pGc Paul Garstki Consulting

# INDEPENDENT REVIEW

## OF A PROPOSED

# DRIVER'S LICENSE/ID SYSTEM REPLACEMENT PROJECT

***For the***
***State of Vermont***
***Agency of Digital Services (ADS)***
***And***
***Vermont Agency of Transportation (AOT)***
***Department of Motor Vehicles (DMV)***

***Submitted to the***
***State of Vermont, Office of the CIO***
***by:***

Paul E. Garstki, JD, Consultant
d/b/a/ Paul Garstki Consulting
344 Laird Pond Rd.
Plainfield, VT 05667
***paulg.consulting@gmail.com***

**May 10, 2018**

FINAL
VERSION 3.0a

e-Signed by John Quinn
on 2018-05-17 20:05:18 GMT

e-Signed by Paul Garstki
on 2018-05-15 16:29:51 GMT

e-Signed by Jayna Guilford
on 2018-05-15 16:25:16 GMT

## TABLE OF CONTENTS

## TABLES



## FIGURES

## 1. EXECUTIVE SUMMARY

The Agency of Transportation (AOT) Department of Motor Vehicles (DMV) operates a Driver's License / ID (DL/ID) System (also known as a credentialing system) through a contract with Idemia (formerly Morpho Trust). The system has been in operation since 2003, and is now aging and vulnerable due to:

- Equipment (e.g., card printers) which is End of Life (EOL) and incurring time and money cost for frequent service and repair, including increased customer waiting time for card issuance
- Software which is reaching EOL and End of Service (EOS)
- A contract with which has expired but has been extended by negotiation with Idemia. This contract expires June 30, 2019

The DMV through the proposed project wishes to implement a new, cloud-based system to replace the existing system, which will address the above issues and also:

- Implement "central issuance," by which cards are manufactured and mailed directly from secure facilities by the vendor. Central issuance is preferred by at least 39 states[1] as it supports and simplifies State and Federal security requirements, including Department of Homeland Security requirements – by including improved physical DL/ID security features, fraud prevention measures and manufacturing facility security requirements.[2]
- Improve card security by adding additional features which became available since the current solution was implemented. These features reduce the possibility of identity fraud and theft, assist law enforcement, meet Real ID Act requirements, and conform to industry best practices.[3]

We have found the project to be well thought-out, efficiently managed, and likely to succeed on budget and on-time. The State issued a very well-crafted Request for Proposals (RFP), which elicited a cost-effective proposal from VALID USA, meeting the State's requirements through a project in close alignment to the State's IT Strategic Plan.

[1]Office of the Illinois Secretary of State, *Central Issuance Frequently Asked Questions*, http://cyberdriveillinois.com/departments/drivers/drivers_license/central_issuance/ci-faq.pdf, retrieved April 2, 2018.

[2] *Ibid.*

[3] American Association of Motor Vehicle Administrators, *2016 AAMVA DL/ID Card Design Standard*, 2016, p. xiii.

## 1.1 COST SUMMARY

Table 1 Cost Summary

| | |
|---|---|
| **IT Activity Lifecycle (years):** | **7** |
| **Total Lifecycle Costs:** | **$ 5,756,595.40** |
| **Total Implementation Costs:** | **$ 431,520.40** |
| **New Annual Operating Costs:** | **$ 760,725.00** |
| **Current Annual Operating Costs** | **$ 978,915.00** |
| **Difference Between Current and New Operating Costs:** | **$ (18,190.00)** |
| **Funding Source(s) and Percentage Breakdown if Multiple Sources:** | **State** |

## 1.2 DISPOSITION OF INDEPENDENT REVIEW DELIVERABLES

**Table 2 - Independent Review Deliverables**

| Deliverable | Highlights from the Review<br>*Include explanations of any significant concerns* |
|---|---|
| **Acquisition Cost Assessment** | Actual first year acquisition costs totaling $431,520.40 appear low, but this is because they reflect only the State's internal and professional services costs. The selected vendor's implementation costs (as well as ongoing Operations & Maintenance costs) are financed by the vendor through an all-inclusive price-per-card-issued pricing model, as requested by the State. A better understanding of the cost to the State is found in the Section Impact Analysis on network Operating Costs, below. |
| **Technology Architecture Review** | The vendor's proposed design and network architecture represent state of the art approaches well aligned with the State's current IT strategic plan and preferences. The vendor's technical proposal is very well detailed and highly responsive to the State's operational, functional, and non-functional requirements. We identified a few gaps and a small number of requirements not fully addressed, and in these cases identified some risks with suggested mitigations. Most will be mitigated by simple agreements memorialized in contract.<br><br>The most serious risk, as we assess it, arises from the lack of an Agency- or Department-wide mechanism and process for data governance. Our strongest recommendation to the State from this Independent Review is to begin implementation of a formal data governance process at the Agency level. We are not suggesting that a process needs to be fully developed and in place before implementation begins, but attention to data governance now will help assure data consistency, security, proper stewardship, and usability over the lifetime of the project. |
| **Implementation Plan Assessment** | The vendor's initial sample Implementation Plan is extensive, comprehensive, and exactly aligned with the State's timeline requirements. Both the State and vendor have engaged or assigned appropriate and experienced human resources for project management, monitoring, design, implementation, testing, and training. We judge the project to be very likely to complete on time and on budget. |
| **Cost Analysis and Model for Benefit Analysis** | With the project as now proposed, we can identify cost savings anticipated – when compared to the current system – of approximately $1,095,809.60 over the 7-year life of the project. |

| | |
|---|---|
| | (We emphasize that the current system has become untenable for reasons described above.)<br><br>The intangible benefits we list are significant, and are the benefits envisioned for this project from its inception, representing significant improvements to customer service, alignment with State strategic plans, and improved public safety and security.<br><br>We believe the benefits significantly outweigh the costs. |
| **Impact Analysis on Net Operating Costs** | The first table (all options) shows a slight increase the first year of the project, due entirely to the initial implementation costs. Breakeven occurs at the ***end*** of the second year of the project, as annual savings catch up with initial implementation costs. **We support this version of the project, as it presents the State with significant improvements in customer service and usability** |

## 1.3 IDENTIFIED HIGH IMPACT &/OR HIGH LIKELIHOOD OF OCCURRENCE RISKS

NOTE: Throughout the narrative text of this document, **Risks and Issues are identified by bold red text**, and an accompanying tag (**_RISK_ID#_0_**) provides the Risk or Issue ID to reference the risk, response, and reference in the Risk Register.

The following table lists the risks identified as having high impact and/or high likelihood (probability) of occurrence.

Please see the **Risk & Issues Register, in Section 10**, for details.

Identified High Impact &/or High Likelihood of Occurrence Risks in this project:

**Table 3 - High Rated Risks**

| Risk Description | RATING IMPACT/ PROB | State's Planned Risk Response | Reviewer's Assessment of Planned Response |
|---|---|---|---|
| **DMV lacks a data governance process** | **63**<br>**7/9** | **We agree and intend to follow the reviewer's recommendation and seek data governance guidance from ADS. We feel the impact is lower and should be in the 5 - 7 range.** | **We understand the impact assessment is speculative; however, since the data *includes* protected information, any possible comprise of such data must be rated as high impact – even if any error is much more likely to be minor.** |

## 1.4 OTHER KEY ISSUES

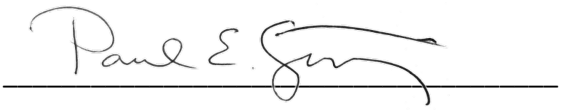
none

## 1.5 RECOMMENDATION

**We recommend that the State continue this project, with attention to the risks identified and mitigations agreed.**

## 1.6 INDEPENDENT REVIEWER CERTIFICATION

**I certify that this Independent Review Report is an independent and unbiased assessment of the proposed solution's acquisition costs, technical architecture, implementation plan, cost-benefit analysis, and impact on net operating costs, based on the information made available to me by the State.**



May 10, 2018

**Signature** **Date**

## 1.7 REPORT ACCEPTANCE

The electronic signature below represents the acceptance of this document as the final completed Independent Review Report.

_____ _____

**State of Vermont Chief Information Officer** **Date**

# 2. SCOPE OF THIS INDEPENDENT REVIEW

## 2.1 IN-SCOPE

The scope of this document is fulfilling the requirements of Vermont Statute, Title 3, Chapter 45, §2222(g):

*The Secretary of Administration shall obtain independent expert review of any recommendation for any information technology initiated after July 1, 1996, as information technology activity is defined by subdivision (a)(10), when its total cost is $1,000,000 or greater or when required by the State Chief Information Officer.*

The independent review report includes:

- An acquisition cost assessment
- A technology architecture review
- An implementation plan assessment (which includes a Risk Analysis)
- A cost analysis and model for benefit analysis; and
- An impact analysis on net operating costs for the Agency carrying out the activity

## 2.2 OUT-OF-SCOPE

- A separate deliverable contracted as part of this Independent Review may be procurement negotiation advisory services, but documentation related to those services are not part of this report.
- Proposals and vendors other than the bidder selected as first choice through the proposed project's procurement process were not evaluated in this Independent Review.

# 3. SOURCES OF INFORMATION

## 3.1 INDEPENDENT REVIEW PARTICIPANTS

Table 4 - Independent Review Participants

| Name | Date | Employer and Title | Participation Topic(s) |
|---|---|---|---|
| **Wanda Minoli** | 3/16/2018 | VT AOT – Interim Commisioner for the Dept. of Motor Vehicles | Overview, planning |
| **Kelly Nolan** | 3/21/2018 & ongoing | ADS - IT Project Manager | Project Manager, General Topics |
| **Jayna Guilford** | 3/21/2018 & ongoing | ADS – IT Portfolio Manager | Single Point of Contact, Project Oversight |
| **Jennifer Pittsley** | 3/21/2018 & ongoing | ADS – DMV Project Coordinator | Work process flow, IT, Architecture |
| **Tom Buonomo** | 3/21/2018 | ADS/AOT - Executive Steering Committee | Overall IT Architecture |
| **Carol Harrison** | 4/6/2018 & followup | AOT – DMV Director of Finance and Logistics | Finance, Funding |
| **Michael Charter** | 4/6/2018 | AOT – DMV Project Coordinator | Finance, Funding |
| **Nancy Prescott** | 3/21/2018 | AOT/DMV – Motor Vehicle Branch Operations Manager | Customer Service Operations |
| **Shannon Fassett** | 3/21/2018 | AOT/DMV – Motor Vehicle Section Chief | Internal Operations |
| **Scott Carbee** | 3/21/2018 | ADS CISO – Deputy Chief Security Officer | Security |
| **Amber DeVoss** | 4/10/2018 & followup | ADS – Chief Technology Officer | Enterprise Architecture |
| **Mark Combs** | 3/16/2018 | ADS EA – Chief Enterprise Architect | Enterprise Architecture |

## 3.2 INDEPENDENT REVIEW DOCUMENTATION

The following documents were used in the process and preparation of this Independent Review

Table 5 - Indpendent Review Documents

| Document | Source |
|---|---|
| **IT Activity Business Case & Cost Analysis (IT ABC Form)<br>DMV DL/ID System Replacement** | State of Vermont |
| **Credentialing System Replacement Project Charter** | State of Vermont |
| **Sealed Bid Information Technology Request For Proposal For Driver's License/ID System Replacement** | State of Vermont |
| **Response: Request for Proposal: Vermont Department of Motor Vehicles – Driver's License/ID System** | VALID USA |
| **Driver's License/ID System Replacement Questions and Answers** | State of Vermont |
| **Roles and Responsibilities Matrix – Credentialing System Replacement Project** | State of Vermont |
| **RACI (responsible, accountable, consulted and informed) Matrix – Credentialing Project** | State of Vermont |
| **VALID Q&A during demo (various email exchanges)** | State of Vermont |
| **Credentialing Proposal Scoring documentation, rounds 1 & 2** | State of Vermont |
| **Vermont Department of Motor Vehicles Records Management Policy – Revised 2/11/2013** | State of Vermont |
| **Information Technology Strategic Plan 2017 – 2021** | State of Vermont |
| **NASCIO Recognition Award Nomination<br>Title: Central Issuance of State Drivers Licenses** | State of North Carolina |
| **2016 AAMVA DL/ID Card Design Standard** | American Association of Motor Vehicle Administrators (AAMVA) |

| | |
|---|---|
| **Digimarc Winds New $30 Million Texas Driver License Contract, 2005** | Business Wire |
| **System Modernization Best Practices (May 2017)** | American Association of Motor Vehicle Administrators (AAMVA) |
| **Security Upgrades to Driver's License/ID Card and Changes to the Issuance Process (May 2016)** | State of Illinois Secretary of State |
| **2017-2019 Biennial Budget Submittal** | Washington State Department of Licensing |

# 4. PROJECT INFORMATION

## 4.1 HISTORICAL BACKGROUND

The Department of Motor Vehicles of the Agency of Transportation provides a credentialing service directly to Vermont citizens, processing initial and renewal applications for a number of personal identification cards, including drivers' licenses, non-driver identification cards, and enhanced ID cards compliant with the federal REAL ID Act (all the various types of cards are referred to below as DL/ID cards). The existing system, operated since 2003 under a contract with Idemia (formerly OT-Morpho, formerly Safran Identity & Security (Morpho)), uses a so-called hybrid approach, by which the State issues cards "over-the-counter" (i.e., printed during the application process at DMV customer service locations throughout the State), by mail (for certain renewal applications, and printed at a State "back office" facility in Montpelier), and printed and mailed centrally by Idemia (for enhanced ID cards). See **6. Technology Architecture Review.**

The existing system is reaching end of life in multiple ways, creating delays and declines in customer service, as well as presenting a vulnerability to a larger-scale breakdown. This system includes

- A vendor contract which initially expired and is currently continuing via a 2-year negotiated extension
- On-site card printers which have reached end-of-life (EOL) and require an average of 16 service calls per month to correct various failures no longer supported by the manufacturer
- A SQL Server database version which will reach EOL in June 2019
- Windows 7 workstation software which has reached End of Mainstream Support in 2015, and will reach End of Extended Support in 2020[4]

In the years since the existing system was implemented, new card technologies, security features, and printing efficiencies, coupled with the increased need for physical security (of card stocks, printing facilities, etc.) to prevent identity fraud have all created a national trend toward "central issuance," the highly secure centralized production of DL/ID cards and subsequent delivery to applicants, usually by US Postal Service.[5]

As a result, the State issued a Request for Proposal (RFP) in November 2017 seeking sealed bids for "a comprehensive set of services that satisfy the State's need for a Driver's License/Identification Card issuance solution."[6] The RFP stated the State's preference for a fixed-price cost-per-card-issued

[4] State of Vermont, *IT ABC Form – DMV DL/ID System Replacement,* pg. 1, 2017.

[5] Office of the Illinois Secretary of State.

[6] Vermont Department of Buildings and Services*, Sealed Bid Information Technology Request For Proposal For Driver's License/ID System Replacement*, p. 4, 2017.

comprehensive solution, while leaving open the possibility of a fixed implementation cost plus labor and materials based on volume.[7]

The RFP elicited several proposals, of which the project scoring team selected two as finalists. Following vendor demonstration sessions, a second round of scoring found a clear preference by the project team for the proposal from VALID USA (VALID), a wholly owned subsidiary of VALID S.A. The proposal envisions a fully cloud-hosted Software-as-a-Service (SaaS) solution, hardware provided (see below), with central issuance from VALID owned secure facilities. The pricing model is fixed-cost-per-card-issued, with an anticipated initial term of 5 years, with State's option to renew for 2 years.

The RFP requested, and the vendor has proposed, implementation of a facial recognition identity control system as part of this project. However, mindful of the Attorney General's determination that facial recognition processes should be suspended pending legislative action on the use of that technology, the DMV has requested implementation of the DL/ID card system *without* activation of the facial recognition capacity. The vendor has complied with an adjusted price and has assured the State that the technology can be activated if and when needed without any changes to the implementation other than configuration changes.

## 4.2 PROJECT GOAL

The Project Charter, approved in November 2017, listed these Objectives and Success Criteria.

**Table 6 - Project Objectives and Success Criteria**

| # | Objective | Success Criteria |
|---|---|---|
| 1 | Implement a new off-the-shelf central issuance solution to replace the outdated system before the current contract with Morpho expires. | The off-the-shelf central issuance solution is implemented on or before July 1 2019 at all 11 DMV locations. |
| 2 | Move production of driver's licenses, instruction permits and identification cards from our 11 DMV locations to secure centralized issuance facility. | 99% Credentials are produced at a secure off-site central issue facility and mailed to customer. |

[7] *Ibid.,* p. 5.

| | | |
|---|---|---|
| 3 | Improve card security by adding additional card features that are available, and more difficult to duplicate or alter. | 100% of newly designed Real ID driver's licenses and Non-driver ID cards contain security features. |
| 4 | Reduce service calls for printer and consumable inventory related down time. | Reduce service calls by 75%. |
| 5 | Credentials are printed and shipped timely to the customer from a secure off-site central issue facility. | 95% of credentials are printed and shipped to customers within three days of file transfer. |
| 6 | Reduce the amount of stock needed on hand for over-the-counter production. | Card stock is reduced by 99%. |
| 7 | Successful Implementation of the identified solution | The agreed upon solution is implemented within fifteen days of the target identified during project planning. |

## 4.3 PROJECT SCOPE

### IN-SCOPE

- Procurement of a Driver's License/Identification Card (DL/ID) services solution that will include the necessary supplies and equipment required to produce identification cards.
- Research the ability to integrate directly with State to State to ensure compliance with Real ID requirements
- Mobile Driver's license option.
- Online renewal option.
- Evaluate & discuss the ability to print on-site at one location for emergency situations
- Research the possibility to have a photo station at each counter at each site.
- Modifications to internal systems such as Phoenix and Mainframe if required.
- Integration with the States' Enterprise Data Environment (EDE).
- Data conversion of current licensing system into new licensing system.
- Major Functionality and Requirements:
    - Photo storage & retrieval solution
    - Design identification cards that meet federal and state regulations
    - Facial recognition solution that must be able to turn off completely with no negative impact
    - Printing and shipping various forms of identification to DMV customers
- Customized reports

### OUT-OF-SCOPE

- Expanding the 2-digit year field in the mainframe (MF) is being handled in a separate project and is not a dependency for this project.

### 4.3.1 MAJOR DELIVERABLES

The table below is derived from the selected vendor's proposal, and shows major design and implementation phases, including training and testing.

**Table 7 - Project Major Deliverables**

| QA / Testing |
|---|
| Equipment Test Plan |
| Equipment Testing Report |
| Functionality Test Plan |
| Functionality Testing Report |
| System Integration Test (SIT) Plan |
| System Integration Testing Report |
| Performance Test Plan |
| UAT Plan |
| Remediation Plan for UAT Issues |
| Security Test Plan |
| Version Release Document |
| **System Design & Development** |
| Fit / Gap Document |
| Solution Design Document |
| Interface Control Documents |
| Requirements Traceability Matrix |
| Interface Control Document |
| Solution System Architect Document |
| System Technical Document |
| **Card Design** |
| Card Layout for DMV review |
| Card Design Specifications |
| Card Prototype Card Layout |
| Card Core Approval Document |
| Card Prototypes |
| Production Card Approval Document (PCAD) |
| **Data Conversion and Migration (DCM)** |
| Data Conversion and Migration (DCM) Plan |
| Data Mapping Document |
| DCM Test Plan |
| **Disaster Recovery /Business Continuity Planning** |
| Disaster Recovery (DR) / Business Continuity (BC) Plan |
| DR/BC Test Plan |
| Test Result for DR/BC Testing |

## 4.4 PROJECT PHASES, MILESTONES, AND SCHEDULE

The following table of milestones is derived from the State Charter document for this project (written before RFP issuance). While the vendor described deliverables above indicate a more finely-grained and solution-specific sequence for the Planning and Execution phases shown below, the present schedule seems a good representation of the project as a whole, and shows the project as broadly on-track as planned.

**Table 8 - Project Milestones and Delivery Timeframes**

| Milestone | Target Delivery Timeframes |
|---|---|
| **Phase: Initiating** | **03/1/2017 - 05/2018** |
| **IT ABC Approved** | 09/11/2017 |
| **RFP Approved** | 11/2017 |
| **Proposals Received** | 01/2018 |
| **Preferred Vendor selected** | 04/2018 |
| **Contract executed** | 05/2018 |
| **Phase: Planning** | **11/2017 – 02/2019** |
| **Requirements gathering** | 11/2017 – 12/2017 |
| **Requirements validation and solution gap analysis** | 3/2018 – 5/2018 |
| **Design** | 06/2018 – 09/2018 |
| **Phase: Execution** | **10/2018 – 06/2019** |
| **Development** | 10/2018 – 02/2019 |
| **User Acceptance Testing (UAT)** | 03/2019 – 04/2019 |
| **End to End Testing** | 04/2019 – 05/2019 |
| **Training** | 05/2019 – 06/2019 |
| **Phase: Closing** | **06/2019 – 09/2019** |
| **Implementation** | 07/1/2019 |
| **Lessons Learned** | 08/2019 |
| **Close Procurement** | 08/2019 |
| **Project End Date** | 09/2019 |

## 5. ACQUISITION COST ASSESSMENT

Acquisition (Implementation) costs *per-se* for this project are all State personnel and professional services costs, because the pricing model for this solution is based on a per-card issued, all-inclusive price. Implementation and hardware costs are borne by the vendor and financed to the State over the life of the contract. The following table shows the strict acquisition costs, all incurred in the first 12 months following contract execution.

**Table 9 - Acquisition Costs**

| Acquisition Costs | Cost | Comments |
|---|---|---|
| **Hardware Costs** | **$ -** | **included in per-card cost** |
| **Software Costs** | **$ -** | **included in per-card cost** |
| **Implementation Services** | **$ -** | **included in per-card cost** |
| **State Personnel** | **$ 394,680.00** | |
| **Professional Services (e.g. Project Management, Technical, Training, etc.)** | **$ 36,840.40** | |
| **Total Acquisition Costs** | **$ 431,520.40** | |

The Cost Summary, in Section 1.1, above, shows a more complete picture of acquisition costs. Based on the State's estimate of number of cards issued (210,000 / year) and proportion of card types (85% "standard" ID, 15% Enhanced ID), and the vendor options selected by the State, yearly cost to the State would be approximately **$760,725.00.** Please see **9. Impact Analysis on Net Operating Costs**, below, for a more detailed comparison of proposed costs to existing costs.

## 5.1 COST VALIDATION:

Describe how you validated the Acquisition Costs.

The vendor's all-inclusive price-per-card-issued costs are presented in the vendor's Price Proposal[8] response to the State's RFP. Subsequent to that proposal, the State requested pricing – within the all-inclusive model – for various options to comply with statutory need, or to add functionality or usability to the project. We reviewed the vendor's responses to those option requests, conferred with State project personnel as to their option choices, and computed the resulting costs **in 9. Impact Analysis on Net Operating Costs**, below.

Additionally, we requested the State's estimate of internal (State employee) personnel needed to implement the project and show these costs both in the Acquisition Cost Table above, and in the Impact Analysis on Net Operating Costs and Cost Spreadsheet Attachment, below.

We believe these summaries represent a reasonable estimate of costs the State is likely to incur. Since the actual costs will depend on the number of credentials actually issued in any given year, the actual cost figures will fluctuate somewhat. However, we have requested and received from the Agency CFO figures demonstrating the actual credential output for the past 10 years and are confident that the estimates we derived are therefore reasonable.

## 5.2 COST COMPARISON:

As most States appear to pay for such services on a per-card issued basis (as in the present proposal), comparing Acquisition Costs *per-se* is meaningless, so we will look at a similar state project. The State of Washington Department of Licensing (WADOL) transitioned from the same previous vendor (Morpho/Idemia) to the same proposed vendor (VALID USA) in 2014. At that time, WADOL was already employing a central issuance system via the previous vendor. They found reduced costs in the transition. The new cost-per-card was $1.89 for regular DL and $4.12 for EDL. We do not know the substrate chosen for the cards. Assuming the basic rate as quoted by the vendor (no options), and a Polycarbonate substrate, Vermont is paying 156% more for DL and 120% more for EDL compared to WADOL's costs of 5 years previous. We think this is a reasonably similar figure, considering that Vermont often suffers some cost impact due to a lower volume (Vermont's population is about 9% of Washington's).

## 5.3 COST ASSESSMENT:

Are the Acquisition Costs valid and appropriate in your professional opinion? List any concerns or issues with the costs.

Yes, this appears to be a very good price for Vermont. The price for the new system in Vermont is very close to the old price (see Impact Analysis on Net Operating Costs, below), and the solution represents a

[8] VALID USA, *Response: Request for Proposal: Vermont Department of Motor Vehicles – Driver's License/ID System*, *Pricing Proposal,* p. 1, 2017.

significant upgrade in features and efficiency, while lowering the impact on State network, hardware, and software.

However, we have noted two areas in which further clarification could protect State interests:

- Although both State and vendor agree at this point in negotiations that the initial contract will be for a 5-year term (with options for renewal), terms of an early termination have not been made explicit, and we identify this as a risk **_RISK_ID# _R5_.** Particularly because the vendor is "financing" the project, including implementation, through a per-card-issued all-inclusive price, we believe a further clarification of respective responsibilities, and especially of financial liabilities, would be useful to protect the State's interests.

- Related to the above concern, the vendor proposes to supply the hardware needed for this project through the same pricing mechanism. However, in our view ownership of the same equipment, especially in the event of an early termination, was not clear enough, and we initially identified this as a risk

  The State responded by leveraging the following contract language is discussions with the vendor: "Valid will transfer title to all equipment delivered to and installed in State Branch Offices and LSO upon acceptance by the State thereof. Valid will provide the State with a Bill of Sale subject to the Warranties as described in the Contract upon completion of all such installations" and "Valid also understand they are responsible for servicing and supporting such equipment."

  We think this addresses our concern, but nonetheless recommend that State procurement specialists review this language to assure its meaning and application in all foreseeable eventualities.

**Additional Comments on Acquisition Costs:**

***none***

# 6. TECHNOLOGY ARCHITECTURE REVIEW

## 6.1 STATE'S IT STRATEGIC PLAN

### DESCRIBE HOW THE PROPOSED SOLUTION ALIGNS WITH EACH OF THE STATE'S IT STRATEGIC GOALS AND ACTIVITIES:

- **Be effective and efficient**
  - **a. Consolidate infrastructure and common services**

    While this project is not a component of a government-wide infrastructure effort, it does contribute to consolidation in these meaningful ways:

    - State-hosted server applications will be retired, removing
      - the need for support and maintenance of physical server instances
      - support with eventual replacement for server operating system instances
      - support with eventual replacement for the application(s) itself
    - The new solution will be web-based for Customer Service Specialists, eliminating the need for installing/supporting/upgrading OS-based workstation software

  - **b. Leverage cloud services**

    The proposed solution is nearly 100% cloud-based Software-as-a-Service (SaaS) with these exceptions:

    - camera/image capture hardware,
    - signature/option/agreement pads for customer use,
    - the workstations used for SOV employee web access
    - the SOV system of record mainframe, enterprise data hub, and associated SOV network infrastructure.

    In our experience, vendor-provided governmental solutions are frequently nominally SaaS, but in practice prove to require significant State infrastructure. The present project is an exception: it offers the hoped-for architectural benefits of SaaS (overlaid on IaaS) with minimal need for State infrastructure resources.

  - **c. Leverage the success of others**

    The project team has consulted frequently and periodically with peers and colleagues through the American Association of Motor Vehicle Administrators (AAMVA) and through professional channels to understand and apply current best practices for DL/ID card

issuance. This consultation resulted in the decision to prefer a central issuance solution, to transition to an entirely new solution (rather than simply upgrading through an existing vendor), and to prioritize business and functional needs.

We note that in general, the project follows quite closely the best practices promulgated by the AAMVA document **System Modernization Best Practices**[9] in these areas

- Analysis of internal and vendor support
- Business Case development
- Governance
- Legislation and Funding
- Requirements and Methodology
- Procurement and Contract Management
- Project Management
- Security
- Organizational Change Management
- Training (prospectively)
- System Design
- Testing (prospectively)

One of the few exceptions we could find to the AAMVA recommendations is the lack of a formal mechanism for data governance, a lack which we identify as a risk **_RISK_ID# _R1_** and consider in more detail below. (In fairness, the AAMVA recommendations primarily consider data governance in the context of data cleansing[10], which the project team has considered. However, a data steward[11] as recommended by the AAMVA is not explicitly identified in the project. Please see **6.9.3 Enterprise Architecture Comments**, below.)

**d. Measure results**

Section 4.2 Project Goals, above, shows a table of project objectives with quantifiable success criteria for each listed objective. We find these criteria to be reasonable, achievable, and in line with project development so far.

The criteria fall into two main areas: achievement of project timeline goals and improvements in customer service responsiveness and cost due to central issuance.[12] The

[9] American Association of Motor Vehicle Administrators, *System Modernization Best Practices, various*, 2017.

[10] *Ibid.*, pg. 42.

[11] The AAMVA *System Modernization Best Practices* states that the data steward "oversees changes to the data, cleaning and purging of data on a regular cycle, and consistency in the use of data for reports or extraction." Pg. 42. The role may have a different title or be performed by more than one individual in Vermont government.

[12] *Charter,* p. 2.

first is supported by the project's continued firm adherence to project milestones, and the second is supported by the solution as proposed in the selected vendor's technical proposal.

- **Reduce risks to data security**

**a. Manage data based on its classification**

The data entered, transmitted, and stored in the solution database, as well as in the State's system of record mainframe database, includes data the State characterizes as "closed"[13] data, containing both Confidential Personally Identifiable Information (PII) and Personal Information from Motor Vehicle Records (PIMVR). The State has required, and the vendor has proposed, safeguards to protect this information, including

- Encryption of data in motion and at rest
- Physical, functional, and operational protections
- Compatibility and coordination with SOV network protections (see 6.3 Security, below)

**b. Defense in depth**

The proposed solution includes multiple and redundant layers of security protection, including private subnets, Network Access Control Lists (NACLs), Security groups, Web Application Firewalls (WAF), Virtual Private Gateways (VGW), and encryption in motion and at rest throughout the system.

**c. Train employees and partners on security awareness**

DMV customer service specialists, and other DMV employees who "touch" closed data – such as DMV internal operations employees – are trained in procedures for protecting information in the current solution and will continue this awareness and these procedures through implementation and operation of the new solution.[14] ADS IT employees at AOT are educated and experienced in relevant security procedures and best practices.

The vendor's proposed training curriculum includes specific training on security processes and procedures[15] for each training cohort (e.g., customer service specialists, administrators, IT employees, etc.).

[13] State of Vermont*, Information Technology Strategic Plan 2017 – 2021*, p. 5, 2017.

[14] Interview, *Motor Vehicle Branch Operations Manager*, with *Motor Vehicle Section Chief*, March 21, 2018.

[15] VALID USA, p. 338.

Additionally, the State has made available government-wide training in security awareness through a third-party vendor.[16]

- **Help project teams deliver successful projects**

  **a. Apply best practices for project management**

  The successful application of project management best practices shows in the excellent results so far evidenced in this project. As an example, we note the very well-crafted RFP. The specificity of the RFP enabled vendors – the selected vendor in particular – to anticipate State concerns and needs, and to respond proactively, which will very likely result in effective and timely contract negotiations. The good RFP is a direct result of the team – and especially the project manager – having done their "homework" in analyzing business processes, collecting needs and preferences, and defining requirements, and crafting a comprehensive yet comprehensible vendor response form.

  Also, please see **7.4 Project Manager**, below.

  **b. Leverage business process optimization (BPO) processes**

  **N/A**

  **c. Apply enterprise architecture**

  The project has had an assigned Enterprise Architect from ADS since approximately from the time the present Independent Review commenced. The assigned Enterprise Architect (EA) has reviewed the vendor's proposal and has begun conversations with the project team about EA matters. Please also see Additional Comments on Architecture at the end of this chapter, below.

## 6.2 SUSTAINABILITY

We characterize the proposed solution as Software as a Service (SaaS) – the vendor's WebID and BioID applications – hosted on Infrastructure as a Service (IaaS) – the cloud hosting service, initially Amazon Web Service (AWS), but potentially any other service meeting the vendor's criteria and providing value for money. The solution requires a minimum of hardware at State customer and back office locations – ID image capture cameras, digital signature pads which double as option choice screens (e.g., for organ donor), and standard web access workstations running common web browsers. Aside from network connectivity *per-se*, the rest of the solution resides entirely "in the cloud" with data returning to the SOV network for storage on the SOV mainframe system of record.

[16] Interview, *Vermont Deputy Chief Information Security Officer,* March 21, 2018.

The resulting hardware and software "footprint" on the State's network is minimal. Most of the potential changes, updates, and improvements over the life of the project would take place "in the cloud," and require little or no replacement or recycling on the part of the State.

## 6.3 SECURITY

The vendor's technical proposal responds in detail to every State security and privacy related non-functional requirement.

The WebID and BioID applications reside within the AWS environment, which is FedRAMP certified, and therefore as a hosting environment, meets State requirements and preferences.[17] As noted by the CISO office, however, the security of a cloud hosting environment does not guarantee the security of the application itself.

The vendor states that:

> *VALID performs a third-party audit every month, and it has numerous compliance certifications stemming from these audits: ISO / IEC 27001:2013; Payment Card Industry (PCI DSS); Service Organization Control (SOC) 2 Type II; GSMA Security Accreditation Scheme (GSMA SAS) Class 1; Visa, MasterCard, Discover, and American Express. These audits require VALID to submit its applications to security vulnerability tests. It hires 3rd parties to run automated penetration tests and "hack" the applications to expose any weaknesses.*[18]

These controls meet the State's requirements and preferences. They do not by themselves, however, fully demonstrate the security status of the solutions since, for example, audits may reveal weaknesses. (We do acknowledge that the vendor states no current weaknesses or vulnerabilities are identified.[19]) The vendor does not, in its proposal, offer periodic reports or attestations of the results of these audits and tests. We identify this as a risk **_RISK_ID#_R3_** and recommend that the State, through contract negotiation, establish a process for regular, periodic provision of security audit and test results/attestations, at least on an annual basis, and to an extent that satisfies the need for demonstration of appropriate security. The POA&M mentioned elsewhere may be an appropriate

[17] State of Vermont, *Attachment D – Other Terms and Conditions for Information Technology Contracts,* various, 2017.

[18] VALID, p. 104.

[19] VALID, p. 114.

container for this documentation.[20] The State CISO office informs us that they will dedicate the necessary resources to timely review, evaluate, and document these attestations.[21]

We find that the proposed solution's role-based authentication mechanisms and procedures align well with the State's preference for integration with the State's Active Directory Policy. The vendor states:

> *The VT DMV Active Directory Group Policy will handle many of the password management functions forced on the applications' users. The system will not store any VALID-supplied default password or users. The applications feature a re-authentication option for critical system processes such as 1:1 overrides or ICAO overrides. VT DMV system administrators decide if it wishes to use the re-authentication function*.

This ensures that the State can used its existing internal controls to regulate which employees have access to which data, automatically adjusting access when individuals leave employment, change roles or level of access, etc.

## 6.4 COMPLIANCE WITH THE SECTION 508 AMENDMENT TO THE REHABILITATION ACT OF 1973, AS AMENDED IN 1998

The proposed solution does not rely on federal funds, nor is it part of a federal project. Therefore, Section 508 does not apply. However, the State requires accessible architecture for its IT projects, and if online portions of the solution are eventually implemented (e.g, online renewal), the State will require accessible interfaces. In that case, Section 508 compliance may serve as a reliable *guide* to what the State would want. The expectation would be that the vendor, designing the interfaces, would employ Section 508 analysis and demonstrate to the State that the interfaces were compliant.

## 6.5 DISASTER RECOVERY

The proposed solution employs a particularly robust approach to disaster recovery (DR). Instead of a conventional approach utilizing a primary and backup datacenter deployment, and a primary and backup central issuance facility, the proposed solution employs and exact live mirrored datacenter, geographically separated from the primary datacenter at an AWS hosting location, and containing at all times live and synchronized data. If one datacenter goes down for some reason, the other datacenter should be able to continue operations with no change in service to the State users.

Similarly, there are two card production and issuance facilities, geographically separated, both of which operate continually at similar levels, and each of which can support 100% of the State's needs. If either facility becomes non-functional, the other can continue the entire needed production without a perceived change in service level to the State. The supporting theory of operation is that traditional

[20] Interview, *Enterprise Architect,* April 10, 2018.

[21] Interview, *Deputy CISO,* March 21, 2018.

"backup" facilities often cannot operate at full efficiency, because they are not staffed, operated, and monitored at the same level as the "primary" facility. Therefore, having two exactly functionally equal facilities, both in production, any with adequate excess capacity, and failover should be invisible to the consumer (in this case, the State).

Details and documentation of the approach, and the status of both datacenters and both production facilities, are to be made available to the State as part of the implementation and operation.

We think this is an excellent approach, and that it addresses well the State's requirement for disaster recovery.

## 6.6 DATA RETENTION

The system of record for DMV data is the SOV mainframe. This database retains records pursuant to 1 V.S.A. § 317a (Disposition of public records). DMV has adopted and adapted General Records Schedules (GRS) issued by the Vermont State Archives and Records Administration (VSARA) of the office of the Secretary of State to ensure compliance with legal requirements. A list of specified Schedules is available from the AOT[22] and has been reviewed for the present report. The applicable schedules appear to us comprehensive and appropriate for the proposed project.

## 6.7 SERVICE LEVEL AGREEMENT

### WHAT ARE THE POST IMPLEMENTATION SERVICES AND SERVICE LEVELS REQUIRED BY THE STATE?

The RFP for this project required bidders to include a sample Service Level Agreement (SLA) as Attachment 8 to the sealed bid.

### IS THE VENDOR PROPOSED SERVICE LEVEL AGREEMENT ADEQUATE TO MEET THOSE NEEDS IN YOUR JUDGMENT?

The selected vendor's sample SLA shows service levels, measurements, and remedies for failure to meet levels for the following categories:

- Solution Availability
- Scheduled Maintenance
- Licensing Office Outage – Onsite Issue Resolution
- Credential Quality

[22] State of Vermont, *Vermont Department of Motor Vehicles Records Management Policy*, Revised February 11, 2013.

- Disaster Resolution
- Security Compliance

The sample also includes a sample monthly SLA report of the sort that would be provided to the State as part of the solution.

We believe the sample SLA shows service levels, measurements, and remedies which are reasonable and adequate given usual industry norms. Regardless of our opinion, we believe the State should review each service level, measurement, and remedy in the course of contract negotiations to confirm that State needs are met.

## 6.8 SYSTEM INTEGRATION

### IS THE DATA EXPORT REPORTING CAPABILITY OF THE PROPOSED SOLUTION CONSUMABLE BY THE STATE?

Yes, the solution includes within the fixed price-per-card-issued the development and implementation of data export and reporting to meet State needs and requirements, including compatibility with the State's Enterprise Data Hub interface(s) to export data to the State's system of record.

### WHAT DATA IS EXCHANGED AND WHAT SYSTEMS (STATE AND NON-STATE) WILL THE SOLUTION INTEGRATE/INTERFACE WITH?

***Please create a visual depiction and include as Attachment 1 of this report.***

[See attachment 1]

***Will the solution be able to integrate with the State's Vision and financial systems (if applicable)?***

N/A

## 6.9 ADDITIONAL COMMENTS ON ARCHITECTURE:

### 6.9.1 EXISTING SYSTEM APPLICANT PROCESS FLOW

Fig. 1, below, shows a simplified diagram of the applicant process flow from the customer applying for a credential (applicant) to the issuance of the final card. The existing system utilizes a Windows-based application installed on DMV workstations accessible to customer service specialists and internal operations employees. The application provides an interface to the State's mainframe system of record.

Applicants at customer service locations provide supporting identification documentation to customer service specialists, who authenticate the documents manually and enter card-relevant data directly into the mainframe system of record. They also query the applicant regarding other statutorily required options, such as “Motor Voter” registration and organ donor status and enter the replies appropriately. The customer uses a digital pad to enter a signature into the system. The card-relevant data is transferred via nearly immediate FTP from the mainframe to the Morpho ID server-based application installed on a virtualized server in a SOV datacenter and employing SQL Server as a backend database.

The customer service specialist or other authorized employee then uses the imaging camera, which is connected to the server application, to capture the applicant’s image and assign it to the card application. When all parts of the application are complete, the card can be issued. Most cards are printed on specialized printers located in the DMV service locations. Most cards are printed at those sites and issued to applicants in person the same day. Card stock is stored in a secured central location. Renewals ordered by mail are printed at DMV internal operations in Montpelier and mailed to applicants via USPS. Enhanced ID cards are printed at current vendor's facility and mailed to consumers as they have an RFID chip in them which means they cannot be printed on the printers in VT DMV offices.

When this process is complete, typically 1-2 days later, other information from the applicant supporting documentation is entered by State employees into the mainframe system of record. Some of this information duplicates or possibly corrects or alters information already entered and now existing in both the system of record and the Morpho ID database, and the possibility exists for discrepancies to arise.

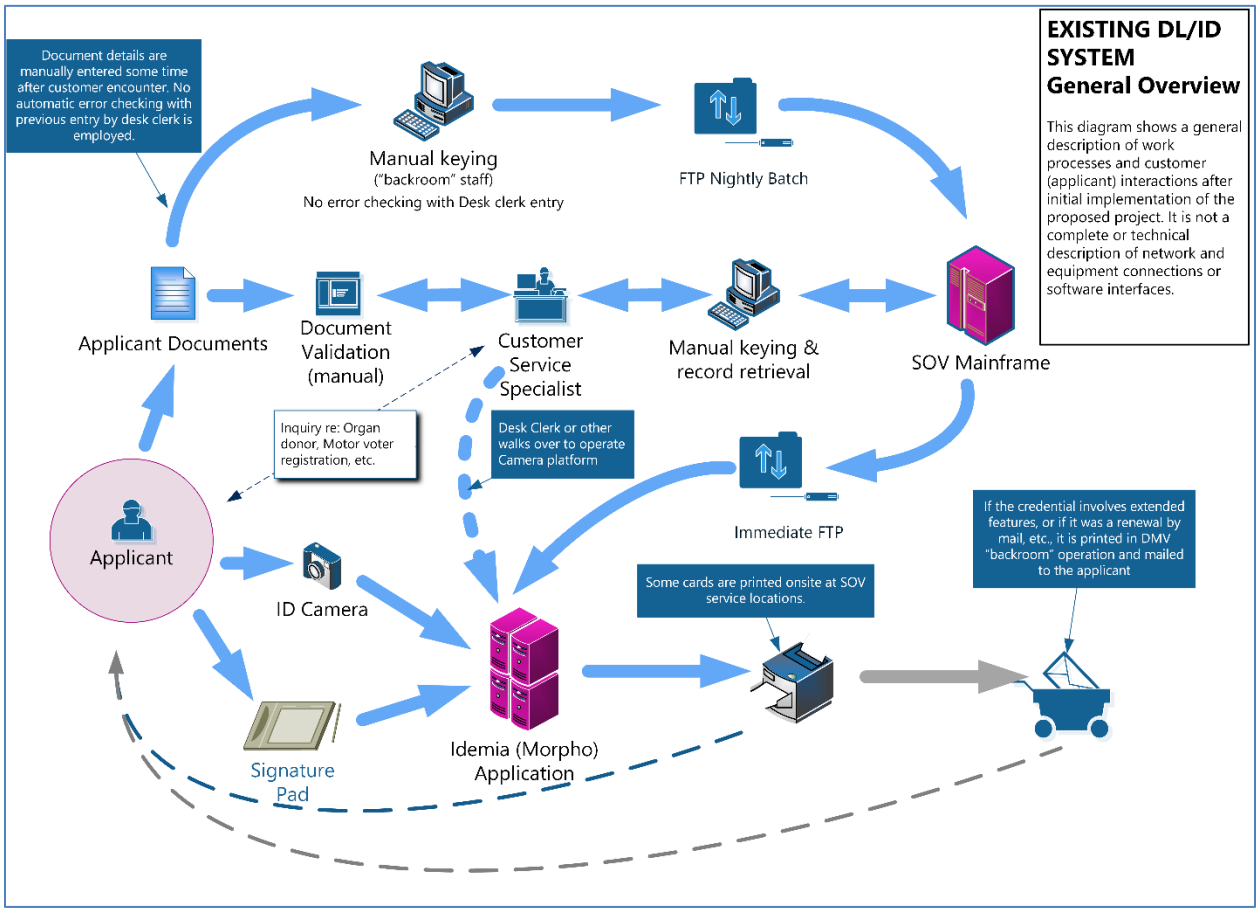



**Figure 1 – Existing DL/ID System**

### 6.9.2 PROPOSED SOLUTION APPLICANT PROCESS FLOW

The proposed solution applicant process flow is shown in simplified form in Figure 1, below. As above, the applicant brings supporting documentation to the customer service location. A customer service specialist reviews the documentation and scans it for submission to a secure 3rd-party document authentication service, which employs sophisticated algorithms to generate a statistical determination on the likely authenticity of the documents presented. The specialist then uses a web browser to access the VALID WebID application, which is cloud-based. The VALID application utilizes the State's Active Directory authentication to ensure only appropriate role-based access to any part of the application.

Data entered in the VALID WebID application immediately updates the WebID database, also cloud-hosted. Signature + option digital entry pads at the service desk allow the applicant to explicitly select or deselect options such as "Motor Voter" registration and organ donor status, as well as to enter a signature for the application. The applicant is directed to a camera station (which also has an identical signature + option pad for an alternative way to complete this function) and an image is captured for the credential and associated with the other application data.

No cards are printed at the customer service facility. Once all parts of the application are complete, the applicant may be issued a temporary credential in the form of a paper printed on a conventional office printer. The temporary credential is meant to be carried by the applicant along with the expiring credential, if any, and serves as a temporary confirmation in the event of a traffic stop, etc. It is not a full credential for all federal and state purposes.

The actual issued DL/ID card is printed by VALID in one of two secure production facilities (factories) and mailed to the applicant via USPS utilizing methods designed to minimize the possibility of theft or diversion in the delivery process. Generally, the issued card is mailed within one day.[23] If the State determines that a DL/ID card is needed as quickly as possible, an expedited process is available at extra cost per expedited card to the State, allowing for overnight delivery of the issued card via courier service. Note that the proposed solution applicant flow process does not have a separate entry step for other supporting documentation, thereby lessening the chance for discrepancy between data in the mainframe system of record and the VALID database, or between mismatched records in the system of record.

[23] VALID, p. 92.

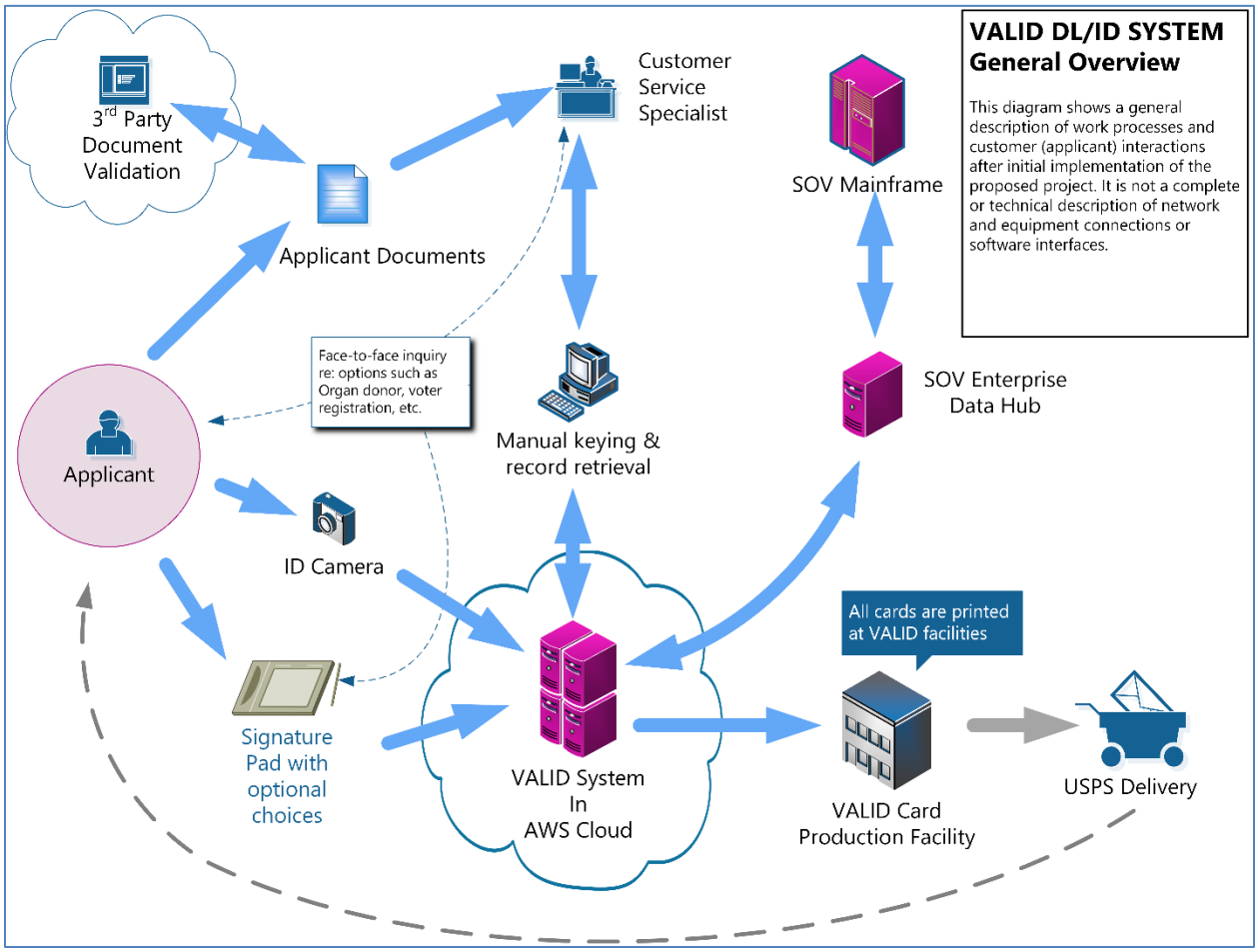



**Figure 2 – VALID (Proposed) DL/ID System**

### 6.9.3 ENTERPRISE ARCHITECTURE COMMENTS

In general, we find the selected vendor's response to architectural requirements, both functional and non-functional, to be comprehensive and detailed. This is due in no small part to the State's excellent preparation work leading to the vendor response form in the RFP, which makes clear to bidders what the State is looking for.

Aside from the high level of responsiveness demonstrated by the selected vendor in the technical proposal, we would emphasize some of the following very general features of the proposal which make it a good fit for the State's architectural preferences:

- As described above, the solution is almost pure SaaS, with a minimum of impact on State network and equipment.
- The cloud hosting solution (Amazon Web Services – AWS) is FedRAMP certified, ensuring a high governmental level of security at the datacenter hosting level.
- The implementation plan is nearly 100% configuration, rather than customization (We define configuration as modification using tools native to the solution and intrinsically available, and customization as any other code changes.) This is highly congruent with the State's architectural preferences, to maximize re-usability and minimize development costs.
- The solution integrates tightly with the State's Active Directory authentication mechanism. This minimizes the cost of resources needed to ensure that only the proper personnel have access to closed data, simplifies training for State employees, and increases usability for those employees, as they can use a single sign-on (SSO) to access the solution in the context of their other work.

The project has engaged Enterprise Architectural review and assistance concurrent with the present review, and an Architect has been assigned to the project. She is currently reviewing aspects of the project and working with the project team to understand all aspects of the architecture. The concerns below have been developed in part by conversation between Independent Reviewer and Enterprise Architect.[24] We recommend the inclusion of the Enterprise Architect in design sessions that the team undertakes with the vendor.

We present the list of concerns below, therefore, not as a "tip of the iceberg" of problems, but rather as a relatively brief list of concerns or needs, most of which are remediable or addressable before contract execution. Of all these concerns, we suggest that the first listed is the most important and in need of attention:

- As acknowledged by both State and vendor, this project involves the acquisition, storage, conversion, migration, and synchronization of protected, "closed" data, particularly

[24] Interview, *Vermont Enterprise Architect,* April 10, 2018.

Personally Identifiable Information (PII) and Personal Information from Motor Vehicle Records (PIMVR). [25] Our interviews have shown that neither the DMV nor the AOT as a whole currently has a formal or informal data governance process in place. We identify this as a risk **_RISK_ID# _R1_**. As the AAMVA states in System Modernization Best Practices, "Data governance is essential for these activities during the project lifecycle, and consideration should also be given to implementation of data stewardship for operational activities related to maintaining data integrity and quality."[26]

The lack of a data governance mechanism is not a failing of the project *per-se*, but represents a serious absence in the Agency context in which the project takes place. We acknowledge that data governance is not consistent across State government, and that it takes time to develop and implement an effective process – so we are not suggesting that a formal data governance process should be up and running before the project is implemented. **We recommend that a data governance process be *initiated* to provide eventual data governance context for this project during its initial lifecycle.** Obviously, the sooner the better; the Agency of Digital Services, through the new Chief Data Officer function, will likely be able to provide guidance in this area.

- The solution as constituted continues the practice of maintaining a system of record on the State mainframe while using the vendor-provided database for the actual process of issuing and maintaining credentials, without having continuous and explicit synchronization in both directions. We identify this as a risk **_RISK_ID# _R2_**, because we believe it increases the opportunity for data to be inconsistent across both databases. The State is aware of this situation and has considered means and methods of retiring the mainframe database(s) and cleaning the data which does exist there, although this is out of scope for the present project. We recommend the State consider solutions, including – if budget permits – discussing with the vendor the possibilities for implementing a full migration of the database to the vendor's cloud database. Whatever solution may be found, we note here the need for a data governance process, as described above, and suggest that having a governance process in place may point to efficient solutions for this and other related databases.

- The vendor response form in the RFP, in the context of security-related non-functional requirements, asked the vendor to describe how the requirement of "POA&M [Plan of Action and Milestones] Management" is met.[27] The vendor tagged this requirement as "Not applicable," as no security weaknesses were currently identified. We identify this as a risk **_RISK_ID# _R8_**. While we think the vendor was sincere in its statement, we believe they

[25] RFP, *Bidder Response Form 4.5 Data Compliance*

[26] AAMVA, p. 42.

[27] RFP, *Bidder Response Form 4.3 Security S16*

missed the point of this requirement, which concerned POA&M ***management***. The State reasonably wants to know how the vendor manages findings/weaknesses/milestones. We recommend the State request and require a description of POA&M management. The State prefers POA&Ms as a management tool; we are told that the tool can be a container for reports and documents such as security audit attestations described above in **6.3, Security**.

- The vendor response form asks whether the solution uses a Business Intelligence (BI) software. The vendor replied that "The AWS solution we are proposing does include a BI engine that VALID utilizes for processing, analytics and reporting." However, the name of that software was not indicated. We first identified this as a risk because the State prefers specific software tools for this purpose. However, the project manager and team asked for further clarification from the vendor, and the details received in response are satisfactory to both the assigned Enterprise Architect and this reviewer.

- The design and activation of online web portals for public use is referenced in the project,[28] but not in scope for the initial implementation. It is, however, planned for implementation immediately following the "go-live" of the proposed system. The State has certain preferences in the design, usability, and consistency of State online portals, to maintain customer satisfaction.[29] At this point, we are not aware of an AOT/DMV "roadmap" for online portal design and use. We identify this as a risk **_RISK_ID# _R10_**. We recommend that the project team include the assigned Enterprise Architect in any design or planning sessions that may arise in advance of online portal implementation.

[28] RFP, *Section 2 Scope of Work*

[29] Interview, *Enterprise Architect,* April 10, 2018.

# 7. ASSESSMENT OF IMPLEMENTATION PLAN

## 7.1 THE REALITY OF THE IMPLEMENTATION TIMETABLE

The initial implementation of the proposed solution has a date certain by which it must be implemented, in order to avoid any additional extension of the already extended contract for the existing solution. In reviewing the progress of the project since the creation of the project Charter, we note that the project team has remained very closely aligned with the original timeline targets. With a very good technical proposal in hand, a vendor with a demonstrably good track record, and a favorable price, the State is on track to complete the project on time as planned.

## 7.2 READINESS OF IMPACTED DIVISIONS/ DEPARTMENTS TO PARTICIPATE IN THIS SOLUTION/PROJECT (CONSIDER CURRENT CULTURE, STAFF BUY-IN, ORGANIZATIONAL CHANGES NEEDED, AND LEADERSHIP READINESS).

In meetings with the project team and its members, we witnessed a high level of commitment, project understanding, determination to meet timeline targets, and flexibility (for example, in response to this reviewer's questions or risk identifications). The buy-in appeared vertically consistent, with top Agency management actively participating when appropriate. Front-line staff are welcoming of the impending changes, and even anxious for the project to proceed.

## 7.3 DO THE MILESTONES AND DELIVERABLES PROPOSED BY THE VENDOR PROVIDE ENOUGH DETAIL TO HOLD THEM ACCOUNTABLE FOR MEETING THE BUSINESS NEEDS IN THESE AREAS:

### 7.3.1 PROJECT MANAGEMENT

The vendor combines traditional PMBOK-style management for monitoring, documentation, and oversight, with Agile/Scrum-style management for configuration tasks. The vendor's assigned project manager is both well-experienced and appropriately credentialed.

### 7.3.2 TRAINING

The vendor provides a sample training curriculum for each of these cohorts:

- DMV operational staff
- DMV administrative staff
- External partners
- IT/Technical staff
- Other roles as determined by DMV

The training plan elements include

- Develop an overall training strategy in partnership with the DMV.

- Coincide the training schedule for DMV locations with the approved installation sequence and schedule.
- Establish the training program and schedule by the functional team, system administrators, the DMV locations, and Help Desk staff, prior to the initial conversion to the new system.
- Develop training materials, as determined by the DMV, for the DL/ID System Solution consisting of:
    - Electronic (fully editable) formats of each training document
    - Self-paced, e-learning training modules

### 7.3.3 TESTING

Testing goals and targets are to be determined in consultation with the State team. The sample testing plan is comprehensive and appropriate to the deliverables of the project.

### 7.3.4 DESIGN

This project is potentially purely configuration rather than customization, in alignment with the State's preferences. All configuration deliverables are related to existing application features and can be demonstrated with past implementations. In the event customization is nonetheless desired by the State for some reason, the proposal lists appropriate processes for design, implementation, and testing.

The vendor employs standard Agile/Scrum methodology for configuration design stages, and standard PMBOK strategies for project documentation, overall management, and tracking. These approaches are consistent with State preference.

### 7.3.5 CONVERSION (IF APPLICABLE)

The vendor addresses data conversion and migration (DCM) in the form of 3 deliverables:

- Data Conversion and Migration (DCM) Plan
- Data Mapping Document
- DCM Test Plan

The vendor's proposal identifies the main processes used for data conversion:

1. **Initial Data Import** – During this phase, the DMV's data is converted to a new schema, imported into staging tables and analyzed for integrity and completeness.
2. **Enrollment into BioLink ID** – During this phase, all historical customer photographs are enrolled into the BioLink ID facial recognition system.
3. **Import into WebLink ID** – During this phase, all existing and historical customer records are imported into VALID's WebLink ID application.

The following diagram of the overall DCM process was provided by the vendor:

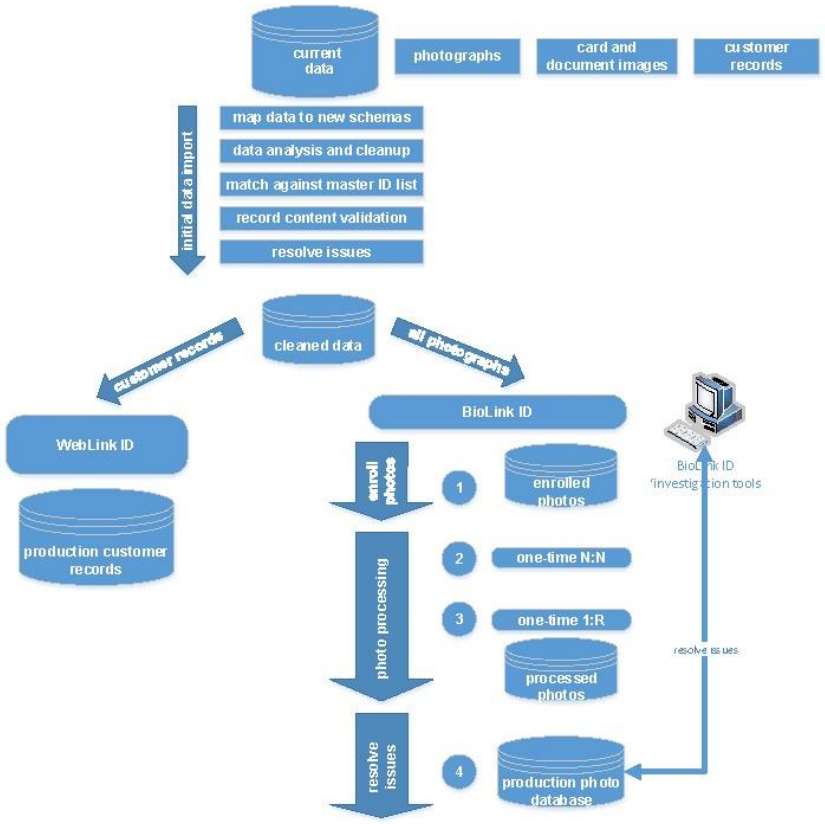



**Figure 3 - DCM Process**

## RISK OF IMPORTING CERTAIN DATA

The State has informed us that

> *In 2017 the business practices around the use of Facial Recognition came into question. The administration and AOT after consulting with the Attorney General's office made the decision to suspend the use of Facial Recognition with the intention of introducing clarify language to the Vermont legislature. Draft language has been developed and will be being introduced next session.*[30]

In the process of importing existing customer and historical data from the State's mainframe SOR, we note the need to be careful about the source of all data imported/migrated. If any facial recognition

[30] Jennifer Pittsley, PMP, *Email*, May 1, 2018.

data not intended to be used at this time *exists as historical data in the SOR*, importing that data into the new cloud database could unintentionally imply use of that data, or at least create the appearance of use. (*Ed: This is a suggestion of possible public perception and should not be construed as legal advice.)* We identify this as a risk, **_RISK_ID# _R11_** and suggest a mitigation process of staging the data migration with careful vendor attention and appropriate State participation to avoid the inclusion of data which should not be used at the present time. **We acknowledge here that image data alone (DL/ID card pictures) are not themselves facial recognition data, and probably constitutes most or all of the data in the database. Nevertheless, we urge caution whenever there is any doubt.**

### 7.3.6 IMPLEMENTATION PLANNING

The vendor-provided sample implementation plan for the DMV project is extensive and comprehensive, containing 652 Tasks to project completion, covering 1 year, and including for each task an ID, Name, Duration, Start Date, Completion Date, Participants, and Dependencies.

### 7.3.7 IMPLEMENTATION

The vendor has assigned adequate and appropriately experienced resources to cover all aspects of the implementation plan.

## 7.4 DOES THE STATE HAVE A RESOURCE LINED UP TO BE THE PROJECT MANAGER ON THE PROJECT? IF SO, DOES THIS PERSON POSSESS THE SKILLS AND EXPERIENCE TO BE SUCCESSFUL IN THIS ROLE IN YOUR JUDGEMENT? PLEASE EXPLAIN.

The project engaged an internal State project manager(PM) who has been deeply involved with all stages of project development since the establishment of the IT ABC form in September 2017. The PM has been professional, active, and efficient throughout the project stages thus far – especially important since this project has a time constraint. A SharePoint document repository contains crucial project documentation and appears to be actively used and referenced by project participants.

The repository contains all important project management tools reflecting ADS preferences and best practices, and uses ADS templates. Some tools are lightly populated, but this is normal at the current pre-contract-execution stage. The tools needed in subsequent stages are in place, and are likely to be actively used according to PM best practices. We would like to have seen more extensive documentation of the vendor proposal scoring process, although what exists in the repository is more than we usually see on a State project, and certainly more than adequate to show that the process was fair, collaborative, and broadly participative.

**Additional Comments on Implementation Plan**

***none***

## 8. COST BENEFIT ANALYSIS

### 8.1 ANALYSIS DESCRIPTION:

As described below and above, this project is intended largely to replace an aging and obsolete system while gaining enhancements in quality and customer service (intangible benefits). Therefore, the most accurate cost benefit analysis is simply the **9. Impact Analysis on Net Operating Costs**, below.

### 8.2 ASSUMPTIONS:

- That current costs as gathered in cooperation with AOT CFO office fairly represent annual expenditures
- That no State employees are displaced as a direct result of this project
- That vendor pricing with included options remains the same through the course of contract negotiation and execution
- That the project will complete on time

### 8.3 FUNDING:

The Transportation Fund of the Vermont AOT comprises 100% of the funding source for the proposed project. The Transportation Fund receives revenue from Gasoline tax + assessment, Diesel fuel tax, Motor vehicle purchase & use tax, Motor vehicle fees, and various other fees & taxes. The fund is sufficient to cover the proposed costs of the project and any reasonable fluctuations, based on the comparison of proposed project cost to existing system cost.[31] (See **9. Impact Analysis on Net Operating Costs**, below)

### 8.4 TANGIBLE COSTS & BENEFITS:

The primary driver for this project came from a need to replace a system that was aging (reaching end-of-life for both hardware and software, and incurring time/money costs for repairing EOL printers) and a service that was obsolete (contract had expired and was extended only by negotiation). No specific tangible benefits were planned or identified for this project; in fact, the initial IT ABC form anticipated significant implementation costs which were not necessary with the selected vendor.

However, with the project as now proposed, we can identify cost *savings* anticipated when compared to the current system, of approximately **$1,095,809.60 over the 7-year life of the project.** This estimate is

[31] Interview, *Chief Financial Officer,* April 6, 2018.

based on the analysis and assumptions shown in **9. Impact Analysis On Net Operating Costs**, below. (We emphasize that the current system has become untenable for reasons described above.)

## 8.5 INTANGIBLE COSTS & BENEFITS:

Provide a list and description of the intangible benefits of this project. Intangible benefits include cost avoidance, the value of benefits provided to other programs, the value of improved decision making, public benefit, and other factors that become known during the process of analysis. Intangible benefits must include a statement of the methodology or justification used to determine the value of the intangible benefit.

**Table 10 - Intangible Benefits**

| Benefit | Justification |
|---|---|
| **Improved security features in DL/ID cards improve public protection against identity fraud and theft, and aid law enforcement** | Industry best practices and government security recommendations provide strong indications that this benefit would be achieved. |
| **Achieve customer service waiting times of 30 minutes or less** | MInimize down time due to equipment issues (no card printers at State sites; cameras and signature pads are new and supported in-contract by vendor, with backup units available at short notice). Recent history of delays due to equipment failures support the likelihood of achieving this benefit. |
| **Cost avoidance if employee time dedicated to tasks replaced by central issuance (e.g., internal processing, printing, mailing) can be dedicated to other functions** | Cards are processed, manufactured, verified, and mailed from vendor's facilities |
| **Diminishment of Fraud** | Card security features significantly increased |
| **Cost avoidance of card printer repair, support, replacement** | Card printers are no longer needed. |
| **Recover secure facilities for storing card stock, etc.** | No longer needed |
| **Cost avoidance for acquisition, replacement, maintenance of State enterprise network resources** | The proposed solution is cloud-hosted and requires minimal State enterprise network resources |
| **Increased security and privacy for citizen's information held in system** | Cloud based solution uses highly secure and frequently tested facilities; disaster recovery system is extremely robust |

## 8.6 COSTS VS. BENEFITS:

The costs of this project represent some tangible savings over the costs of the current solution and are probably much lower than the costs (speculative) of *continuing* the current solution, if that were possible. Nearly all of the new cost is contained in the implementation phase, and that is largely assigned to assignment of existing State resources.

The intangible benefits we list are significant, and are the benefits envisioned for this project from its inception, representing significant improvements to customer service, alignment with State strategic plans, and improved public safety and security.

We believe the benefits significantly outweigh the costs.

## 8.7 IT ABC FORM REVIEW:

The IT ABC Form represents estimates of project cost and implementation appropriate to the inception of the project, but at some variance with the project as it stands on the eve of contract execution. The IT ABC form anticipated a 10-year project lifecycle (based on current expiring project), while the project now expects a 7 year lifecycle (5 year initial contract, 2 year optional extensions). Costs compare as shown in this table

**Table 11 - IT ABC Form Comparison**

| | Implementation Cost | Annual Cost | Lifecycle Cost |
|---|---|---|---|
| **IT ABC Form** | $ 3,063,500 | $ 732,000 | **$ 8,187,500** Pro-rated |
| **Proposed Project** | $ 431,520 | $ 750,225 | **$ 5,683,095** |
| **Difference** | $ 2,631,980 | ($ 18,225) | **$ 2,504,405** |

The table demonstrates that the IT ABC form was very conservative on implementation costs, and almost exactly on target for annual costs. This is largely due to the significant development, hardware, and software costs – which are largely mitigated in a project which relies on cloud deployment and configuration over customization. This latter point seems to provide good support for the State's strategic preference for these characteristics. Of course, hardware cameras and pads are included in the proposed project and financed by the vendor in the per-card price, so regardless of the implementation

cost difference, we conclude (1) that the IT ABC was very conservative; and (2) that the proposed project price seems a good deal for the State.

**Additional Comments on the Cost Benefit Analysis:**

***none***

# 9. IMPACT ANALYSIS ON NET OPERATING COSTS

## 9.1 PRICING COMPONENTS

The following table lists the *per-card-issued all-inclusive* price for the State's chosen type of card substrate and various chosen options (including the option to employ facial recognition technology). These prices are expected to be valid throughout the 5-year life of the contract (and potential extension period of 2 years).

The table also shows the cost division of an estimated 210,000 cards issued per year between standard DL/ID cards, estimated at 85% of the total, and Enhanced DL cards, estimated at the remaining 15%. The table does *not* include totals for "expedited" cards (at $30.00 @), since the number of expedited cards is not predictable.

**Table 12 - Pricing Components**

| All-inclusive Per-Card Cost | DL/ID per-card incl. implementation | EDL per-card incl. implementation |
|---|---|---|
| Polycarbonate | $ 2.95 | $ 4.68 |
| + Facial Recognition[32] | $ - | $ - |
| + Document Authentication | $ 0.296 | $ 0.296 |
| +100 Topaz Pads | $ 0.065 | $ 0.065 |
| + Breeder Doc Scanners | $ 0.052 | $ 0.052 |
| **TOTAL PER-CARD** | **$ 3.363** | **$ 5.093** |
| % | 85.00% | 15.00% |
| # of cards | 178,500 | 31,500 |
| Annual Cost | $ 600,295.50 | $ 160,429.50 |

The above table is the source for the figures in the tables on the following page

[32] Facial Recognition technology is implemented as part of the vendor's basic all-inclusive price-per-card issued. An option is included by State request to delay implementation of the technology; this option is presented as a negative cost (-$0.50/card) and only available if FR is delayed for 12 months or more. Therefore, including FR results in zero cost in this table.

## 9.2 INSERT A TABLE TO ILLUSTRATE THE NET OPERATING COST IMPACT.

**Table 13 - Impact Analysis, All Options**

| ALL OPTIONS, NO FACIAL RECOG. : | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CURRENT** | **Implementation** | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7 | **Total** |
| Annual Total Cost | $- | $978,915.00 | $978,915.00 | $978,915.00 | $978,915.00 | $978,915.00 | $978,915.00 | $978,915.00 | $6,852,405.00 |
| Cumulative Cost | | $978,915.00 | $1,957,830.00 | $2,936,745.00 | $3,915,660.00 | $4,894,575.00 | $5,873,490.00 | $6,852,405.00 | |
| **VALID SOLUTION** | **Implementation** | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7 | **Total** |
| Estimated Annual Cost | $431,520.40 | $750,225.00 | $750,225.00 | $750,225.00 | $750,225.00 | $750,225.00 | $750,225.00 | $750,225.00 | $5,683,095.40 |
| Cumulative Cost | | $1,181,745.40 | $1,931,970.40 | $2,682,195.40 | $3,432,420.40 | $4,182,645.40 | $4,932,870.40 | $5,683,095.40 | |
| Project Annual Savings | | $(202,830.40) | $228,690.00 | $228,690.00 | $228,690.00 | $228,690.00 | $228,690.00 | $228,690.00 | $1,169,309.60 |

The table above shows the annual and cumulative costs (including implementation in Year 1) for the Current Solution and the proposed solution, using the prices shown on the previous page, with all options chosen (including facial recognition). Annual and total savings are shown in the bottom row. This represents the most likely annual cost projections, as it represents the options currently preferred by the State.

**Table 14 - Impact Analysis, No Options**

| NO OPTIONS: | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **CURRENT** | **Implementation** | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7 | **Total** |
| Annual Total Cost | $- | $978,915.00 | $978,915.00 | $978,915.00 | $978,915.00 | $978,915.00 | $978,915.00 | $978,915.00 | $6,852,405.00 |
| Cumulative Cost | | $978,915.00 | $1,957,830.00 | $2,936,745.00 | $3,915,660.00 | $4,894,575.00 | $5,873,490.00 | $6,852,405.00 | |
| **VALID SOLUTION** | **Implementation** | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7 | **Total** |
| Estimated Annual Cost | $431,520.40 | $673,995.00 | $673,995.00 | $673,995.00 | $673,995.00 | $673,995.00 | $673,995.00 | $673,995.00 | $5,149,485.40 |
| Cumulative Cost | | $1,105,515.40 | $1,779,510.40 | $2,453,505.40 | $3,127,500.40 | $3,801,495.40 | $4,475,490.40 | $5,149,485.40 | |
| | | | | | | | | | |
| Project Annual Savings | | $(126,600.40) | $304,920.00 | $304,920.00 | $304,920.00 | $304,920.00 | $304,920.00 | $304,920.00 | $1,702,919.60 |

The table above shows the annual and cumulative costs (including implementation in Year 1) for the Current Solution and the proposed solution, using the prices shown on the previous page, with all options declined (but including facial recognition as part of the basic package). Annual and total savings are shown in the bottom row. This represents the lowest possible cost for the project but does not represent likely option choices by the State. It is shown here for comparison.

## 9.3 NARRATIVE SUMMARY OF THE ANALYSIS CONDUCTED AND ASSUMPTIONS.

### ANALYSIS

**We first note that continuing the existing solution does not appear to be an option for the State, due to end-of-life equipment and software, and an expired contract for the primary service. Therefore, the analysis which follows is present especially to understand the *impact* of project cost on State finances, and not to indicate whether the project should proceed on financial grounds.**

The table in 9.2 Pricing Components, above, lists the pricing offered by the vendor for the issued (Polycarbonate) cards and the various options requested by the State. We have used the options the State currently indicates as chosen, along with the State's estimate of the number of cards issued annually and the breakdown of that total between DL and EDL cards. This total price gives us the Estimated Annual Cost in the first Operating Cost Impact table. We add to this the Implementation Costs from Section 5, above ((S431,520.40).

We used the same source table but with no options chosen, along with the State's estimate of the number of cards issued annually and the breakdown of that total between DL and EDL cards, to derive an Estimated Annual Cost for the second Operating Cost Impact table. We add to this the Implementation Costs from Section 5, above ((S431,520.40).

To represent current annual costs, we used the per-card-issued all-inclusive price currently paid by the State under extended contract with Idemia. These costs are:

- Idemia contract (current) cost for DL/ID card: $3.91
- Idemia contract (current) cost for Extended DL card: $8.92

The Idemia figures are used as multipliers to the same estimated number of cards and DL/EDL breakdown as used in the proposed project.

Both tables show cumulative cost comparison between current and proposed projects, to show potential savings/loss/break-even.

- The first table (all options) shows a slight increase the first year of the project, due entirely to the initial implementation costs. Breakeven occurs at the ***end*** of the second year of the project, as annual savings catch up with initial implementation costs. **We support this version of the project, as it presents the State with significant improvements in customer service and usability**.
- The second table (no options chosen, still includes facial recognition) shows more savings over the lifecycle, due to a higher annual savings (approx. 12% per year, not counting implementation). In this scenario, there is a breakeven point at the ***beginning*** of the second year of the project, again since project annual savings are greater. **Although this version of the**

**project is slightly less expensive, it comes at the expense of reduced usability and customer service**.

Section 9.4, below, shows these conclusions in graphical form

### ASSUMPTIONS:

- That 210,000 cards per year represents a reasonable estimate of cards issued annually
- That 85% DL and 15% EDL represents a reasonable estimate of the ratio of card types issued annually
- That the project lifecycle totals 7 years (5 years initial contract, 2 years renewal)
- That the estimated current annual cost is reasonably accurate
- That the estimated current annual cost would continue going forward 7 years (*Note: as explained above, this assumption is necessary for this cost impact exercise, but probably unrealizable*)

## 9.4 WHAT IS THE BREAK-EVEN POINT FOR THIS IT ACTIVITY (CONSIDERING IMPLEMENTATION AND ON-GOING OPERATING COSTS)?

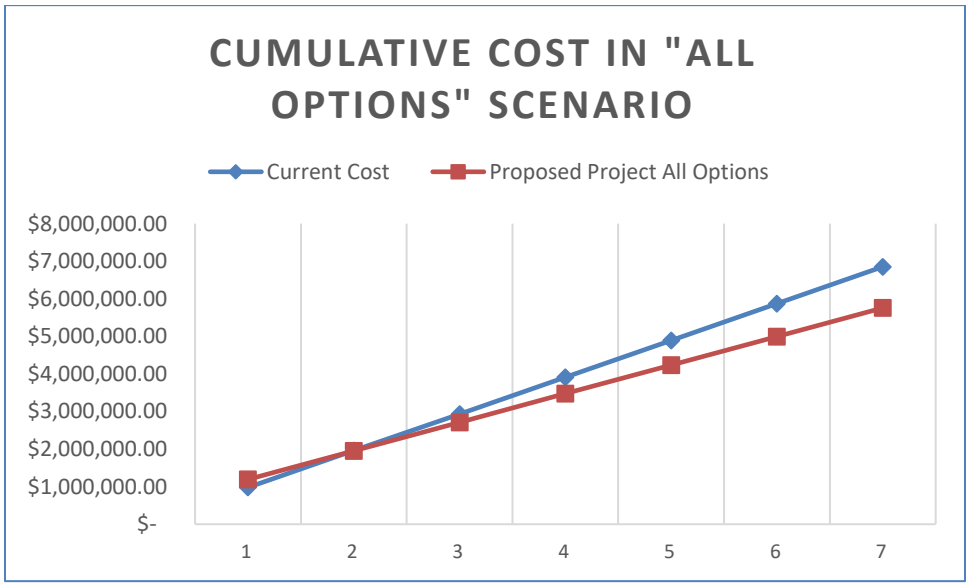



**Figure 4 - Breakeven - All Options**

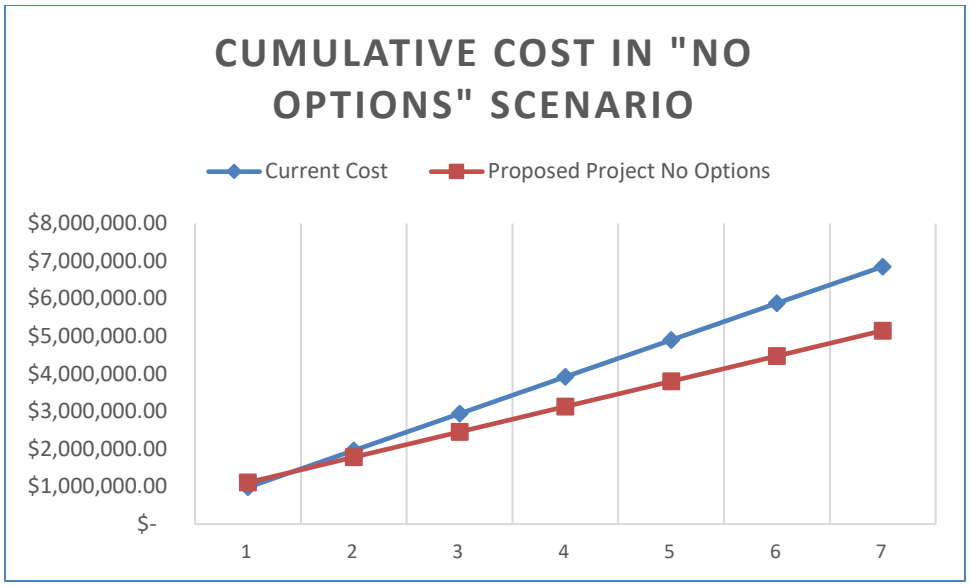



**Figure 5 - Breakeven, No Options**

## 9.5 EXPLAIN ANY NET OPERATING INCREASES THAT WILL BE COVERED BY FEDERAL FUNDING. WILL THIS FUNDING COVER THE ENTIRE LIFECYCLE? IF NOT, PLEASE PROVIDE THE BREAKOUTS BY YEAR.

No federal funds apply to this project.

# 10. RISK ASSESSMENT & RISK REGISTER

## 10.1 RISK REGISTER LEGEND

NOTES: There are gaps in the sequence of Risk ID numbers, because some identified risks were mitigated or obviated during the Independent Review. The original Risk IDs of the remaining risks were retained to prevent confusion over existing communications.

**Table 15 - Risk Register Legend**

| | |
|---|---|
| Risk ID: | Identification number assigned to risk or issue. |
| Risk Rating: | An assessment of risk significance, based on multiplication of **(probability X impact ratings)** (*see below*).<br>**1-30 = low**<br>**31-60 = moderate**<br>**61 – 90 = high** |
| Probability: | Assessment of likelihood of risk occurring, scale of **1 – 9**, from least to most likely |
| Impact: | Assessment of severity of negative effect, scale of **1 – 10**, from least to most severe |
| Finding: | Review finding which led to identifying a risk |
| Risk Of: | Nature of the risk |
| Risk To: | What may be impacted, should the risk occur |
| Reviewer's recommendation | Decision to *avoid*, *mitigate*, or *accept* risk<br>Detailed description of response to risk, in order to accomplish decision |
| State's response | State's planned action in light of recommendation |
| Reviewer's Assessment: | Reviewers evaluation of the State's planned response |

| | | |
|---|---|---|
| Risk ID: R1 | Rating:<br>Probability:<br>Impact: | **21**<br>**3**<br>**7** |
| Finding: | Solution when fully implemented contains redundant, potentially sensitive data in two separate databases (in vendor cloud and in SOV mainframe) which are not explicitly synchronized and error-checked. This may lead to errors of inconsistent data. | |
| Risk Of: | Data error | |
| Risk To: | reliability, accuracy, increased cost due to remediation efforts | |
| Reviewer's recommendation | MITIGATE:<br><br>-Pursue development of plan to consolidate<br>-If funding is available, consider requesting deliverable for vendor planning potential migration process to single cloud-based database. | |
| State's response | We realize the risk but disagree with the severity. We feel probability is 3. The DMV will work with ADS to put procedures in place to minimize risk of ensure data is synchronized. | |

| | | |
|---|---|---|
| Risk ID: R2 | Rating:<br>Probability:<br>Impact: | 63<br>7<br>9 |
| Finding: | DMV lacks a data governance process | |
| Risk Of: | Data error, loss, or mis-use; unforeseeable downstream consequences | |
| Risk To: | reliability, accuracy, project success, proper use by external agents | |
| Reviewer's recommendation | MITIGATE:<br><br>-Seek data governance guidance from ADS<br>- Initiate data governance process at Agency level.<br>- Implement reasonable data quality effort at Department level. | |
| State's response | We agree and intend to follow the reviewers recommendation and seek data governance guidance from ADS. We feel the impact is lower and should be in the 5 - 7 range. | |

| | | |
|---|---|---|
| | Rating: | 42 |
| Risk ID: R3 | Probability: | 6 |
| | Impact: | 7 |
| Finding: | Vendor's proposal contains appropriate assertions of security/privacy controls but does not offer verification process for State | |
| Risk Of: | Security/privacy breach | |
| Risk To: | Citizens' privacy, State reputation | |
| Reviewer's recommendation | MITIGATE:<br><br>-Negotiate regular attestation sharing process to be memorialized in contract<br>-open shared POA&M can be container for security artifacts such as attestations. (See narrative for possible schedule);<br>CISO reviews provided attestations, documents findings | |
| State's response | We agree and will work with the EA and CISO office to ensure it is built into the contract. | |

| | | |
|---|---|---|
| | Rating: | 40 |
| Risk ID: R5 | Probability: | 5 |
| | Impact: | 8 |
| Finding: | Vendor's proposal does not propose specific terms for early termination or contract extension | |
| Risk Of: | increased cost, dependency on vendor | |
| Risk To: | project success, customer service | |
| Reviewer's recommendation | MITIGATE:<br><br>negotiate and clarify contract terms | |
| State's response | We agree with the risk and will negotiate and clarify contract terms. If the SOV decides at such time to enter in the optional contract extensions we will negotiate a cap agreement on costs. | |

| | | |
|---|---|---|
| | Rating: | 54 |
| Risk ID: R8 | Probability: | 6 |
| | Impact: | 9 |
| Finding: | Vendor did not describe POA&M management process in proposal as requested, but instead suggested POA&M was not required because no remediation was currently needed. SOV requires participation by vendor in POA&M process. | |
| Risk Of: | Inadequate problem remediation process; non-compliance with SOV EA requirement. | |
| Risk To: | Security; privacy; reliability; efficient process; | |
| Reviewer's recommendation | MITIGATE:<br><br>Require SOV-compliant POA&M process in contract negotiations. (Also see Risk R3 above for POA&M as security artifiact container) | |
| State's response | We will follow CISO guidance. | |

| | | |
|---|---|---|
| | Rating: | 20 |
| Risk ID: R10 | Probability: | 4 |
| | Impact: | 5 |
| Finding: | Not clear what the "roadmap" will be for eventual development of online portals, how they will integrate with existing SOV/AOT/DMV sites, etc. | |
| Risk Of: | decreased useability, incompatibility with existing SOV portals, increased maintenance cost | |
| Risk To: | Efficiency, useability | |
| Reviewer's recommendation | MITIGATE:<br><br>Include the assigned Enterprise Architect in any design or planning sessions that may arise in advance of online portal implementation. | |
| State's response | This is part of the implementation plan. | |

| | | |
|---|---|---|
| | Rating: | 40 |
| Risk ID: R11 | Probability: | 4 |
| | Impact: | 10 |
| Finding: | If any facial recognition data not intended to be used at this time exists as historical data in the SOR, importing that data into the new cloud database could unintentionally imply use of that data, or at least create the appearance of use. | |
| Risk Of: | Improper data use, privacy violation | |
| Risk To: | State/DMV reputation, citizens' privacy, liability | |
| Reviewer's recommendation | MITIGATE:<br><br>Negotiate vendor-SOV cooperative oversight of data migration/import with careful attention to any data associated with facial recognition technology, pending clarification from legislature, and in consultation with the Attorney General's office where appropriate. | |
| State's response | The DMV acknowledges regardless of their end use that photos will need to be migrated. The photo by itself is not FR data.<br><br>The DMV will work with the Attorney Generals office to mitigate any concerns regarding business decisions they are making around FR.. | |

## 11. ATTACHMENTS

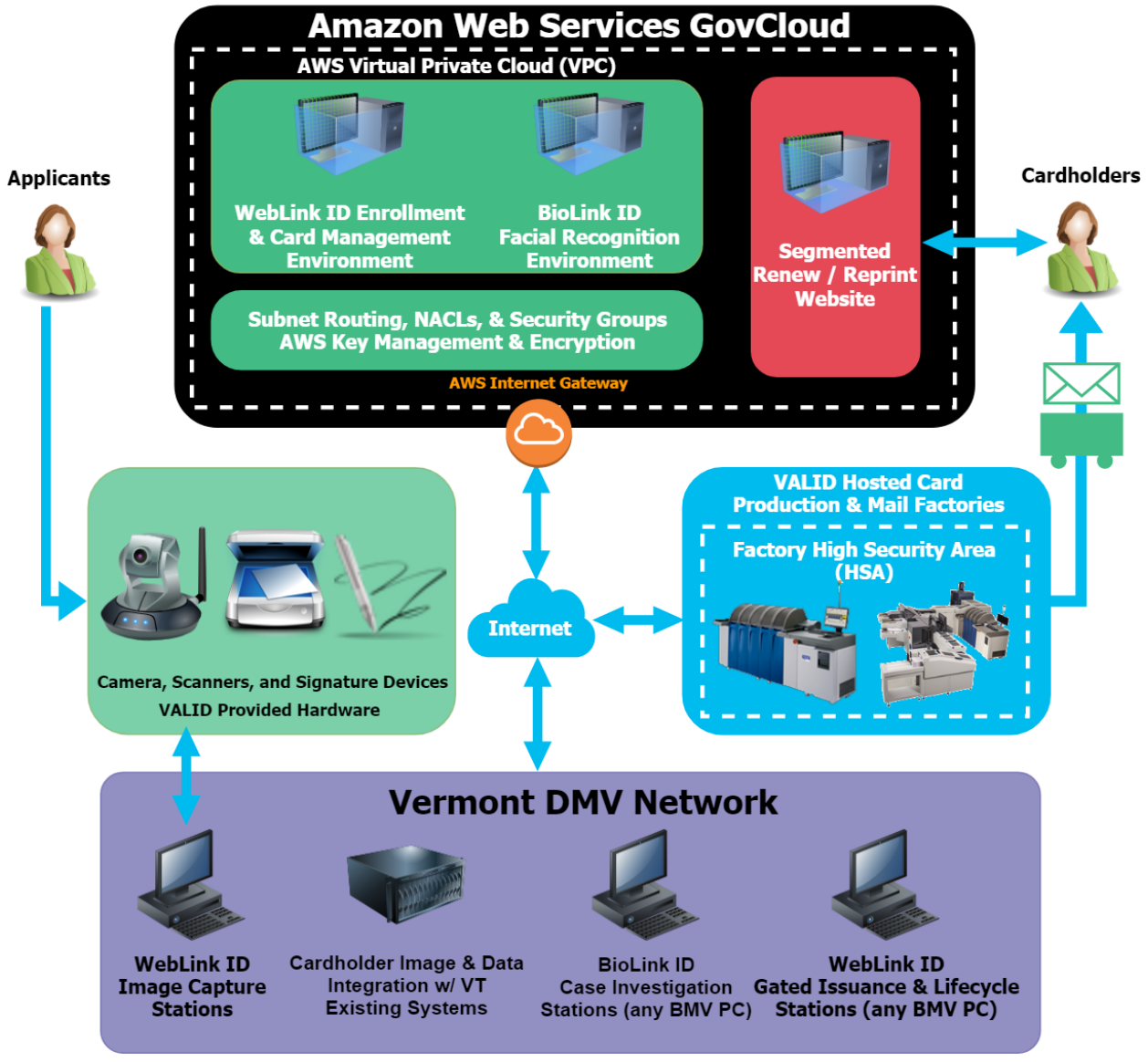
**Attachment 1 – Illustration of System Integration**

**Attachment 2 – Risk & Issues Register Summary**

**Attachment 3 – Lifecycle Cost Benefit Analysis**

**Attachment 4 – Cost Impact Analysis**

## ATTACHMENT 1 – ILLUSTRATION OF SYSTEM INTEGRATION



## ATTACHMENT 2 – RISK & ISSUES REGISTER SUMMARY

## ATTACHMENT 2 - AOT DL/ID INDEPENDENT REVIEW -- Risk and Issues Register -- version 3.1.a -- 2018-May-01 -- Paul E. Garstki, JD -- Paul Garstki Consulting

**RISKS**

**What is the finding that leads to identifying a risk? (This is a highly condensed version that is explained more fully in the report narrative)**

**What exactly are the risks implied by the finding?**

**What aspects of the project are at risk if the risk(s) are realized?**

**What is the Independent Reviewer recommending?**

**What is the State's response to the recommendation(s) (e.g., agree, or alternative risk response.)**

**1-30 = low**
**31-60 = moderate**
**60-90 high**

| Risk # | Finding | risk of | risk to | Reviewer Recommendation | SOV response | probability 1-9 | impact 1-10 | total rating |
|---|---|---|---|---|---|---|---|---|
| **R1** | Solution when fully implemented contains redundant, potentially sensitive data in two separate databases (in vendor cloud and in SOV mainframe) which are not explicitly synchronized and error-checked. This may lead to errors of inconsistent data. | Data error | reliability, accuracy, increased cost due to remediation efforts | MITIGATE:<br><br>-Pursue development of plan to consolidate<br>-If funding is available, consider requesting deliverable for vendor planning potential migration process to single cloud-based database. | We realize the risk but disagree with the severity. We feel probability is 3. The DMV will work with ADS to put procedures in place to minimize risk of ensure data is synchronized. | **3** | **7** | **21** |
| **R2** | DMV lacks a data governance process | Data error, loss, or mis-use; unforeseeable downstream consequences | reliability, accuracy, project success, proper use by external agents | MITIGATE:<br><br>-Seek data governance guidance from ADS<br>- Initiate data governance process at Agency level.<br>- Implement reasonable data quality effort at Department level. | We agree and intend to follow the reviewers recommendation and seek data governance guidance from ADS. We feel the impact is lower and should be in the 5 - 7 range. | **7** | **9** | **63** |
| **R3** | Vendor's proposal contains appropriate assertions of security/privacy controls but does not offer verification process for State | Security/privacy breach | Citizens' privacy, State reputation | MITIGATE:<br><br>-Negotiate regular attestation sharing process to be memorialized in contract<br>-open shared POA&M can be container for security artifacts such as attestations. (See narrative for possible schedule); CISO reviews provided attestations, documents findings | We agree and will work with the EA and CISO office to ensure it is built into the contract. | **6** | **7** | **42** |
| **R5** | Vendor's proposal does not propose specific terms for early termination or contract extension | increased cost, dependency on vendor | project success, customer service | MITIGATE:<br><br>negotiate and clarify contract terms | We agree with the risk and will negotiate and clarify contract terms. If the SOV decides at such time to enter in the optional contract extensions we will negotiate a cap agreement on costs. | **5** | **8** | **40** |
| **R8** | Vendor did not describe POA&M management process in proposal as requested, but instead suggested POA&M was not required because no remediation was currently needed. SOV requires participation by vendor in POA&M process. | Inadequate problem remediation process; non-compliance with SOV EA requirement. | Security; privacy; reliability; efficient process; | MITIGATE:<br><br>Require SOV-compliant POA&M process in contract negotiations. (Also see Risk R3 above for POA&M as security artifact container) | We will follow CISO guidance. | **6** | **9** | **54** |
| **R10** | Not clear what the "roadmap" will be for eventual development of online portals, how they will integrate with existing SOV/AOT/DMV sites, etc. | decreased useability, incompatibility with existing SOV portals, increased maintenance cost | Efficiency, useability | MITIGATE:<br><br>Include the assigned Enterprise Architect in any design or planning sessions that may arise in advance of online portal implementation. | This is part of the implementation plan. | **4** | **5** | **20** |
| **R11** | If any facial recognition data not intended to be used at this time exists as historical data in the SOR, importing that data into the new cloud database could unintentionally imply use of that data, or at least create the appearance of use. | Improper data use, privacy violation | State/DMV reputation, citizens' privacy, liability | MITIGATE:<br><br>Negotiate vendor-SOV cooperative oversight of data migration/import with careful attention to any data associated with facial recognition technology, pending clarification from legislature, and in consultation with the Attorney General's office where appropriate. | The DMV acknowledges regardless of their end use that photos will need to be migrated. The photo by itself is not FR data.<br><br>The DMV will work with the Attorney Generals office to mitigate any concerns regarding business decisions they are making around FR.. | **4** | **10** | **40** |
| **R12** | | | | | | **0** | **0** | **0** |
| **R13** | | --- | --- | --- | --- | **0** | **0** | **0** |

**ISSUES**

none at this time

## ATTACHMENT 3 – COST SPREADSHEET

| Attachment 3: AOT DL/ID Cost Spreadsheet -- ver. 2.0 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Description** | **Qty** | **Unit Price** | **Initial Implementation** | **Maintenance** | **Maintenance** | **Maintenance** | **Maintenance** | **Maintenance** | **Maintenance** | **Maintenance** | **Total** |
| **Fiscal Year** | | | **Year 1** | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Year 5** | **Year 6** | **Year 7** | |
| **Hardware** | | | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - |
| Other | | | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - |
| **Hardware Total** | | | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - | **$ -** |
| **Software** | | | | | | | | | | | |
| Other | | | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - |
| **Software Total** | | | $ - | $ - | $ - | $ - | | | $ - | $ - | **$ -** |
| **Consulting** | | | | | | | | | | | |
| Other | | | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - |
| Independent Review | | | $ 25,000.00 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 25,000.00 |
| **Consulting Total** | | | $ 25,000.00 | $ - | $ - | $ - | | | $ - | $ - | **$ 25,000.00** |
| **Training** | | | | | | | | | | | |
| Trainer | | | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - |
| Other | | | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ - |
| **Training Total** | | | $ - | $ - | $ - | $ - | | | $ - | $ - | **$ -** |
| **Other** | | | | | | | | | | | |
| Solution Cost on Per-Card Basis | | | | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 5,325,075.00 |
| Est. 3% EA Charge to ADS (Internal) | | | $ 11,840.40 | | | | | | | | |
| **Other Total** | | | $ 11,840.40 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | $ 760,725.00 | **$ 5,336,915.40** |
| **Personnel Additional** | | | | | | | | | | | |
| Subject Matter Expert 1 | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Subject Matter Expert 2 | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Subject Matter Expert 3 | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Subject Matter Expert 4 | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Subject Matter Expert 5 | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Subject Matter Expert 6 | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Subject Matter Expert 7 | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Subject Matter Expert 8 | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Business Lead | | | $40,040 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 40,040.00 |
| Project Manager | | | $85,800 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 85,800.00 |
| IT Manager | | | $28,600 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 28,600.00 |
| Oversight Project Manager | | | $11,440 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | $ 11,440.00 |
| **Personnel Additional Total** | | $ | 394,680.00 | $ - | $ - | $ - | $ - | $ - | $ - | $ - | **$ 394,680.00** |
| | | | | | | | | | | | |
| **Totals:** | | **$** | **431,520.40** | **$ 760,725.00** | **$ 760,725.00** | **$ 760,725.00** | **$ 760,725.00** | **$ 760,725.00** | **$ 760,725.00** | **$ 760,725.00** | **$ 5,756,595.40** |
| | | | | | | | | | | **LIFECYCLE TOTAL** | **$ 5,756,595.40** |