Stage 2 Alternatives Analysis

California Department of Technology, SIMM 19B.2 (Ver. 3.0.8, 02/28/2022)

2.1 General Information

1. **Agency or State Entity Name:** 2740 - Motor Vehicles, Department of

   If Agency/State entity is not in the list, enter here with the organization code.

2. **Proposal Name:** State to State Verification (S2S)

3. **Department of Technology Project Number (0000-000):** 2740-229

4. **S2AA Version Number:** Version 2

5. **CDT Billing Case Number:** CS0068543

   Don't have a Case Number? Click here to get one.

2.2 Submittal Information

1. **Contact Information**

   Contact Name: Nakisha Howard

   Contact Email: Nakisha.Howard@DMV.ca.gov

   Contact Phone: 916-657-5691

2. **Submission Type:** Updated Submission (Post-Approval)

   If withdrawn, select Reason**:** Choose an item.

   If Other, specify reason here: Click or tap here to enter text.

   Sections Changed if an update or resubmission:

   All sections have changed, since Version 1 (approved on 05/14/2021) was completed using SIMM 19B template version 2.1, revision 5/21/2018.

   Summary of Changes:

   Section 2.3.1: Current Business Environment - Minor edits.
   Section 2.3.2: Added RESTful API interface and Minor edits.

Section 2.3.7: Technical Complexity score change from 2.8 to 2.7.
Section 2.4: Revised Mid-level Requirements.
Sections 2.5: Revised Assumptions/Constraints.
Section 2.6: Revised Dependencies - Added the need of legislative proposal or trailer bill language to allow sharing of SSN with AAMVA.
Sections 2.8: Viable Alternative Solutions: Alternative Solution 2 (AAMVA S2S System with SSN Presentation) is now the proposed solution. DMV is planning to utilize the existing AAMVA S2S electronic exchange and provide information for verification between other states on all CA DL/ID Card Applicants. Removed other solutions due to AAMVA requirements.
Section 2.9: Revised Project Organization Chart (Attachment) and new language added to sub-sections.
Section 2.10.1: Revised PM score from 1.2 to 0.3.
Section 2.10.2: Revised Project Charter.
Section 2.10.3: Revised All PM Plans.
Section 2.10.4: Revised Project Roadmap with updated dates.
Section 2.11: Data Migration - Will be completed on a later date when DMV has the confirmed Data Migration strategy.
Section 2.12: Revised Financial Analysis Worksheet (FAWs).

3. **Attach Project Approval Executive Transmittal to your email submission.** **See Attached**

4. **Attach Procurement Assessment Form to your email submission.** **See Attached**

5. **Conditions from Stage 1 Approval** (Enter any conditions from the Stage 1 Business Analysis approval letter issued by CDT or your AIO):

   Upon approval of Stage 2, no conditions identified by CDT or AIO.

2.3 Baseline Processes and Systems

1. **Current Business Environment (Describe the current business environment of which the effort will be understood and assessed in 500 words)**

   The current business and technical infrastructure supports DMV's commercial driver and problem driver functionalities, including the Commercial Driver's License Information System (CDLIS) and the Problem Driver Pointer System (PDPS). The Commercial Motor Vehicle Safety Act (CMVSA) of 1986 is based on the Federal Motor Carrier Safety Regulations (FMCSRs) in 49 CFR §§ 383 and 384 was passed in a national effort to remove unsafe and unqualified drivers from the nation's highways. Some significant features of the CMVSA, focused on improving traffic safety, include:

   • All jurisdictions are required to participate in CDLIS and PDPS.
   • The single license requirement, which became effective on July 1, 1987, mandates that commercial drivers hold only one driver license (DL).

   CDLIS is a nationwide computer system with a repository that enables State Driver Licensing Agencies (SDLAs) to ensure that commercial drivers have only one DL and one complete driver record. Data and driver records are accessible to individual states via the American Association of Motor Vehicle Administrators (AAMVA) CDLIS portal for matching or verifying purposes. In

addition to name, date of birth, and social security number (SSN), other data related to the driver and driver record is provided.

California Vehicle Code (CVC) §15200 et seq. requires California to comply with federal regulations for commercial drivers. CVC §15210(a) defines a commercial driver license (CDL) as one issued in accordance with 49 CFR § 383. These federal provisions require the issuing state to verify the name, date of birth, and SSN provided by the applicant with information on file with the Social Security Administration (SSA) prior to issuing a CDL. The state is prohibited from issuing, renewing, upgrading, or transferring a CDL if the SSA database does not match the applicant-provided data. Pursuant to 49 CFR § 383.73(n), the state must establish computer system controls that will prevent the issuance of CDLs to unqualified applicants. Additionally, 49 CFR § 383.73(b)(3)(ii) requires the state to check with CDLIS prior to issuing a CDL.

Attach relevant documentation to email submission (i.e., business process, workflow, problem analysis, user/stakeholder list, research findings). If these types of documents are not available, please indicate "Not Available," and explain the reason below: **See Attachment**

2. **Technical Context (Describe the technical environment of which the effort will be understood and assessed in 500 words)**

S2S is owned by and governed through AAMVA. The AAMVA S2S Governance Committee is in charge of the development of the system requirements, the definition of enforcement of compliance, as well as oversight of the operational and financial aspects of S2S.

At this time, California does not have existing business processes for the S2S program; however, it most closely resembles the CDLIS program. S2S leverages the existing pointer system that allows SDLAs to "talk" to each other through a third-party proprietary technology platform, known as CDLIS. S2S extends this platform beyond commercial drivers to all non-commercial DL cards and all REAL ID compliant cards to empower states to check with each other upon issuance.

AAMVA is the operator of the State Pointer Exchange Services (SPEXS) Central Site, which encompasses both CDLIS and S2S credentials, supports the telecommunications network used by SPEXS, and provides help desk support. AAMVA supports both Unified Network Interface/AAMVA Message Interchange Envelope (UNI/AMIE) and Web Services platform, which provides DMV with an opportunity to implement S2S utilizing the existing CDLIS platform (AMIE) or a new platform, such as Web Services using the National Information Exchange Model (NIEM) or Representational State Transfer (REST) Application Programming Interface (API).

SPEXS contains three types of data records, including data stored at the SPEXS Central Site, Driver History Record data kept by the State of Record (SOR), and ancillary data records. The data stored at the SPEXS Central Site contains only the information needed to properly identify a driver, which includes the following data elements:

- SOR and DL/ID number
- Driver name
- Driver date of birth
- Driver SSN

- The date and time the driver was added to SPEXS
- The date and time the record was last updated
- Indicator of a change state of record in progress
- Type of document issued (DL, permit for base DL, or ID)
- CDLIS Pointer indictor
- REAL ID compliant indicator
- Indicator if the SSN is one assigned by SSA, a substitute SSN, or a pseudo SSN.

Attach relevant documentation to email submission (i.e., logical system environment diagrams, system interactions, business rules, application flows, stakeholder information, data flow charts). If these types of documents are not available, please indicate "Not Available," and explain the reason below: **See Attachment**

Not available reason: Click or tap here to enter text.

3. **Data Management (Enter the information to indicate the data owner and custodian of the current system, if applicable.)**

   Data Owner Name: Deanna Wida

   Data Owner Title: Assistant Division Chief/Program Manager

   Data Owner Business Program area: Licensing Technology Section

   Data Custodian Name: Eric Harrald

   Data Custodian Title: Information Security Officer

   Data Custodian Technical area: Information Systems Division

   Security - Data Classification and Categorization Yes

   Security - Privacy Threshold & Impact Assessment. Yes

4. **Existing Data Governance and Data**

   a) Do you have existing data that must be migrated to your new solution?

   Answer (Unknown, Yes, No): Yes

   If data migration is required, please rate the quality of the data.

   Select data quality rating: Few issues identified with the existing data.

   b) Does the Agency/state entity have an established data governance body with well-defined roles and responsibilities to support data governance activities?

   Answer (Unknown, Yes, No): No

   If Yes, include the data governance organization chart as an attachment to your email submission.

   c) Does the Agency/state entity have data governance policies (data policies, data standards, etc.) formally defined, documented, and implemented?

Answer (Unknown, Yes, No): No

If Yes, include the data governance policies as an attachment to your email submission.

d) Does the Agency/state entity have data security policies, standards, controls, and procedures formally defined, documented, and implemented?

Answer (Unknown, Yes, No): Yes

If Yes, attach the existing documented security policies, standards, and controls used to your email submission.

e) Does the Agency/state entity have user accessibility policies, standards, controls, and procedures formally defined, documented, and implemented?

Answer (Unknown, Yes, No): Yes

If Yes, attach the existing documented policies, accessibility governance plan, and standards used to the email submission.

5. **Security Categorization Impact Table**

Consult the SIMM 5305-A Information Security Program Management Standard - Security Categorization Impact Table.

Attach a table (in PDF) that categorizes and classifies the agency/state entity's information assets related to this effort (e.g., paper, and electronic records, automated files, databases requiring appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion). Each information asset for which the agency/state entity has ownership responsibility shall be inventoried and identified. **See Attachment.**

6. **Security Categorization Impact Table Summary**

Consult the SIMM 5305-A Information Security Program Management Standard - Security Categorization Impact Table to provide potential impact levels of the following areas:

Confidentiality: Medium

Integrity: Medium

Availability: Medium

7. **Technical Complexity Score:** 2.7

(Attach a SIMM Section 45 Appendix C with Business and Technical Complexity sections completed to the email submission.) **See Attachment.**

2.4 Requirements and Outcomes

At this time in the project planning process, requirements and outcomes should be documented and indicative of how the Agency/State Entity envisions the final solution. This shall be accomplished

either in the form of mid-level requirements (predictive methodology)/business capabilities or representative epics and user stories (adaptive methodology) that will become part of the product backlog. The requirements or representative epics and user stories must tie back to the Objectives detailed in the Stage 1 Business Analysis. Regardless of which tool/method is used, an understanding of the following, at a minimum, must be clearly articulated:

- Functional requirements
- Expected user experience(s)
- Expected system outcome
- Expected business operations (e.g., How do you envision operations in the future?)
- Alignment to the project's objectives identified in Stage 1
- Product ownership (e.g., Who owns these requirements?); and
- Verification of need(s) fulfillment (e.g., How will success be measured?)

Attach Requirements and/or Outcomes narratives, mid-level requirements, and/or epics/user stories to submission email. **See Attachment.**

2.5 Assumptions and Constraints

Relevant assumptions and constraints help define boundaries and opportunities to shape the scope and complexity of the project.

Assumption: Funding will be available no later than July 1, 2025.

> **Description/Potential Impact**: BCP is pending approval for funding to start in the FY 25/26 and to continue through implementation. If funding is denied, effort will not move forward, and DMV will not meet mandated implementation date

Assumption: Functional and non-functional requirements will not change substantially during project development.

> **Description/Potential Impact**: If substantial changes are made to the requirements, potential vendors may not be able to meet project objective within the time constraints.

Assumption: Assume state SMEs will be available for the project duration.

> **Description/Potential Impact**: If resources are no longer available or engaged, the project could fall behind schedule causing the project to miss the targeted implementation date.

Assumption: Issues and risks will be resolved, and risk mitigated in a timely manner.

> **Description/Potential Impact**: If the potential issues and risks are not addressed in a timely manner, it could affect the completion and performance of the project as required.

Assumption: In order to meet deadlines for contract award to vendor, the approval process will be done quickly to allow contract award in the last quarter of the Fiscal Year (FY) 2024/25.

> **Description/Potential Impact**: If the contract award is delayed, the effort will not make the mandated implementation date.

Assumption: DHS will approve S2S operational date no later than January 2025.

Description/Potential Impact: Project schedule has an operational date pending approval for 02/16/2027.

Constraint: The solution must be fully implemented by February 16, 2027.

Description/Potential Impact: If the selected vendor does not have the available resources, it could cause project delays and jeopardize DMV to miss the mandated implementation date.

2.6 Dependencies

Dependencies are elements or relationships in a project reliant on something else occurring before the function, service, interface, task, or action can begin or continue.

Dependency Element: Legislative Proposal / Trailer Bill Language

Dependency Description: California statute currently does not authorize the sharing of SSN information via S2S. Trailer Bill language must be approved before DMV can share SSN information via S2S.

2.7 Market Research

Market Research (CDT Market Research Guidelines) determines whether products or services available in the marketplace can meet the business needs identified in this proposal. Market Research can also determine whether commercial practices regarding customizing/modifying products or tailoring services are available, or even necessary, to meet the business needs and objectives of the business.

Before undertaking a Market Research approach. Contact your PAO Manager to schedule a collaborative review to review planning to date and discuss the procurement approach.

Preface: Market Research was completed in 2019-2020 when S2S initially started.

1. **Project Management Methodology: Predictive Approach (Waterfall)**
2. **Procurement approach recommended:** Challenge-based Procurement
3. **Market Research Approach**

   Provide a concise narrative description of the approach used to perform market research.

   The REAL ID Act of 2005 includes new requirements for SDLAs to abide by in order to remain compliant with the REAL ID Act. According to REAL ID federal regulations (6 CFR § 37.29), states must check with all other states to determine if an applicant currently holds a DL or REAL ID card in another state. To comply with this requirement, many states are opting to enroll in S2S: an electronic tool that allows states to determine whether an applicant already holds a DL or REAL ID card in another state.

   The S2S Verification System is a means for states to electronically check with all other

participating states to determine if an applicant currently holds a DL or REAL ID card in another state. The AAMVA S2S Governance Committee is in charge of the development of the system requirements, the definition and enforcement of compliance, as well as the oversight of the operational and financial aspects of the service.

Thus far, CADMV has determined that the following policy consideration must be addressed before signing any agreement with AAMVA to participate in S2S. DMV's concerns in providing the last five digits of SSN are related to creating a potential exposure of AB 60 DL holders, potential privacy/security breaches of SSN data, and existing sensitivity to DMV sharing information with other entities not specifically identified by statute.

While the SSN remains the single most reliable identity verification source, DMV has explored the following alternatives to the SSN data element:

Option 1: Do not provide the actual SSN data for any California DL or ID card holders – only provide the last five digits of the SSN when a request is made by a jurisdiction to verify a match.

Option 2: Provide a pseudo number (randomly generated) to complete this data field for all card holders - there is a finite number of pseudo numbers available per state (999,999). Additional discussions would need to occur with AAMVA to determine feasibility to increase the pseudo numbers for California.

Option 3: Substitute SSN with all 9s – this format is used when a non CDL driver has been convicted of a commercial motor vehicle violation and no SSN was provided or available for that driver. This is not advisable as it would not provide an accurate depiction of the record.

Option 4: Provide the actual last five digits of the SSN for applicants who have an SSN, and a pseudo number (randomly generated) for those who do not have an SSN.

Option 5: Consider providing the DL/ID card record for only REAL ID compliant records.

Option 6: Develop a California-exclusive system to fulfill the federal requirement to provide an electronic tool that allows states to verify issuance per REAL ID requirements and compliant with California's privacy and security requirements. This would require a significant investment by DMV at a time that it is also focused on the modernization of its technology systems versus subscribing to AAMVA's S2S system.

<u>Market Research Methods and Activities</u>
Vendor Demonstrations – SSN Alternatives
On September 9, 2020, DMV facilitated a Vendor Day event and presented the following problem statement to identify potential solutions for engaging in S2S: CADMV would like to explore the use of a unique identifier versus the use of the last 5-digits or full social security number as currently required. We are seeking solutions to develop an alternative data point that meets the spirit of the REAL ID Act while limiting the reliance on an SSN. The solution will need to include the ability to interface with states that will continue to use S2S and rely on SSN as a data source for verification.

1. Proposed Solution

An identity resolution leveraging proprietary linking technology to match DL records with other states nationwide was proposed to DMV following Vendor Day. In lieu of an SSN, an exclusive numerical identifier would be used to connect records nationwide.

2. AAMVA Research – Design and SSN Alternatives

Via a grant from DHS, the Commonwealth of Kentucky provided funding to the REAL ID Verification Systems Working Group (RIVSWG) to undertake an analysis of design alternatives for S2S. In conducting the analysis, the RIVSWG reached out to the many stakeholders associated with REAL ID to obtain their input and advice on the alternatives to be analyzed, the analysis methodology, and the evaluation criteria. The RIVSWG evaluated alternative designs and published their results in the REAL ID State-to-State Verification Design Alternatives Analysis white paper, issued in January 2009. In this study, the use of the SSN was discussed in the context of privacy and was reduced from 9 to 5 digits. In a system that relies only on demographics to identify individuals, it was considered as too critical of a data element to remove it entirely from the key identifiers.

3. Other States Research

The Business and IT efforts for S2S are significant and come during a time when California is grappling with other large-scale initiatives: REAL ID, IT Modernization, and digital transformation in response to COVID-19. The following examples provide levels of effort among other states:

- Arizona (4.8 million drivers) estimated approximately 17,000 staff hours to implement S2S.
- Maryland (4.2 million drivers) estimated over 30,000 staff hours and a 50% increase in ongoing operational staffing hours.
- By comparison, California has approximately 30 million DL/ID card records.

Additionally, California contacted Alaska, Colorado, Illinois, Louisiana, Maryland, New Hampshire, Oregon, Texas, and Utah in an effort to gain additional insight on their S2S implementation efforts. Of these states, Colorado, Illinois, Maryland, and Utah offer DLs to undocumented applicants, similarly to California. In addition to the other minimum information required to identify a credential, these states either currently or plan to submit their undocumented applicants to the SPEXS Central Site utilizing the following SSN numeric values:

- Colorado submits substitute SSNs (‘999-99-9999’).
- Illinois recently passed legislation to allow for sharing SSNs via S2S [625 ILCS 5/2-123(h)] and will submit substitute SSNs (‘999-99-9999’) upon their implementation date in November 2021.
- Maryland submits substitute SSNs (‘999-99-9999’).
- Utah requires applicants to either have an SSN or ITIN, among other documentation, in order to apply for a credential. Therefore, Utah submits pointers for undocumented applicants in the same manner as all other applicants.

Summary of Findings from Market Research

To satisfy the REAL ID regulations, California intends to utilize the S2S platform. However, California’s concerns in entering into the S2S agreement through AAMVA to provide the minimum data elements, including the last five digits of the SSN, are related to creating a potential exposure for AB 60 DL holders, potential privacy/security breaches of SSN data, and existing sensitivity to

DMV sharing information with other entities not specifically identified by statute. Therefore, allowing an encryption of the SSN is the preferred method for sharing this particular data element within the S2S platform. However, this approach would require AAMVA to modify their agreement and their current system requirements for SSN sharing.

California proposed alternative S2S system mechanics for consideration by AAMVA and its S2S Governance Committee. Although this approach was not accepted, CADMV continues to prepare for and undertake the steps necessary to join the S2S system in February 2027.

4. **Market Research Artifacts**

Market Research Artifacts can include internet research, collaboration with other governmental entities, or other documentation.

Attach Market Research artifacts to the email submission.

2.8 Viable Alternative Solutions

The CDT expects Agencies/state entities to conduct a thorough analysis of all feasible alternatives that will meet the proposal's objectives and requirements. Agencies/state entities should provide at minimum the three (3) most viable solutions, one (1) of which could be leveraging and/or enhancing the existing solution (if applicable).

1. **Viable Alternative Solution #1**

Name: AAMVA S2S System with SSN Presentation

Description: Utilizing the existing AAMVA S2S electronic exchange, CA DMV will provide information for verification between other states on all California Driver License Applicants and on all Driver License/Identification Card Applicants. This system will be utilized no later than February 16, 2027, in order to stay in compliance with the Federal REAL ID Act.

In order to keep the current system in line with AAMVA to ensure S2S Go-Live in 2027, several incremental, preparatory activities must occur within 1 year preceding the S2S System Go-Live that include system upgrades for security, and compliance to federal mandates for commercial drivers (FMCSA). In addition, activities related to data cleaning will occur to ensure the best possible outcome when matching up drivers on the S2S database.

In order to remain in compliance with the provisions of the REAL ID Act and the associated compliance letter, DMV will report on driver and identification cardholder information and the DMV would be required to provide SSNs to AAMVA.

Once implemented the S2S inquiry service will interface with AAMVA to provide real-time batch service during the processing of DL/ID applications. The service will send and process a request to other state licensing agencies to cancel a DL/ID card upon issuance in California as well as cancel California DL/ID cards upon issuance in requesting states. In addition, the S2S service will send and process DL/ID history requests to other state driver licensing agencies.

DMV will procure a vendor to create a system that will provide data and messaging with the AAMVA S2S system. Through a Challenged Based Procurement (CBP), a vendor will be awarded a contract to provide an information technology solution for a modern, cloud platform to assist in data extraction, migration, storage, updating, and messaging to the S2S system. The new system, owned and maintained by DMV after initial implementation, will:

1. Extract data from the Master Record to populate the new data base, synch with the Master on a continuous basis, and perform the initial pointer data with AAMVA.
2. Create a new real-time/batch service invoked during processing of DL/ID applications.
3. Integrate with DL/ID processing systems.
4. Send and process requests to other state driver licensing agencies to cancel a DL/ID card, upon issuance in California.
5. Receive and process requests from other state(s) to cancel a CA DL/ID card, upon issuance in requesting state(s).

Why is this a viable solution? Please explain:

- Allows California to meet the REAL ID requirements and remain compliant.
- Leverages the only existing system to fulfill the needs of the State.

Approach

Increase staff – new or existing capabilities: **Yes**

Modify the existing business process or create a new business process: **Yes**

Reduce the services or level of services provided: **No**

Utilize new or increased contracted services: **Yes**

Enhance the existing IT system: **No**

Modify Statute/Policy/Regulations: **Yes**

Please Specify: Trailer Bill language must be approved prior to sharing SSN.

Create a new IT system: Yes

Other: Choose Yes or No. **Specify:** Click or tap here to enter text.

Architecture Information

Business Function(s)/Process(es): S2S will have new process flows and will be developed.

Conceptual Architecture

See Attachment.

COTS/SaaS/Cloud Technology or Custom: COTS/SaaS/Cloud Technology

Name/Primary Technology: AWS Cloud

Explain Existing System Interfaces: Legacy

Explain New System Interfaces: RESTful

Data Center Location of the To-be Solution: Other

If Other, specify: To be determined

Security

Access

Public: No

Internal State Staff: Yes

External State Staff: No

Other: Yes **Specify:** Outside agency (Law enforcement)

Type of Information (Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.)

Personal: Yes

Health: Yes

Tax: No

Financial: No

Legal: No

Confidential: Yes

Other: **Choose Yes or No.** Specify: **Click or tap here to enter text.**

Protective Measures (Select Yes or No to identify the protective measures used to protect information.)

Technical Security: Yes

Physical Security: Yes

Backup and Recovery: Yes

Identity Authorization and Authentication: Yes

Other, specify: Click or tap here to enter text.

Total Viable Alternative #1 Solution Cost (copy from FAW – Executive Cost Summary tab, cells E7 through E11):

Planning Costs: $8,775,204

One-Time (Project) Costs: $41,669,465

Total Future Ops. IT Staff OE&E Costs: $5,038,933

Total Proposed Cost: $55,483,601

Annual Future Ops. Costs (M&O): $4,204,200

2. **Viable Alternative Solution #2**

Name: Not Applicable. Due to AAMVA requirements, Alternative Solution 1 is the only viable solution.

Description:

Why is this a viable solution?

Approach

Increase staff – new or existing capabilities: **Choose Yes or No.**

Modify the existing business process or create a new business process: **Choose Yes or No.**

Reduce the services or level of services provided: **Choose Yes or No.**

Utilize new or increased contracted services: **Choose Yes or No.**

Enhance the existing IT system: **Choose Yes or No.**

Modify Statute/Policy/Regulations: **Choose Yes or No.**

Please Specify: **Click or tap here to enter text.**

Create a new IT system: **Choose Yes or No.**

Other: **Choose Yes or No.** Specify: **Click or tap here to enter text.**

Architecture Information

Business Function(s)/Process(es): Click or tap here to enter text.

Conceptual Architecture

Attach a copy of the conceptual architecture to your email submission.

COTS/SaaS/Cloud Technology or Custom: **Choose an item.**

Name/Primary Technology: **Click or tap here to enter text.**

Explain Existing System Interfaces: **Click or tap here to enter text.**

Explain New System Interfaces: **Click or tap here to enter text.**

Data Center Location of the To-be Solution: **Choose an item.**

If Other, specify: **Click or tap here to enter text.**

Security

Access:

Public: **Choose Yes or No.**

Internal State Staff: **Choose Yes or No.**

External State Staff: **Choose Yes or No.**

Other: **Choose Yes or No.** Specify: **Click or tap here to enter text.**

Type of Information (Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.)

Personal: **Choose Yes or No.**

Health: **Choose Yes or No.**

Tax: **Choose Yes or No.**

Financial: **Choose Yes or No.**

Legal: **Choose Yes or No.**

Confidential: **Choose Yes or No.**

Other: **Choose Yes or No.** Specify: **Click or tap here to enter text.**

Protective Measures (Select Yes or No to identify the protective measures used to protect information.)

Technical Security: **Choose Yes or No.**

Physical Security: **Choose Yes or No.**

Backup and Recovery: **Choose Yes or No.**

Identity Authorization and Authentication: **Choose Yes or No.**

Other, specify: **Click or tap here to enter text.**

Total Viable Alternative #2 Solution Cost (copy from FAW – Summary tab, cell AL33):

Total Proposed Cost: **Click or tap here to enter text.**

3. **Viable Alternative Solution #3**

Name: Not Applicable. Due to AAMVA requirements, Alternative Solution 1 is the only viable solution.

Description: Click or tap here to enter text.

Why is this a viable solution? Please explain:

Click or tap here to enter text.

Approach

Increase staff – new or existing capabilities: **Choose Yes or No.**

Modify the existing business process or create a new business process: **Choose Yes or No.**

Reduce the services or level of services provided: **Choose Yes or No.**

Utilize new or increased contracted services: **Choose Yes or No.**

Enhance the existing IT system: **Choose Yes or No.**

Modify Statute/Policy/Regulations: **Choose Yes or No.**

Please Specify: **Click or tap here to enter text.**

Create a new IT system: **Choose Yes or No.**

Other: **Choose Yes or No.** Specify: **Click or tap here to enter text.**

Architecture Information

Business Function(s)/Process(es): Click or tap here to enter text.

Conceptual Architecture

Attach a copy of the conceptual architecture to your email submission.

COTS/SaaS/Cloud Technology or Custom: **Choose an item.**

Name/Primary Technology: **Click or tap here to enter text.**

Explain Existing System Interfaces: **Click or tap here to enter text.**

Explain New System Interfaces: **Click or tap here to enter text.**

Data Center Location of the To-be Solution: **Choose an item.**

If Other, specify: **Click or tap here to enter text.**

Security

Access:

Public: **Choose Yes or No.**

Internal State Staff: **Choose Yes or No.**

External State Staff: **Choose Yes or No.**

Other: **Choose Yes or No.** Specify: **Click or tap here to enter text.**

Type of Information (Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.)

Personal: **Choose Yes or No.**

Health: **Choose Yes or No.**

Tax: **Choose Yes or No.**

Financial: **Choose Yes or No.**

Legal: **Choose Yes or No.**

Confidential: **Choose Yes or No.**

Other: **Choose Yes or No.** Specify: **Click or tap here to enter text.**

Protective Measures (Select Yes or No to identify the protective measures used to protect information.)

Technical Security: **Choose Yes or No.**

Physical Security: **Choose Yes or No.**

Backup and Recovery: **Choose Yes or No.**

Identity Authorization and Authentication: **Choose Yes or No.**

Other, specify: **Click or tap here to enter text.**

Total Viable Alternative #3 Solution Cost (copy from FAW – Summary tab, cell AL50):

Total Proposed Cost: **Click or tap here to enter text.**

2.9 Project Organization

Project planning includes the process of identifying how and when specific labor skill sets are needed to ensure that the proposed project has sufficient staff with the appropriate knowledge and experience by the time the project moves into execution. All staff identified in the following sections should be included in the Financial Analysis Worksheet to be completed in Section 2.12.

1. **Project Organization Chart:**

   Attach the Project Organization Chart to your email submission. **See Attachment.**

2. **Is the department running this project as a matrixed or projectized organization?**

   Matrixed

In each of the following sections, provide a concise description of the approach to staffing the proposed project including contingencies for business/program, IT, or administrative areas to maintain ongoing operations in conjunction with the proposed project.

1. **Administrative**

   The DMV Administrative sections have the capacity and capability of providing the project support necessary for this project. The DMV's Budget and Fiscal Analysis Branch (BFAB) is part of the existing duties of the Budget Office Staff. An analyst from BFAB with the support of the Budget Office management team, will provide budget-related assistance and guidance to the proposed Information Technology project team. Responsibilities include consulting with the

programs areas in determining the costs associated with staffing and operational needs for the project and acting as a liaison between the DOF and other control agencies in preparing and submitting the Budget Change Proposal (BCP). The Budget Office staff has extensive experience in budgeting.

The DMV Contract Manager administers all contracts for the project to ensure compliance with appropriate regulations and policies, will research contract issues and monitor the contractor's performance against the requirements of the contract. The Contract Manager works with the Project Manager to ensure the expectations and due dates for each deliverable set forth in the contract or Statement of Work (SOW) is clear and complete. The Contract Manager also monitors the contract in accordance with Disabled Veterans Business Enterprise (DVBE) contract requirements (if applicable). The Contract Manager tracks all contract deliverables and milestones and validates deliverable acceptance prior to authorization of payment. The Contract Manager will have full responsibility and oversight of the contract and knowledge of: Contract administration, maintaining a working copy of the contract file, the elements of the contract, when to notify the contractor to begin work, monitoring the contractor to assure the compliance with contract provisions are met, approving the final product/service, monitoring expenditures and approving/disputing invoices for payment/nonpayment, and requesting modifications, renewals, or a new contract as required.

The Assessment Team Members responsibilities are: understanding the requirements of the Solicitation prior to the beginning of the offer evaluations, timely review of the offer, attending all Assessment Team meetings, working to gain consensus with other Assessment Team members, completing review worksheets and the Assessment Selection Report in accordance with the Assessment Plan, notifying the CDT Office of Statewide Procurement (OSTP) and DMV IT Acquisitions Official if any questions or concerns during the review process, Assessment the Final offers, and determining the materiality of deviations from the procurement requirements with input from the CDT Legal staff.

The DMV IT Acquisitions Unit assists with procuring a contract through solicitations, contacting prospective contractors, developing, or reviewing the solicitation packages (including the SOW), coordinating the encumbrance of funds for the contract, and distributing copies of the signed executed contract to the appropriate parties.

The DMV IT Acquisitions Official coordinates final approval of the contracts with the DMV IT Acquisitions Manager and advises the project of new or modified state procurement policies and regulations. Throughout the project life cycle, the DMV IT Acquisitions Official continues to serve the project with contract amendments and staff replacement and must work with the CDT OSTP Office as required. The DMV IT Acquisitions Official is a subject matter expert on the State of California's Solicitation process and acts as an advisor to members of the Assessment Team. Specific duties related to the assessment and selection process include Coordinating with CDT STP on a regular basis, assisting the CDT STP with training the assessor on the review process and the use of the assessment materials such as worksheets and evaluation sheets, and assisting the CDT STP in preparation of the Assessment and Selection Report. This position is the primary point of contact for CDT OSTP, Project Team, and the Assessment Team in regard to the solicitation.

The CDT Procurement Officer is the person designated by the State to have full responsibility for coordination and oversight of the acquisition process and gaining approval of the Solicitation Assessment and Selection Report. Specific duties related to the procurement process include Maintaining the Master Copy of all Bids and the official procurement files, acting as the single point of contact for correspondence sent to and received from Bidders, managing the proposal materials to include safeguarding proprietary information, assist with preparing the Assessment and Selection Report, and contacting prospective contractor(s).

2. **Business Program**

Business Program Policy staff are the primary policy users and are directly involved throughout the project as chief stakeholders, assisting with the development of the PAL artifacts, and implementing its processes through the vendor solution. Business Program staff will engage with vendor, identify the business outcomes, and achieving those goals with the vendor through the solution's implementation, pilot, testing, validation, developing procedures, system administration, and communication with staff, stakeholders, and the DMV as determined necessary. DMV Business Program areas will continue to oversee the system and the Business Program area will need to request additional resources to implement the proposed solution. The Business resources will collaborate with IT staff during the development and throughout the project to ensure proper user acceptance testing (UAT) is performed and the solution meets the customer and stakeholder's requirements.

3. **Information Technology**

DMV's Information Systems Division has conducted a thorough analysis of the current resource capacity and determined DMV does not have the capacity to absorb the additional workload without assistance. The DMV will be requesting permanent IT positions to ensure continued support throughout the project's implementation lifecycle and ongoing operations. The IT resources will collaborate with program staff and training staff during the development and throughout the project to ensure proper user acceptance testing (UAT) is performed, training essentials are met, and the solution meets the customer and stakeholder's requirements.

4. **Testing**

DMV's Product Quality Assurance (PQA) Section will assign a test manager and contract services to provide guidance for the overall testing. All other impacted business teams will conduct UAT to ensure their existing systems are functioning as designed. Responsibilities for the Test Manager include review and approval of a strategy and scope of testing, review, and approval of the test approach, defining a defect management plan, providing the defect severity classification, providing the pass/fail criteria for test cases, identifying, and raising any risks related to testing throughout the effort and monitoring all test phases. (e.g. – Unit, Integration, System, etc.) and types of testing (e.g. – Black Box, White Box, Regression, Stress, etc.)

5. Data Conversion/Migration

POL and ISD will work together to manage the impact of migration on daily activities. The team will help ensure that critical business functions remain unaffected during data migration. POL staff will be identified to manage and oversee business continuity and any interim processes needed during the data conversion/migration activities. This team will work closely with IT and the contractor to address any operational challenges that arise.

This approach ensures that while the contractor handles the technical aspects of the data migration, there is a strong support structure within the business and IT teams to maintain ongoing operations and prevent any disruption during the process.

6. Training

The Learning and Development Branch (LDB) is responsible for the development and delivery of all program-related training, as well as leadership, management and general training conducted throughout the state and manages the Learning Management System to support learning for the Department. Furthermore, LDB manages various training environments (EASE and DMVA) that will be impacted due to any changes or modifications to the current process. LDB would be responsible to support the updates for the records in those systems that are used in real time training as well as updating resources in the DMV U courses. Additionally, LDB manages the Department training budget and tracks mandatory training. LDB has conducted a thorough analysis of the current resource capacity and determined DMV does not have the capacity to absorb the additional workload without assistance. DMV will be requesting three (3) positions to assist during the project phase and ongoing support. Funding requested for three (3) Staff Services Managers (specialist) to supply essential services related to departmental training, curriculum development and design, the success of OCM services, and system management support during the project phase, through implementation, and post implementation. LDB resources will collaborate with program staff and any vendors during the training course development, throughout the project and ongoing to ensure proper development of training for operational needs. LDB will work directly with vendors and program staff to ensure continuity with information flow as well as content development. LDB will ensure all training content will adhere to state accessibility requirements and training standards through quality assurance checks and vetting the systems that are used to develop content.

7. Organizational Change Management

DMV plans to leverage consultant services for OCM. OCM will work in conjunction with the Project stakeholders to ensure that the stakeholders are educated about the changes, are given opportunity to buy-in to the vision and are able to adopt the change.

The OCM team will work with LDB, Policy, and Office of Public Affairs (OPA) to disseminate project information regarding the changes introduced by S2S.

8. Resource Capacity/Skills/Knowledge for Stage 3 Solution Development

The DMV Enterprise Governance Council makes informed decisions regarding DMV's technology direction and technology investment strategies. The governance framework includes procurement and project management related decision-making descriptions and

actions. The DMV's procurement officials have experience using the proposed procurement methodologies identified in this document, Section 2.7 and using the Department of Technology Stage 3 Solution Analysis (S3SA) process. The DMV's IT Acquisition unit is familiar with protest types, use of Public Contract Code (PCC) 6611, and has participated with Statewide Technology Procurement Division in the negotiations of various contracts.

2.10 Project Planning

1. **Project Management Risk Assessment**

   Updated Project Management Risk Score: 0.3

   Attach Updated PM Risk Assessment to your email submission. SIMM Section 45A
   See Attachment.

2. **Project Charter**

   Is your project charter approved by the designated Agency/state entity authority and available for the Department of Technology to review? **Choose**: 'Yes,' 'No,' or 'Not Applicable.' If 'No' or 'Not Applicable,' provide the artifact status in the space provided.

   Project Charter (Approved): **Yes**

   Status: **See Attachment.**

   Attach a copy of the Project Charter to your email submission. **See Attachment.**

3. **Project Plans**

   Are the following project management plans or project artifacts approved by the designated Agency/state entity authority and available for the Department of Technology to review? **Choose**: 'Yes,' 'No,' or 'Not Applicable.' If 'No' or 'Not Applicable,' provide the artifact status in the space provided.

   Note: For Low to medium complexity and cost projects, discuss with your PAO manager the option of submitting a Master Project Management Plan in place of individual plans.

   Scope Management Plan (Approved): **Yes**

   Status **See Attachment.**

   Communication Management Plan (Approved): **Yes**

   Status **See Attachment.**

   Schedule Management Plan (Approved): **Yes**

   Status **See Attachment.**

   Procurement Management Plan (Approved): **Yes**

   Status **See Attachment.**

Requirements Management Plan (Approved): **Yes**

Status **See Attachment.**

Stakeholder Management Plan (Draft): **Yes**

Status **See Attachment.**

Governance Plan (Draft): **Yes**

Status **See Attachment.**

Contract Management Plan (Draft): **Yes**

Status: **Completed**

Resource Management Plan (Draft): **Yes**

Status **See Attachment.**

Change Control Management Plan (Draft): **Yes**

Status: **Completed**

Risk Management Plan (Draft + Risk Log): **Yes**

Status **See Attachment.**

Issue and Action Item Management Plan (Draft + Issue Log): **Yes**

Status **See Attachment.**

Cost Management Plan (Approved if planning BCP approved): **Yes**

Status **See Attachment.**

4. **Project Roadmap (High-Level)**

   Attach a high-level Project Roadmap showing remainder of planning phase and transition into execution phase to the email submission. **See Attachment.**

   a) Planning Start Date: **11/4/2024**

   b) Estimated Planning End Date: **8/21/2025**

   c) Estimated Project Start Date: **8/21/2025**

   d) Estimated Project End Date: **2/16/2027**

2.11 Data Cleansing, Conversion, and Migration

If in Section 2.3 (above) the answer to the question "Do you have existing data that must be migrated to your new solution?" was marked "Yes," please complete this section.

The California Dep artment of Technology recommends having a Data Consultant start data cleansing, conversion, and migration activities as soon as possible.

Identify the status of each of the following data activities. If “Not Applicable” is chosen, explain why the activity is not applicable or if “Not Started” is chosen, explain when the activity will start and its anticipated duration:

This section will be completed in a later date when DMV has the confirmed data migration strategy.

1. **Current Environment Analysis:** In Progress

   Click or tap here to enter text.

2. **Data Migration Plan:** Not Started

   Click or tap here to enter text.

3. **Data Profiling:** In Progress

   Click or tap here to enter text.

4. **Data Cleansing and Correction:** Not Started

   Click or tap here to enter text.

5. **Data Quality Assessment:** In Progress

   Click or tap here to enter text.

6. **Data Quality Business Rules:** In Progress

   Click or tap here to enter text.

7. **Data Dictionaries:** Completed

   Click or tap here to enter text.

8. **Data Conversion/Migration Requirements:** In Progress

   Click or tap here to enter text.

2.12 Financial Analysis Worksheets

Attach F.2 Financial Analysis Worksheet(s) to the email submission. **See Attachment FAWs v2.1**

End of agency/state entity document.

Please ensure ADA compliance before submitting this document to CDT.

When ready, submit Stage 2 and all attachments in an email to ProjectOversight@state.ca.gov.

Department of Technology Use Only

Original "New Submission" Date: 4/8/2025

Form Received Date: 4/8/2025

Form Accepted Date: 4/8/2025

Form Status: Completed

Form Status Date: 7/17/2025

Form Disposition: Approved

Form Disposition Date: 7/17/2025