project is described in Section 2.3 Purpose of Information.

10.2 SYSTEM DEVELOPMENT STAGE

What stage of development is the system in and what project development lifecycle was used?

SPEXS is currently in the production pilot stage. All 51 U.S. jurisdictions use SPEXS for their CDLIS participation. A select few Jurisdictions have implemented, or are in the process of implementing, their access to the S2S capabilities.

10.3 TECHNOLOGY PRIVACY CONCERNS

Does the project employ technology which may raise privacy concerns and, if so, what are the implications for implementation?

The SPEXS pointer index does not employ technology that will raise additional privacy concerns. SPEXS provides some services via an Internet-accessible interface. Protective measures have been included in the security plan to define the appropriate levels of protections, commensurate with the additional level of risk, for authentication and authorization mechanisms, firewall protections, intrusion monitoring, proactive penetration testing, and the security of sensitive information as it is transmitted across the Internet.

GLOSSARY OF ACRONYMS

AAMVA	American Association of Motor Vehicle Administrators
CDL	commercial driver’s license
CDLIS	Commercial Driver’s License Information System
CMVSA	Commercial Motor Vehicle Safety Act
DLN	driver license number
DIVS	DL/ID Verification Systems (DIVS)
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMCSA	Federal Motor Carrier Safety Administration
MCSIA	Motor Carrier Safety Improvement Act
MPR	master pointer record
NIST	National Institute of Standards and Technology
PIA	privacy impact assessment
PII	personally identifiable information
SAFETEA-LU	Safe, Accountable, Flexible, Efficient Transportation Equity Act – a Legacy for Users
SOR	State of record
SPEXS	State Pointer Exchanger Services
SSN	social security number