VALID

THE SECURE SIDE OF INNOVATION

Response:

Request for Proposal:

Vermont Department of Motor Vehicles - Driver's License/ID System

VERMONT

This response represents Valid USA, Inc.'s proposed solution for Vermont Department of Motor Vehicles - Driver's License/ID System Request for Proposal.

January 12, 2017

Table of Contents/Table of Figures

This section contains the Table of Contents and Figures for this RFP.

Table of Contents

Table of Contents.....ii

Table of Figures vi

Glossary and Definition..... x

Preamble xiii

Cover Letter..... 1

Forms 5

Part 1: Bidder Profile 13

Part 2: Bidder Proposal Solution 27

Part 3: Functional Requirements..... 71

Part 4: Non-Functional Requirements 99

Part 5: VALID's Implementation/Project Management Approach..... 193

Part 6: Technical Services..... 205

Part 7: Maintenance and Support Services..... 225

Part 8: Pricing 248

Part 9: Terms and Conditions 250

Part 10: Authorized Company Signature 252

Attachments..... 254

Table of Figures

Figure 1: VALID's History 15
Figure 2: Sample Workflow 65
Figure 3: Advanced Search Parameters 73
Figure 4: Manual Gate Flag Creation 74
Figure 5: Buckets 75
Figure 6: VALID without Signature and Photo Options 76
Figure 7: WebLink ID Reports Module 78
Figure 8: Example of Canned Report Interface 79
Figure 9: BioLink ID Report Configuration 80
Figure 10: Ad-hoc Reporting User Interface 81
Figure 11: Query Editor 82
Figure 12: List of Roles in WebLink ID 85
Figure 13: Permissions Given to a WebLink ID Role 86
Figure 14: Sample Project Dashboard Displaying Transactional Data 87
Figure 15: Sample Project Dashboard Displaying Overview and Reconciliation of Facial Recognition Activity 87
Figure 16: Sample Project Dashboard Displaying Transactional Data and Trends 88
Figure 17: Sample Project Dashboard Displaying Reconciliation of Application Errors 88
Figure 18: Toolbar to Add or Modify Dashboards 89
Figure 19: Temporary Document Without Photo 90
Figure 20: Temporary Document with Photo 91
Figure 21: Unacceptable Photo Capture 93
Figure 22: Camera Tower 94
Figure 23: Bucket View 95
Figure 24: Card Management - Card Life Cycle 97
Figure 25: Network Diagram 133
Figure 26: UV-A Dull Substrate Material 136
Figure 27: Card Core Inclusions 137
Figure 28: Serialized Card Blanks 137
Figure 29: Composite Card with DOB Embossed over Portrait 138
Figure 31: CMYK Colors 139

Figure 30: Spot Colors 139
Figure 32: Microprinted Text 139
Figure 33: Duplex Security Pattern 140
Figure 34: Deliberate Error 140
Figure 35: UV Fluorescent Ink 141
Figure 38: OVI Showing as Green 142
Figure 36: Polycarbonate Card with Optically Variable Ink 142
Figure 37: OVI Showing as Gold 142
Figure 39: IR-Fluorescent Ink 142
Figure 40: Color Portrait 143
Figure 41: Composite Card with Variable UV Data 144
Figure 42: Embedded Data in Portrait 146
Figure 43: Embossed Polycarbonate Card also containing Tactile Laser Engraving 147
Figure 44: Indent Printed Composite Card 147
Figure 45: Secure Indent Print, Magnified View 147
Figure 46: WebLink ID screenshot displaying 1:1 Image success from BioLink ID. 153
Figure 47: mID/DL 154
Figure 48: Error Message 155
Figure 49: Save Message 155
Figure 50: WebLink ID Navigation Panel 156
Figure 51: Special Mailing Address Entry 157
Figure 52: Failed ICAO Quality Check Override 158
Figure 53: Facial Recognition 1:1 Override 159
Figure 54: 'Tab Stop' Order 160
Figure 55: Field Validation Regex 161
Figure 56: Invalid Entry Notification 162
Figure 57: Missing Field Notification 163
Figure 58: Required Field Flag 164
Figure 59: Search Log 167
Figure 60: Network Outage Process and Back-up 171
Figure 61: System Monitoring 178
Figure 62: Access Logs 179

Figure 63: Iteration Cycle in Agile Project **208**
Figure 64: PDF Proof **209**
Figure 65: Overview of VALID's Data Migration Process **217**
Figure 66: Routine Escalation Process **227**
Figure 67: Urgent Escalation Process **227**
Figure 68: Urgent Escalations **228**
Figure 69: Government ID/DL Personalization **242**
Figure 70: Sample Monthly SLA Achievement Report **324**

Glossary and Definition

- **AAMVA** – American Association of Motor Vehicle Administrators
- **ACD** – Automated Call Distribution – manages a Help Desk call volume and maintains statistics on the calls.
- **ADF** – Automatic Document Feeder.
- **Ad hoc** – Latin, which translates to "as the occasion requires"
- **Ad hoc investigation** – An investigation added to the system by a user (rather than opened from WebLink ID).
- **Ad hoc reporting** – enables end users to rapidly generate dynamic, tailored reports that meet their information requirements.
- **AES** – Advanced Encryption Standard is a symmetric encryption algorithm.
- **AWS –** Amazon Web Services
- **API –** Application Programming Interface – a set of subroutine definitions, protocols, and tools for building application software and integrating to other software platforms.
- **BioLink ID** – BioLink ID is VALID's web-based, image capture, case management, and biometric investigation tool.
- **Buckets** - Buckets are containers used to organize flags. The Buckets correspond to different security roles in WebLink ID, ensuring the correct users review information related to the flags that fall within their area of expertise or responsibility.
- **Case** – A case is open when an issuance image from WebLink ID is being investigated. All cases are investigations, but not all investigations are cases.
- **CDLIS** – Commercial Driver's License Information System
- **CDS** – Card Design Standard or Card Design Specification.
- **CIF** – Customer Image File.
- **CIS** – Central Issuance System.
- **CISO** – Certified Information Security Officer
- **CMYK colors** -- Commercial printing presses print with cyan, magenta, yellow and black (CMYK) ink.
- **CPF** – Card Personalization Facility.
- **CPS** – Credential Production System.
- **Database Synchronization –** The process of establishing and maintaining data consistency and uniformity between two or more databases where harmonization of the data is performed continuously.
- **DCM** – Data Conversion and Migration.

- **DL/ID** – Driver's License / Identification card.
- **DPI** – Dots per inch
- **DPV** – Delivery Point Verification
- **DR/BC** – Disaster Recovery / Business Continuity.
- **EDL** – Enhanced driver's license.
- **EID** – Enhanced identification.
- **Enrollment transaction** – Process of enrolling (entering) a subject in BioLink ID.
- **EOL** – End of Life
- **Factory Allocation Manager (FAM)** – A physical and logical component that accumulates print requests continuously until, at a scheduled time, all accumulated requests are assembled and separated into sub-jobs by configurable business rules; whereupon the sub-jobs are distributed to one or more CPFs.
- **Finger Print (FP) Recognition** – A biometric modality that uses the physical structure of an individual's fingerprint for recognition purposes.
- **FR** – Facial Recognition – A biometric modality that uses an image of the physical structure of an individual's face for recognition purposes.
- **Gate** – Checkpoints in the card issuance workflow that stop a card from being processed. Each gate processes different types of flags.
- **Gate Flag** (Flag) – Each gate flag in a sequence must be resolved before the card can move to the next gate. When a card application has successfully passed through all of the gates, it is automatically sent for production, and the card is mailed to the customer. All gate flags must be reviewed and resolved in order to issue the card.
- **Grayscale** – An image composed exclusively of shades of gray, in which the value of each pixel is a single sample, representing the amount of light it carries - also known as black-and-white or monochrome.
- **HSA** – Hight Security Area
- **HSM** – Hardware Service Module
- **ICAO** – International Civil Aviation Organization standard check for photos, which is the standard applied to passport photos. This check examines the photo for facial characteristics and irregularities such as smiles, eyes, brightness, blur, and cropping.
- **ICW** – Image Capture Workstation or Workflow, depending on context.
- **IIS** – Internet Information Services
- **IPM** – impressions per min (for printers)
- **JCS** – Job Control System. This is the nerve center of the personalization facilities which creates release sheets, machine control files, consumes audit files, and hosts the card test procedures.

- **JIRA** – Developed by Atlassian, this is software tracking tool for system defects and issues used for project management.
- **KPI** – Key Performance Indicators
- **NCOA** – National Change of Address
- **One-to-Many Biometric Matching** – Also seen as 1:n or 1:N. Checks photo against all photos in the database.
- **One-to-one Biometric Matching** – Also seen as 1:1 biometric testing or facial recognition testing - this check through BioLink ID ensures the new photo matches the most recent passing photo for the customer and checks photos only against photos of that individual in the database.
- **O&M** – Operations and Maintenance – The phase immediately following the project completion.
- **PCAD** – Production Card Approval Document contains actual card sample of each card type; they serve as baseline references for future produced cards.
- **PCI** – Payment Card Industry.
- **PCI SSC** – Payment Card Industry's Security Standards Council
- **PDPS** – Problem Driver Pointer System
- **PIER** – Post Implementation and Evaluation Review.
- **Pixel** – The term was invented from "picture element", and it is the basic unit of programmable color on a computer display or in a computer image. The physical size of a **pixel** depends on how you have set the resolution for the display screen.
- **PMI** – Project Management Institute
- **PMP** – Project Management Plan.
- **QA** – Quality Assurance – The set of processes used to measure and assure the quality of a solution.
- **QC** – Quality Control – The process of ensuring that products and services meet customer expectations via testing, checking and reviews.
- **RAID** – Redundant Array of Independent Disks– is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both.
- **S2S** – State-to-State
- **SDD** – Solution Design Document.
- **SLA** – Service Level Agreement.
- **SOC** – Service Organization Control.
- **SOW** – Statement of Work.

- **SQL** – Structured Query Language.
- **SSAS** – Microsoft's SQL Server Analysis Services is a tool that mines data for reporting purposes.
- **SSOLV** – Social Security Onliine Verification
- **Transaction** – Any action executed in BioLink ID that is tracked and recorded (e.g. enrollment, 1:1 matching, 1:N matching, etc.), making it possible for administrators to view a list of transactions.
- **UAT** – User Acceptance Test.
- **UI** – User Interface.
- **WBS** – Work Breakdown Structure.
- **WebLink ID** – A web-based enrollment and workflow solution that deploys on premise to customer-hosted data centers or hosted at a VALID data center.
- **White List** – A register of individuals who are eligible for a particular service or privilege such as VIPs or undercover law enforcement eligible to bypass facial recognition when applying for a Driver's License.
- **Widget –** a reusable, modular, simple-to-use component of a software applications that simplifies configuration of a predefined function

Preamble

VALID has strived to exactly follow the instructions established in the RFP, Section 3, Bid Preparation. We have tried to present the question / item statement from the DMV's RFP, and then respond, using color as distinctive separator as to which was the query and which was the response. We did take two liberties: we created Attachment 9 to showcase our Card Feature Sheets, and we used Attachment 10 to provide the DMV with the requested Knowledge Transfer and Training Plan.

Cover Letter

Valid USA, Inc. (VALID) is pleased to respond to the Vermont DMV regarding its RFP for ID/DL System Replacement. We carefully examined the RFP objectives, scope of solution required, and desired business outcomes as well as the specific project requirements; and we are confident our proposed solution meets or exceeds DMVs requirements for performance, security, quality, and delivery schedule. The following are the highlights of our proposal.

We will provide the DMV a comprehensive, secure software solution configured to match your preferred workflow process and gated issuance sequence as outlined in this detailed response. Our front-end software applications for enrolment and vetting applicants and back-end applications for managing and reporting credential lifecycle will seamlessly integrate with the DMV's internal systems to enable up-to-date and accurate operational visibility and status reporting. Data services and reporting offered will include: real-time status updates and dashboards, comprehensive logging reports, printed card images, and other card processing information as required.

We recognize how critically important it is for public-facing organizations, such as the DMV, to provide uninterrupted, high quality services to their residents. Therefore, we have developed a unique program to ensure simultaneous dual-facility operations for card production and personalization to support your program. Each of our card personalization facilities has more than enough capacity to support all of the DMV's ID/DL volume at peak demand. We will split the daily ID/DL demand from the DMV between two card personalization sites. In the event of any unplanned interruptions at a given facility, the full DMV production demand will shift to the second facility seamlessly. This program will minimize operational risk for the DMV.

VALID is uniquely positioned to offer the DMV a fully-integrated supply chain of identification card materials, services, and products. We own and operate the vertical stack of hardware, software, and services that includes card stock manufacturing within our secure environments. This provides the DMV unmatched security, flexibility and assurance that all of the DMV's secure card stock and consumable components are always properly controlled.

Our product approach to custom configured ready-made solutions provides the DMV with a flexible and obsolescence-free solution. Because of our product approach, experience with similar programs, and our efficient delivery, we will implement the proposed solution in the short time frame available for this project all while ensuring the solution meets the DMV's exact needs.

Our Qualifications

VALID is an identity and data solution business. VALID, a wholly-owned subsidiary, and its parent company VALID S.A., have successfully issued more than 100 million ID/DL cards and deployed more than 1,400 enrollment workstations across 13 government agencies globally. In the USA, VALID directly owns and operates four card production and personalization facilities staffed by 500+ professionals, and over 505,000 square feet of production space; 261,000 square feet of this space is dedicated to secure card manufacturing and personalization.

VALID S.A. has been performing secure printing since 1957. Valid USA, Inc. has roots dating back to the first government-issued photo ID card by Polaroid ID Systems, assets of which was acquired by ScreenCheck N.A. and eventually by Valid USA, Inc. We manufacture our own secure card stock and personalize cards at US based, company owned and operated central issuance facilities. We also operate our own data centers and failover facilities for disaster recovery and thereby eliminating unplanned interruptions at primary facilities. Our fully-integrated identification card supply chain is unique and offers the DMV tremendous value by reducing risk and providing greater overall security and flexibility.

VALID offers modern, differentiated software and hardware for identity solutions. Our software products include robust, browser-based platforms that span the identity continuum: image capture and data enrollment, biometric analysis, case management, data verification and vetting, card issuance and credential lifecycle management. Additional services include data management and business intelligence.

Our fully-redundant, US-based production facilities are certified by Visa, MasterCard, and Discover, in meeting the security standards set by the Payment Card Industry (PCI) Security Standards Council. VALID manufactures financial cards for many large, US financial institutions and retailers, which leverages experience, value, and security to our government clients and programs. Our experience in payment card market has been a key factor in successful implementation of DL/ID programs in the State of Washington and the US Territory of Guam.

In our US facilities, VALID currently issues approximately one million secure cards per month and can scale capacity as needed to easily produce ten times that amount.

Management Team & Implementation

Our implementation approach is custom configured to seamlessly integrate the DMV's operations and our organizations to reduce risk, and to ensure an on-time high-quality delivery.

Highlights of our implementation strategy include:

- Our Senior Management Team brings Vermont DMV decades of management experience, as well as Identification Card industry experience and lessons learned resulting in a lower risk implementation.
- Our "best practices" project management methodology is repeatable, time tested, and collaborative, ensuring that the solution proposed is delivered on time and with the highest quality.
- We will work collaboratively and transparently with the DMV. Our philosophy is to work together towards the greater goal of the DMV objectives and treat project issues, regardless of where they reside, as common challenges to solve together.
- We have assigned an experienced Project Manager with a deep and skilled project team behind him. This Project Manager will serve as the overall implementation leader and primary point of contact for the DMV. He will work with the DMV to ensure a smooth implementation as well as provide ongoing support after the implementation is complete.

- Our Operations and support teams will be engaged throughout the development and implementation processes to ensure a smooth transition between deployment and service/support phases of the program.
- VALID promises 100% company-wide commitment to the DL/ID System project throughout the entire contract term. We commit to fully staff a dedicated DMV team with US-based resources available to mitigate risks and reduce critical paths as needed.

Our Commitment to the DMV

VALID understands that this system is integral to carrying out the DMV's mission of providing the Citizens of Vermont with the highest level of customer support, security and public safety. The Vermont DL/ID System project will have the highest visibility throughout VALID. We will earn, develop, and maintain a trusted relationship with the DMV while becoming its partner and placing Vermont's interests above all else. The sections within our response demonstrate full understanding and compliance with each DMV requirement; provide further details concerning our proposed solution including implementation and support; and outline the specific benefits to the DMV. We appreciate that budget constraints, increasingly sophisticated security threats, and increased public service demands place stress on government agencies. Our proposal mitigates those factors and offers the DMV the best overall value through cost savings, enhanced security, and the highest quality obsolescence-proof solution.

Sincerely,

Michael Fox
Vice President, Chief Commercial Officer
Valid USA, Inc.

Forms

This section contains the completed forms.

Form A – Certificate of Compliance

Form B – Subcontractor Reporting Form

Exhibit A – Certificate of Compliance

❑ **RFP/PROJECT:**

DATE:
Page 1 of 3

EXHIBIT A

CERTIFICATE OF COMPLIANCE

For a bid to be considered valid, this form must be completed in its entirety, executed by a duly authorized representative of the bidder, and submitted as part of the response to the proposal.

A. **NON COLLUSION:** Bidder hereby certifies that the prices quoted have been arrived at without collusion and that no prior information concerning these prices has been received from or given to a competitive company. If there is sufficient evidence to warrant investigation of the bid/contract process by the Office of the Attorney General, bidder understands that this paragraph might be used as a basis for litigation.

B. **CONTRACT TERMS:** Bidder hereby acknowledges that is has read, understands and agrees to the terms of this RFP, including Attachment C: Standard State Provisions for Contracts and Grants, and any other contract attachments included with this RFP.

C. **FORM OF PAYMENT:** Does Bidder accept the Visa Purchasing Card as a form of payment?

✓ Yes____No

D. **WORKER CLASSIFICATION COMPLIANCE REQUIREMENT:** In accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54), the following provisions and requirements apply to Bidder when the amount of its bid exceeds $250,000.00.

Self-Reporting. Bidder hereby self-reports the following information relating to past violations, convictions, suspensions, and any other information related to past performance relative to coding and classification of workers, that occurred in the previous 12 months.

Summary of Detailed Information	Date of Notification	Outcome

Valid USA, Inc. has no violations, convictions, or suspensions related to past performance relative to coding and classification of workers, that occurred in the previous 12 months.

Subcontractor Reporting. Bidder hereby acknowledges and agrees that if it is a successful bidder, prior to execution of any contract resulting from this RFP, Bidder will provide to the State a list of all proposed subcontractors and subcontractors' subcontractors, together with the identity of those subcontractors' workers compensation insurance providers, and additional required or requested information, as applicable, in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54), and Bidder will provide any update of such list to the State as additional subcontractors are hired. Bidder further acknowledges and agrees that the failure to submit subcontractor reporting in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54) will constitute non-compliance and may result in cancellation of contract and/or restriction from bidding on future state contracts.

Revised: March 2017

RFP/PROJECT:
DATE:

E. Executive Order 05 – 16: Climate Change Considerations in State Procurements Certification

Bidder certifies to the following (Bidder may attach any desired explanation or substantiation. Please also note that Bidder may be asked to provide documentation for any applicable claims):

1. Bidder owns, leases or utilizes, for business purposes, space that has received:
   - ☐ Energy Star® Certification
   - ☐ LEED®, Green Globes®, or Living Buildings Challenge℠ Certification
   - ☐ Other internationally recognized building certification:

_____

2. Bidder has received incentives or rebates from an Energy Efficiency Utility or Energy Efficiency Program in the last five years for energy efficient improvements made at bidder's place of business. Please explain:

_____

3. Please Check all that apply:
   - ☐ Bidder can claim on-site renewable power or anaerobic-digester power ("cow-power"). Or bidder consumes renewable electricity through voluntary purchase or offset, provided no such claimed power can be double-claimed by another party.
   - ☐ Bidder uses renewable biomass or bio-fuel for the purposes of thermal (heat) energy at its place of business.
   - ☑ Bidder's heating system has modern, high-efficiency units (boilers, furnaces, stoves, etc.), having reduced emissions of particulate matter and other air pollutants.
   - ☐ Bidder tracks its energy consumption and harmful greenhouse gas emissions. What tool is used to do this? _____
   - ☑ Bidder promotes the use of plug-in electric vehicles by providing electric vehicle charging, electric fleet vehicles, preferred parking, designated parking, purchase or lease incentives, etc..
   - ☐ Bidder offers employees an option for a fossil fuel divestment retirement account.
   - ☐ Bidder offers products or services that reduce waste, conserve water, or promote energy efficiency and conservation. Please explain:

_____;

_____

4. Please list any additional practices that promote clean energy and take action to address climate change:

The lighting in all Valid USA, Inc. locations is motion-sensored to save energy.

Valid USA, Inc. does not use a sprinkler system for the lawn to conserve water and energy.

Valid USA, Inc. has an active company-wide recycling program to cut down on waste.

Revised: March 2017

F. Acknowledge receipt of the following Addenda:

Updated Bidder Response Form Dated 12/21/2017

Addendum_____ No.: Dated_____

Addendum_____ No.: Dated_____

Addendum_____ No.: Dated_____

Bidder Name: Valid USA, Inc. Contact Name: Michael Fox

Address: 2621 Corrinado Ct. Fax Number: 260-483-4287

Ft. Wayne, IN 46808 Telephone: [redacted]

E-Mail: Michael.Fox@valid.com

By: _____ Name: Michael Fox

Signature of Bidder (or Representative) (Type or Print)

END OF CERTIFICATE OF COMPLIANCE

Revised: March 2017

Exhibit B – Subcontractor Reporting Form

VALID is not using subcontractors for this project.

RFP/PROJECT:
DATE:

EXHIBIT B

SUBCONTRACTOR REPORTING FORM

This form must be completed in its entirety and submitted prior to contract execution and updated as necessary and provided to the State as additional subcontractors are hired.

The Department of Buildings and General Services in accordance with Act 54, Section 32 of the Acts of 2009 and for total project costs exceeding $250,000.00 requires bidders to comply with the following provisions and requirements.

Contractor is required to provide a list of subcontractors on the job along with lists of subcontractor's subcontractors and by whom those subcontractors are insured for workers' compensation purposes. Include additional pages if necessary. This is not a requirement for subcontractor's providing supplies only and no labor to the overall contract or project.

Subcontractor	Insured By		Subcontractor's Sub	Insured By
No Subcontractors				

Date: 12/18/2017

Name of Company:_____ Contact Name: _____

Address:_____ Title: _____

_____ Phone Number: _____

E-mail:_____ Fax Number: _____

By:_____ Name: _____

Failure to adhere to Act 54, Section 32 of the Acts of 2009 and submit Subcontractor Reporting: Worker Classification Compliance Requirement will constitute non-compliance and may result in cancellation of contract and/or forfeiture of future bidding privileges until resolved.

Send Completed Form to: Office of Purchasing & Contracting
109 State Street
Montpelier, VT 05609-3001
Attention: Contract Administration

Revised: March 2017

Part 1: Bidder Profile

1. **Complete the table below.**

Item	Detail
Company Name:	Valid USA, Inc.
Physical Address:	1011 Warrenville Road, Suite 450, Lisle, IL 60532
Postal Address:	1011 Warrenville Road, Suite 450, Lisle, IL 60532
Business Website:	http://www.VALID.com
Type of Entity (Legal Status):	C Corp
Primary Contact:	Michael Fox
Title:	Vice President
Email Address:	Michael.Fox@VALID.com
Phone Number:	Landline: 260-407-1177 x3177 Cell: [redacted]
Fax Number:	260-483-4287

2. **Provide a brief overview of your company including number of years in business, number of employees, nature of business, and description of clients. Identify any parent corporation and/or subsidiaries.**

Company Overview

VALID S.A. began in Brazil in 1957 under the name of Thomas de La Rue, as a subsidiary of an English company specializing in the printing of securities and banknotes. In 2010 the company was restructured and its name was changed to VALID. Having secured its global presence in Brazil, Argentina and Spain, VALID consolidated its presence in the United States by acquiring several identity management, card production, personalization, secure packaging, data analytics and technology companies.

Valid USA, Inc. will be the solution provider for Vermont for this project and is a wholly-owned subsidiary of VALID S.A. Valid USA is incorporated in the State of Delaware, and has been in operation in its current form for over five years (since April 16, 2012). However, as part of the United States growth strategy, Valid USA acquired companies that had a rich history of over 25 years in the production and distribution of Drivers License and Identification Cards, Financial and Gift cards, and Data Management Solutions.

In fact, one of the companies acquired by Valid USA (ScreenCheck North America and prior to that Polaroid Identification Systems) dates to when the first Photo Drivers License was produced in Fort Wayne, Indiana – one of only two companies in the United States that can make this claim. Additionally, through targeted acquisitions Valid USA (hereafter called VALID) now has a data management company which manages hundreds of millions of data records performing in-depth analytics for our customers.

VALID is a global leader in innovative identity management systems. With over 500 US employees, we offer exceptional value through our comprehensive, highly reliable card solutions, U.S.-based identification production facilities and intelligent identification software applications. From driver's licenses to smart cards to transit cards to employee IDs, we provide hundreds of our clients with low-risk, obsolescence-free, secure solutions.

VALID has extensive experience in designing, implementing and supporting identification card solutions, and will use its own software products as part of the overall solution for the state of Vermont. Because of our experience with similar programs and our efficient delivery processes, we can implement a solution in the time frame available for this project. VALID's product approach to customized software applications provides Vermont with a flexible and obsolescence-proof solution.

With VALID, Vermont can rest assured because of our long and rich history of successful implementations for identification card solutions.

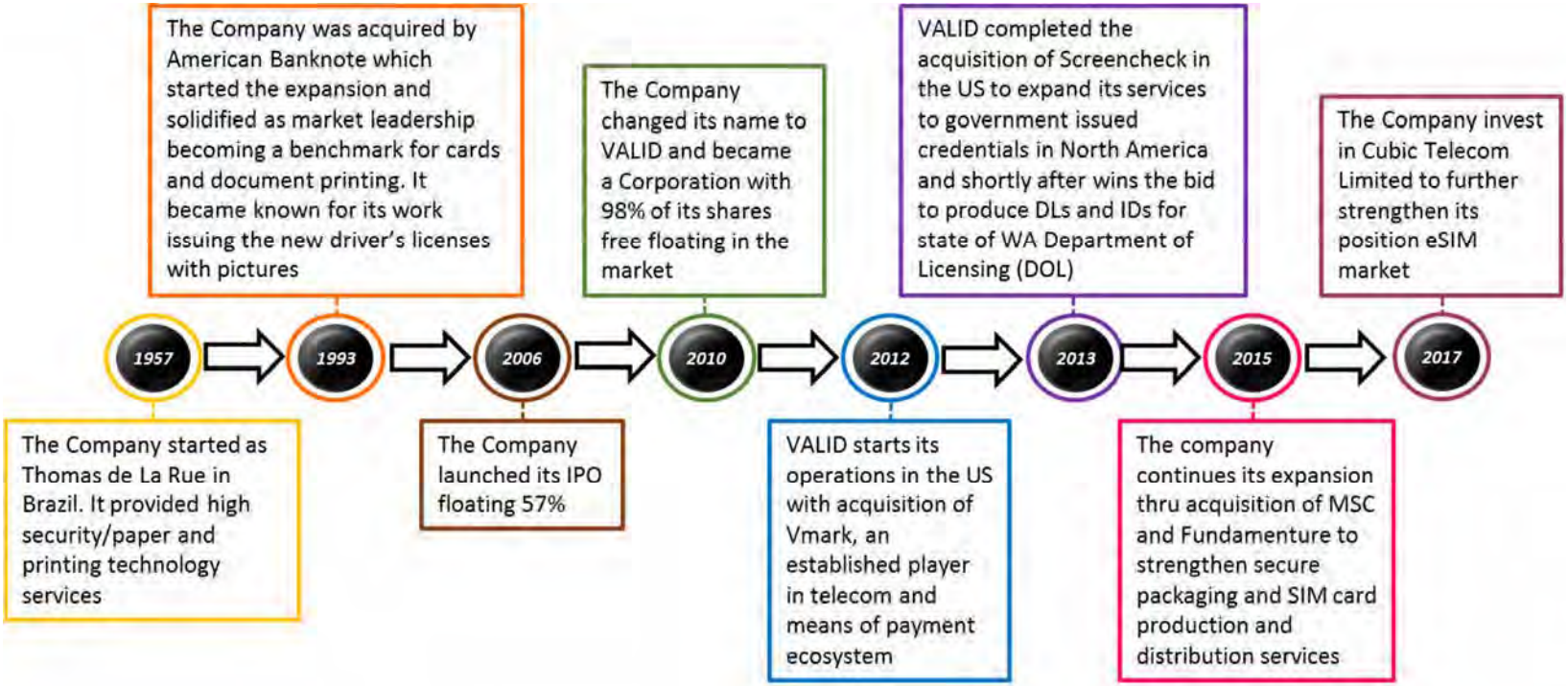


Figure 1: VALID's History. *Over the past 60 years, we have shown our capacity of evolving and offering products and solutions that meet market demand***.**

3. **Provide a Financial Statement* for your company and label it Attachment #1. A confidentiality statement may be included if this financial information is considered non-public information. This requirement can be filled by:**
   - **A current Dun and Bradstreet Report that includes a financial analysis of the firm;**
   - **An Annual Report if it contains (at a minimum) a Compiled Income Statement and Balance Sheet verified by a Certified Public Accounting firm; or**
   - **Tax returns and financial statements including income statements and balance sheets for the most recent 3 years, and any available credit reports.**

Some types of procurements may require bidders to provide additional or specific financial information. Any such additional requirements will be clearly identified and explained within the RFP, and may include supplemental forms in addition to this Bidder Response Form.

4. **Disclose any judgments, pending or expected litigation, or other real potential financial reversals, which might materially affect the viability or stability of your company or indicate below that no such condition is known to exist.**

Valid USA, Inc. has not had any judgments against it, does not have pending or expected litigation, nor has it had any financial reversals. There is nothing known to us which might affect the viability or stability of VALID. Effectively, no such condition exists.

5. **Provide a list of three references similar in size and industry (preferably another governmental entity). References shall be clients who have implemented your Solution within the past 48 months.**

References

Reference 1	Detail
Reference Company Name:	State of Washington, Department of Licensing (DOL)
Company Address:	Department of Licensing, PO Box 9020, Olympia, WA 98507-9020
Type of Industry:	State Government
Contact Name:	[redacted]
Contact Phone Number:	[redacted]
Contact Email Address:	[redacted]
Contact Name:	[redacted]
Contact Phone Number:	[redacted]
Contact Email Address:	[redacted]

Description of system(s) implemented:	***CIS Solution*** **-** The statewide driver's license and ID issuance project for the State of Washington Department of Licensing (WA DOL) produces over 3 million DLs and IDs annually. VALID implemented a Central Issuance System (CIS) solution, which enables the efficient capture of customer data, images and signatures, and accurately combines and maintains a record of these items. VALID's software solution was fully integrated with Washington's back office systems, and was deployed at 56 field offices across the state. The solution set includes software and hardware to enroll, verify, create, and manage identity credentials for the state's residents. The project required card design and production, project management, system development, extensive testing, staff training, system deployment, equipment installation, reporting, and ongoing operations and maintenance.
Date of Implementation:	[redacted]
Similarities with the DMV	The following is a list of significant similarities between the WA CIS project and the DMV project. • *Central Issuance* – For Washington, VALID used its highly-secure card production and personalization facilities while strictly adhering to required SLAs, AAMVA guidelines, and ICAO standards. VALID will use a similarly rigorous issuance process for the DMV. • *General Software Solution* – Just as in Washington, VALID expects to use its well-proven software platforms, WebLink ID and BioLink ID (facial recognition), custom configured to the DMV's specific requirements. • *Card Design* – Washington DOL wanted a highly durable license with extensive security features. VALID worked with an array of Washington stakeholders to design a card that met all their needs. It was a comprehensive effort that required multiple iterations, but in the end everyone seems very satisfied with the results. • *Project Management* – VALID successfully managed an on-time rollout of Washington's solution using a combination of PMI standard project oversight, planning and status reporting combined with Agile iterative and adaptive software development. This combination will be used to ensure the success of the DMV's program.

	• *Equipment Refreshment* – VALID used its long experience as a credential issuance hardware provider to efficiently replace existing Washington equipment with new image capture stations, workstations, and printers. VALID will similarly upgrade the DMV equipment to the best available models available today. • *Data Conversion and Migration* – VALID migrated millions of records and photographs from existing databases to its new Washington solution. VALID will follow the same detailed and repeatable process to ensure that the DMV historical data is accurately migrated to the new system. • *Interfaces* – VALID provided customized interfaces including file transfer, web services and direct database connections to accommodate information exchange between VALID provided systems and Washington's specified systems. VALID's software easily accommodates any interface type, and expects to efficiently connect to all of the DMV's required systems. • *Systems Testing* – To ensure the large and complex Washington solution met all requirements, VALID performed a full range of verification activities including functional testing, system integration testing, user acceptance testing, and regression testing. The same rigorous testing will be applied to the DMV solution. • *Reporting* – To fulfil Washington's financial and performance reporting, VALID Provided standard reports, custom reports, and an ad-hoc reporting tool. This combination effectively targets the main reporting need and VALID will use a similar strategy for the DMV. • *Training* – VALID provided direct training for state personnel in operations, administrative, and technical roles, in addition to creating print and web-based training materials. VALID will use its proven set of training curricula and multiple delivery modes (live, print, and web-based) to comprehensively train the DMV personnel. • *Documentation* – Any large scale driver's license program requires detailed and accurate documentation. For Washington, VALID created project planning and control documents, requirements and design documents, ongoing management and status documents in addition to training materials. For the DMV, VALID will follow a similar process. • *Disaster Recovery* – VALID provides Washington 100% hot-site backup and disaster recovery using duplicate, geographically diverse, personalization facilities. VALID will provide the same, worry-free, disaster recovery system to the DMV.

	• *Ongoing Operations and Maintenance* – To support Washington's 50+ locations, VALID stood up a network of local technicians as well as a help desk available by email and phone and subject to a strict SLA. VALID expects to leverage this infrastructure and experience to support the DMV's implementation and offices.

Reference 2	Detail
Reference Company Name:	U.S. Territory of Guam
Company Address:	General Services Agency, Department of Administration, Government of Guam, 148 Route 1, Marine Drive, Piti. Guam, 96925
Type of Industry:	Government
Contact Name:	[redacted]
Contact Phone Number:	[redacted]
Contact Email Address:	[redacted]
Description of system(s) implemented:	**WebLink ID solution** - In 2013, VALID developed for Guam the first version of WebLink ID, the first web-based ID product to be certified by the American Association of Motor Vehicle Administrators [AAMVA] for the three Real ID web portals: VLS, USPASS and SSOLV. VALID's current solution is integrated into Guam's back-end systems and is deployed at both Guam DMV locations. The solution includes procurement and installation of hardware (document scanners, printers, cameras, and signature capture devices) and software to create and manage identity credentials for Guam's residents, as well as ongoing card production, training, reporting, and continued support.
Date of Implementation:	[redacted]
Similarities with the DMV	The following is a list of significant similarities between the Territory of Guam project and the DMV project: • *Issuance* - AAMVA integration, adherence to AAMVA guidelines, ICAO photo validation and biometric security. VALID uses high-security card stock as the basis for Guam's over-the-counter printing solution. All of these technologies would be used to develop a solution for the DMV. • *General Software Solution* – Using WebLink ID for card management and production and BioLink ID for facial recognition and investigation, as well as close integration with the AAMVA portal and REAL ID validation.

	• *Project Management* - Project Management Institute best practices for the REAL ID compliance project, including a dedicated project manager, regularly updated project plan, continuous status reporting and project documentation. • *Equipment Refreshment* - Sourced all equipment, including image capture, workstations, signature capture devices, and printers. The equipment refreshment for the DMV is substantially similar to the hardware solution provided to Guam. • *Data Conversion and Migration* – Migration of all historical data to a new data structure and improved server architecture. All existing photographs will be enrolled into the biometric software and will be subjected to 1:1 and 1:N checks. • *Interfaces* - Developed a complete set of interfaces and access layer to integrate with the AAMVA portals providing Validation of identity, lawful status and social security number. VALID also developed a bi-directional interface to Guam's back-end system. • *Systems Testing* – Each software release is subjected to functional testing, system integration testing, user acceptance testing and regression testing. • *Reporting* – Easily accessible standard and customer-defined reports that can be downloaded in a variety of formats • *Training* - VALID provides in-person and web-based training, also called computer-based training (CBT), as well as training materials, as part of every release. • *Documentation* - VALID has produced a full set of documentation in support of the Guam Project, including software specifications, design documents, wireframes, project charters, projects plans, training materials, user guides, quick reference guides, presentation materials, and E-learning presentations. • *Disaster Recovery* – As part of the REAL ID project, VALID is supervising the creation of Guam's first true backup and failover system using both hardware and software. In addition, VALID assisted Guam's preparation of an emergency response plan. • *Ongoing Operations and Maintenance* – Continuous maintenance and operation support, including troubleshooting and bug fixes, regular software updates and planned enhancements. VALID also dispatches personnel to Guam as needed for maintenance, installations and training.

Reference 3	Detail
Reference Company Name:	Regional Transportation Authority (RTA)
Company Address:	175 W. Jackson Blvd, Suite 1650, Chicago, IL 60604
Type of Industry:	Government
Contact Name:	[redacted]
Contact Phone Number:	[redacted]
Contact Email Address:	[redacted]
Description of system(s) implemented:	VALID has provided reduced-fare transit card services to RTA for more than a decade. VALID prints approximately 15,000 photo ID transit cards per month, in addition to processing all paper transit card applications. VALID manages the RTA card lifecycle, including application, approval, expiration notices and special programs. The most recent project launched in May of 2015 involved the following: • Supported the transition of existing RTA customers to Ventra compatible cards. • Enhanced customer application processing and data entry. • Secured customer demographic information, including sensitive data. • Streamlined data transmission between RTA, CTA, Metra, and Pace.
Date of Implementation:	[redacted]
Similarities to the DMV	The following is a list of significant similarities between the RTA project and the DMV project: • *Central Issuance* – VALID prints an average of 15,000 cards per month for RTA using highly-secure personalization facilities managing sensitive personal information using multi-step workflows. • *General Software Solution* – To accommodate legacy software and RTA's complex business rules, VALID created a hybrid solution using WebLink ID and custom developed software. VALID's solution design for

	the DMV will take advantage of the experience integrating our solution with existing systems and processes. • *Data Conversion and Migration* – VALID migrated over a million customer records for the initial implementation. Since then, VALID has managed several database transitions for RTA. VALID is familiar with mass data transfers and migrations and will apply this expertise to the DMV solution. • *Interfaces* – Developed and upgraded data exchange interfaces between VALID and customers (RTA, CTA, Metra, and Pace), all with disparate requirements. VALID expects to apply similar flexibility to develop interfaces for the DMV system. • *Reporting* – VALID has developed multiple customized reports to meet RTAs changing requirements over the long life of the program. VALID will apply its report creation experience to the DMV solution. • *Training* – Over VALID's ten-year association with RTA, our personnel have traveled to Chicago to provide direct training as well as providing training materials. VALID applies its commitment to training to all clients, including the DMV. • *Ongoing Service Support* – VALID's support staff has serviced RTA account for over ten years. VALID will apply its proven support process to ensure prompt and efficient resolutions to any service and support required by the DMV for the duration of the contract.

Reference 4	Detail
Reference Company Name:	Wisconsin Department of Natural Resources
Company Address:	P O Box 7924, Madison, WI 53707
Type of Industry:	Natural Resources State Agency
Contact Name:	[redacted]
Contact Phone Number:	[redacted]
Contact Email Address:	[redacted]
Description of system(s) implemented:	The system solution used for Wisconsin DNR tracks on a single card various DNR licenses purchased by individuals rather than carrying multiple paper licenses – one for each activity. DNR officers can read the magnetic stripe on the card produced by VALID to verify license validity. Citizens purchase card updates as new licenses each year. With VALID's system, data files are submitted through an SFTP site and run through USPS address verification. The card are then personalized with the individual's demographic data, and the magnetic stripe is encoded.
Date of Implementation:	[redacted]
Similarities to the DMV	The following is a list of significant similarities between the Wisconsin DNR project and the DMV project: • Card Design – It was critically imporant to Wisconsin DNR to issue a highly secure card that was also attractive and durable. VALID worked with their stakeholders to design and produce a high quality, secure card; and VALID can help Vermont design the best card for its needs. • *Central Issuance* – VALID prints an average of 5,000 cards per month for Wisconsin DNR using highly-secure personalization facilities managing sensitive personal information. • *General Software Solution* – To accommodate legacy software and Wisconsin DNR's business rules, VALID successfully created a custom solution using WebLink ID as the core. VALID's solution design for the DMV will take advantage of the experience integrating our solution with existing systems and processes. • *Interfaces* – Developed and upgraded data exchange interfaces with Wisconsin DNR. VALID stands ready to apply similar focus to develop interfaces for the DMV system.

	• *Reporting* – VALID has developed multiple customized reports to meet Wisconsin DNR s shifting requirements. DNR possesses the rights to pull inquiries and reports directly from the system using a secure cloud-based login. VALID will provide a versatile set of reports tailored to DMV's needs. • *Training* – During VALID's association with Wisconsin DNR, our personnel have traveled to Wisconsin to provide direct training as well as providing online training and all training materials in an electronic format. VALID applies its commitment to training to all clients. • *Ongoing Service Support* – Quoting an email from one of the WI DNR contacts: "Valid has always been easy and accommodating, never a hassle. I really do appreciate that, immensely. I've had several calls with other states who are taking notice of what we've done and I always tell them how outstanding you've been to work with." VALID offers similar ongoing support for Vermont DMV.

Part 2: Bidder Proposal Solution

1. **Provide a description of the technology solution you are proposing.**

Solution Introduction

VALID offers an integrated identity management platform, that enables jurisdictions to perform all necessary tasks to capture data and images for applicant enrollment; to evaluate, screen, and confirm the collected identity data; and to issue a secure credential and manage its ongoing lifecycle. VALID's proposed solution includes WebLink ID and BioLink ID, our own web-based software products, which will be hosted in the Amazon Web Services cloud. The solution includes all hardware needed for enrollment, all software needed for front and back office needs, all integrations with existing systems, and the production of secure credentials at VALID's production facilities.

- **WebLink ID enrollment** workflows feature an easy-to-use camera tower, signature tablet, and document scanner. It captures and stores photos and signatures, biometric data (optional), and identity breeder documents. The software and hardware are tightly integrated for incredibly fast applicant processing with no device manipulation by the DMV staff. The workflow's look and feel, required tasks, task sequencing, and business rules are configurable and user friendly which reduces the training burden on staff. The VT DMV front office users will enjoy working the modernized VALID solution.

- **WebLink ID gated issuance** and release readiness is optional and configurable, and it improves front and back office workflow at the DMV, if implemented. Many legacy applications, reports, and business processes are candidates for consolidation into WebLink ID which reduces burden on the DMV staff to maintain documentation and IT support for those solutions, and it lowers required training for new hires.

  For example, VALID implemented an intricate gated issuance (Release Readiness) WebLink ID process at the State of Washington Department of Licensing (DOL) which automates and streamlines the processing of issuances with exception flags. DOL worked exceptions from a series of reports before WebLink ID gated issuance, and it required human intervention to stop, restart, and permanently hold issuances.

  After DOL's WebLink ID implementation, the VALID solution handles a complex, multi-gate issuance vetting process driven by various exception flags including: (1) biometric fraud review resulting from one-to-many process; (2) possible fraud exceptions applied by front office DOL staff; (3) 1-time special mailing for enhanced driver licenses; (4) address verification; (5) CDLIS-PDPS; (6) AAMVA verification systems; (7) record response; (8) document review; (9) restricted license; (10) 24-hour administrative hold.

This is automated in WebLink ID and software users research the case and release the exception flags from WebLink ID gate workflows.

WebLink ID gated issuance optionally includes a biometric review sub-process. VALID offers its robust BioLink ID biometric engine with case management and investigation tools for the proposed solution. It integrates with WebLink ID's issuance process. VT DMV administrators define exception flag quantity and types (including biometric review), flag processing sequence, and flag-to-gate mapping (issuance queues available to staff to resolve exceptions).

- **WebLink ID card management** workflows available to VT DMV back office staff include real-time factory status updates for better insight into card issuance timing. This integration also displays front and back card images to VT users captured by the printer's QC camera module representing the final produced card vs. a rendered image of its theoretical appearance.

  Card management functions are optional and configured by WebLink ID user roles. DMV staff can view (download, print, and email directly from the app) the final produced card and templates (for example temporary letters with card image for lost issuance scenarios), and manage its lifecycle to terminate, reissue, and return cards.

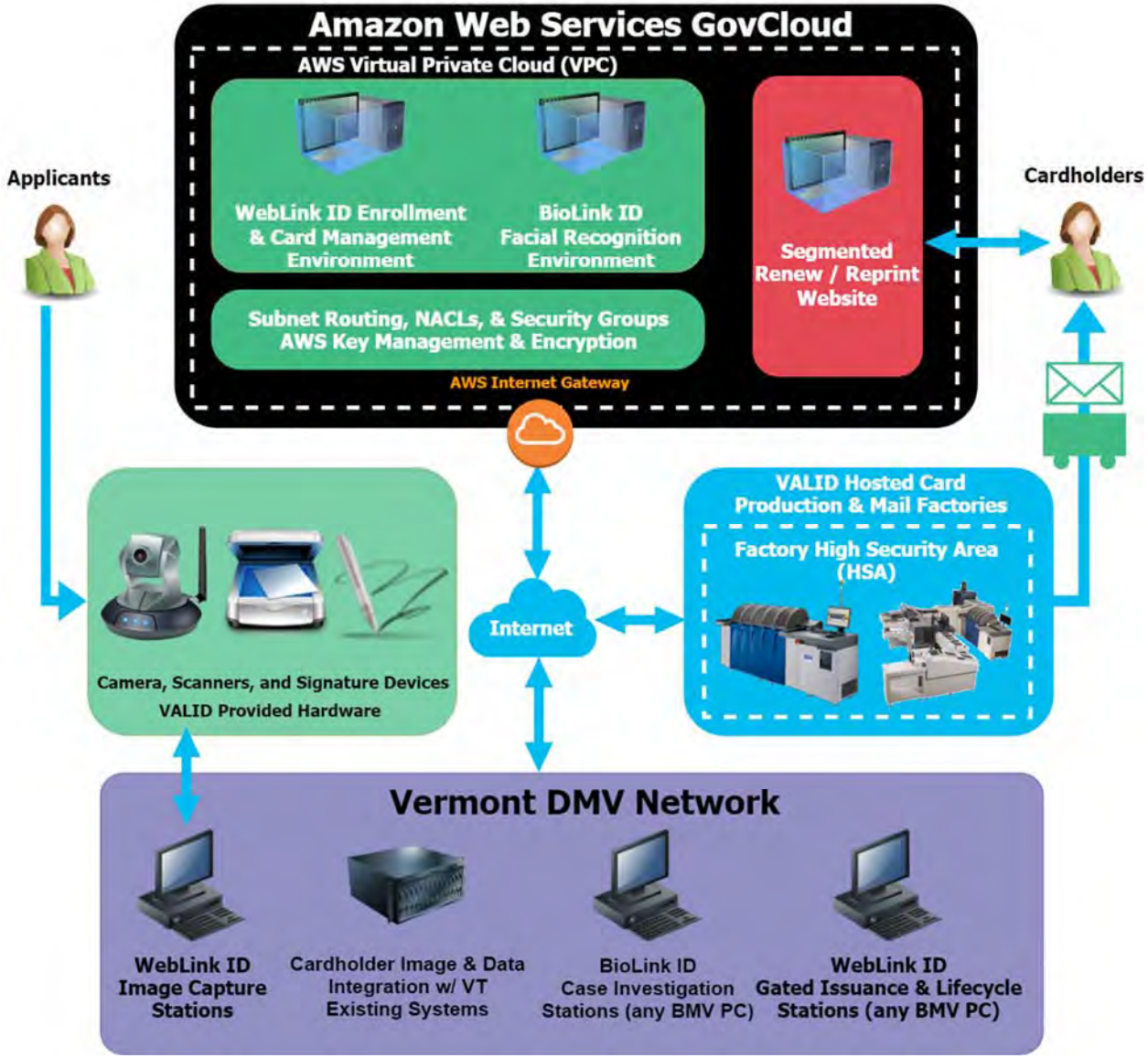
- **Secure card issuance** occurs from two primary VALID facilities (factories). VALID proudly offers it as the industry's most innovative solution regarding high availability and disaster recovery (DR). Each factory produces a share of the daily VT DMV volume while both facilities independently have capacity to deliver 100%+ daily volume if needed.

  Contrast daily production from two facilities (each having capacity for 100%+ volume) with the typical model for DR: primary site with a failover backup. It presents tremendous problems for the DR site: insufficient staff training, unexercised equipment, inadequate standard operating procedures, scarce or missing inventory for job completion, and many more. These concerns are completely removed by the VALID solution. The State of Washington Department of Licensing (DOL) sleeps well knowing that VALID issues its cards daily from two redundant, secure facilities, and the VT DMV will share that same production continuity guarantee if a VALID facility ever faces an unanticipated disaster scenario.

VALID obsesses about physical and logical security: every facility, software product, and process executed within VALID has security embedded. VALID manufactures and personalizes financial cards for large bank issuers and SIM cards for major telecom network operators. These markets require its partner manufacturers to undergo compliance audits for physical and logical security. VALID typically 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. Additionally, VALID operates with seven full-time guards and one supervisor monitoring secure operation; fire detection; and intrusion (physical and logical) detection: CCTV, motion sensor, glass break detectors, and card readers. VALID grants facility ID card access using least-privileged methodology, and the card access system has dual controls, "hold open" and "dead-man alarms."

VT DMV Solution Overview

The proposed VALID solution utilizes WebLink ID and BioLink ID as the cornerstone for the issuance process. VALID develops its software applications as products and not custom, one-off applications. Therefore, software proposed for VT DMV is widely deployed in multiple markets and hundreds of implementations. The solution diagram below displays a high-level view with WebLink ID and BioLink ID (shaded green and hosted in Amazon GovCloud) driving the issuance process with VALID provided capture hardware deployed locally within VT DMV offices. The VALID hosted factory (shaded blue) performs the central issuance card production, and VALID staff operate a third application called Job Control System. It drives the factory process and integrates tightly with WebLink ID, but VT DMV staff never function in it. These three applications constitute the heart of the VALID Driver's License and ID Card production solution, and the red item contains the optional self-registration, renewal, and reprint website.


Amazon Web Services GovCloud
AWS Virtual Private Cloud (VPC)
WebLink ID Enrollment & Card Management Environment
BioLink ID Facial Recognition Environment
Subnet Routing, NACLs, & Security Groups
AWS Key Management & Encryption
AWS Internet Gateway
Segmented Renew / Reprint Website
Applicants
Cardholders
Camera, Scanners, and Signature Devices
VALID Provided Hardware
Internet
VALID Hosted Card Production & Mail Factories
Factory High Security Area (HSA)
Vermont DMV Network
WebLink ID Image Capture Stations
Cardholder Image & Data Integration w/ VT Existing Systems
BioLink ID Case Investigation Stations (any BMV PC)
WebLink ID Gated Issuance & Lifecycle Stations (any BMV PC)

Facial Recognition Use Case

Facial recognition (FR) augments applicant identity assessment and provides potential fraud alerts before the issuance process finalizes through biometric templating techniques. There are three common biometric workflow types used by jurisdictions during the issuance process:

1. 1:1 – newly captured image compared against the known subject's last enrolled image
2. 1:R – newly captured image compared against the known subject's image history (all)
3. 1:N – newly captured image compared against all images of all subjects within the database (deduplication)

The first two workflows are verification transactions which enhance the applicant screening process. The applicant enters the DMV office for an issuance service and declares her identity, and the system compares the captured photo against that known identity's previous photo (1:1) or all (1:R). This amplifies the current DMV techniques to verify an individual for a renewal service. The biometric verification (1:1 and 1:R) will not occur for those receiving a first issuance (or have no photos on record). The third workflow is an identity transaction, and it mitigates multi-identity fraud. The applicant enters the DMV office for an issuance service and declares her identity. The newly captured photo might be a first issuance, or even a legitimate renewal, using the declared identity. The verification workflows (1:1 and 1:R) pass without issue. However, what if this applicant previously received a VT DMV credential using a different established identity? The 1:N comparison of the newly captured photo against all photos for all subjects will trigger a potential fraud (the photo for the new issuance matches a photo used previously for a different identity). The issuance is flagged for biometric review. This is one fraud use case that 1:N prevents and there are many more.

VALID Facial Recognition

The VALID solution includes a facial recognition (FR) system. System administrators configure this optional step in the workflow. Legislative changes or other drivers may prevent biometric review of applicants. This does not present a problem; VALID configured its solution so that biometric processing turns on and off without disrupting the overall issuance process.

VALID offers BioLink ID to the VT DMV which features biometric analysis and matching, fraud investigation tools and case management, and a robust application programming interface (API) which integrates BioLink ID with WebLink ID. There are several primary integration points between WebLink ID and BioLink ID.

- The first occurs when front office operators capture a photo within the WebLink ID enrollment workflow for those applicants with declared identities. The captured photo auto-enrolls (without operator intervention) into the BioLink ID engine which executes a verification transaction (1:1 or 1:R or both), and WebLink ID presents that result to the operator within the enrollment workflow. VT DMV establishes a front office business process which drives one or more options within the WebLink ID workflow. The system supports 1:1 and 1:R override permissions (additional benefit: overrides are logged and auditable; and VT DMV system administrators define the system roles and the associated permissions available to those roles); or users apply exception flags for potential fraud; or another business process defined by VT DMV.

- The next WebLink ID and BioLink ID interface occurs after the 1:N identity transaction (deduplication) occurs. The system supports a real-time 1:N (at time of WebLink ID photo capture) or a batch (typically overnight) 1:N transaction. VT DMV drives this configuration; typically most customers choose overnight batch 1:N transactions for various customer service reasons, such as: processes do not exist in the front office for staff to handle potential fraud, front office users are not trained investigators, and more. Regardless when the 1:N occurs, WebLink ID internally marks the issuance as 1:N pending after it captures a photo and enrolls it into BioLink ID. This prevents the issuance from moving to the next stage until it receives the biometric 1:N update from BioLink ID.

  Meanwhile BioLink ID executes the 1:N, and it updates WebLink with its two possible results: 1) The issuance passed the 1:N deduplication (all subjects and all images). 2) It failed the 1:N process. Successful 1:N transactions drive WebLink ID to move the issuance forward through its additional, optional downstream gated issuance processes and workflows. WebLink ID marks those issuances that fail the 1:N process for biometric review; it will not move the issuance forward until the photo and identity are adjudicated by VT DMV staff.

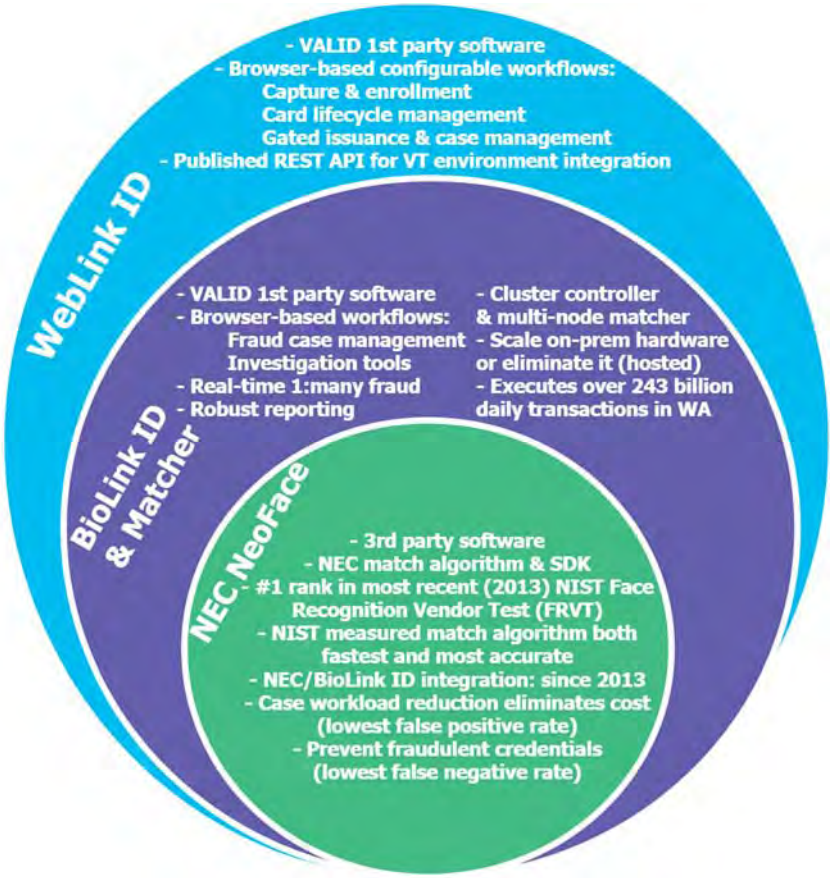
  A highly trained team reviews the failed 1:N queue the following day (if exercising the BioLink ID 1:N nightly batch option) using BioLink ID. Its queues for potential fraud review, investigation tools, and case management are highly optimized for ease of use. VALID organized the queues and tools for speed which enables investigation teams to adjudicate potential fraud cases efficiently to quickly empty pending review queues. It features a masterful user interface that offers multiple investigation tools to compare the subject photo with candidate photos the system returned as potential fraud. These tools include: (1) varying views including side-by-side, image overlap (up/down and left/right), tile selection, and image blend; (2) image enhancement features; (3) pins & measurements; and many more. The investigator then closes the case making final judgement to allow (false positive) or halt (legitimate fraud) the issuance, and the case moves into the BioLink ID case management history.

- The investigator's judgment drives the last WebLink ID and BioLink ID interface. The case judgment auto-updates the issuance status in WebLink ID which previously held it pending the biometric review. WebLink ID now moves it forward through the downstream issuance process if the investigator allowed it, or permanently holds it if the investigator marked it fraudulent.

VALID Software: Proven Scale + NEC Partnership

The proposed VT DMV solution includes the VALID-built BioLink ID and WebLink ID which also operate at the State of Washington Department of Licensing (DOL) and many other non-driver license customers. WebLink ID drives the enrollment and issuance for up to 20K cards/day at DOL, and the WebLink ID database contains 31MM total issuance records. VALID also leveraged its massive WebLink ID APIs to create a highly integrated system at the request of DOL. WebLink ID integrates with multiple stakeholders in the State of Washington: Secretary of State, Washington State Police, U.S. Customs and Border Protection (CBP reads Enhanced documents at the Canada and U.S. border and queries WebLink ID), Washington Courts and Department of Corrections, and several DOL-systems: queueing system at licensing offices, DMV driver record management software, address verification service, and countless more.

BioLink ID features biometric fraud investigation tools and case management for DOL, and offers a hyperscale matcher application: web services, cluster controllers, and multi-node matchers. It processes over 243 billion daily transactions for DOL against an 18 million biometric photo database. Its pristine architecture provides fault tolerance, high availability, and load balancing throughout the various server components. The application also supports additional biometric modalities beyond facial recognition if VT DMV wishes to extend its biometric processing in the future to iris or another modality.



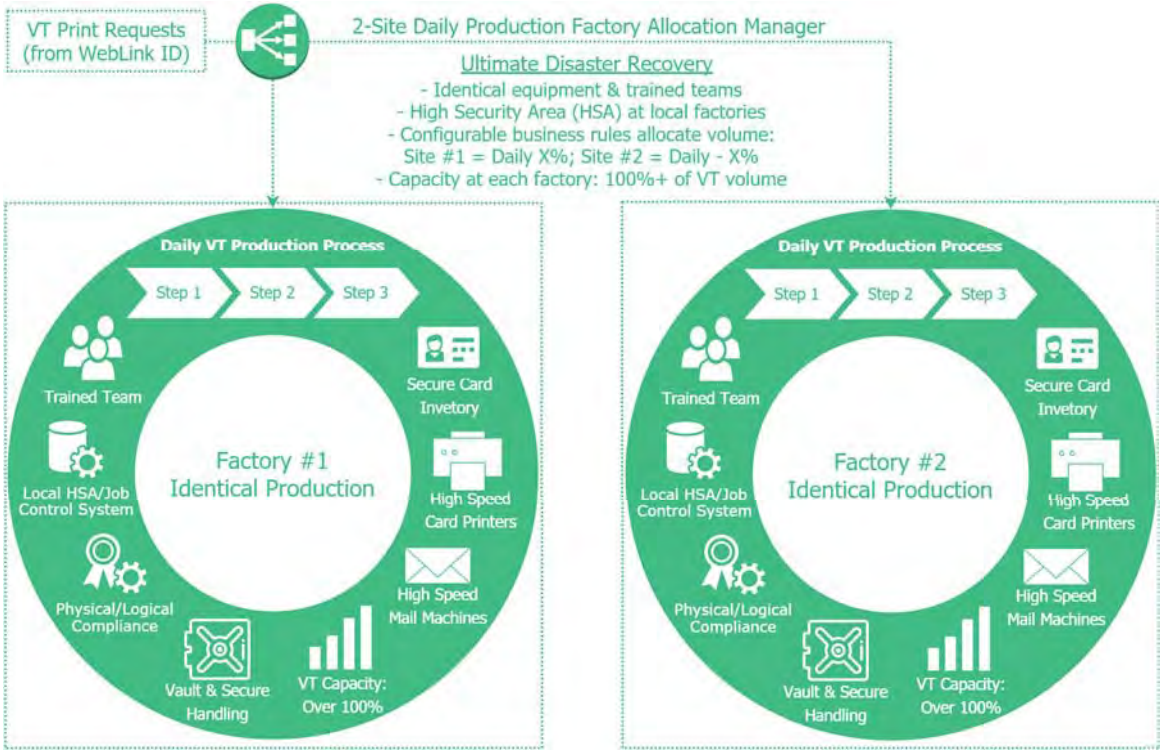
BioLink ID integrates the #1 rated facial recognition algorithm tested by the National Institute of Standards and Technology (NIST) in its most recent Facial Recognition Vendor Test (FRVT) from 2013. It tested algorithms offered by the leading providers: NEC, Toshiba, Cognitec, 3M/Cogent (Gemalto), Sarfran Morpho, and more. NIST rated the NEC algorithm #1 in accuracy and speed. DOL experienced a significant drop in facial recognition false positive investigations when converting from its legacy issuance provider to VALID, and this decreased the overhead placed on the investigation team. VALID will always support the leading algorithm provider(s) to offer its clients. However, the BioLink ID matcher engine is algorithm agnostic; it supports multiple algorithms from multiple providers. The leader today is NEC, but VALID offers technology to support top algorithms from other providers if someone else is king.

VALID confidently offers VT DMV its WebLink ID, BioLink ID, and NEC solution knowing its scale. The deployed system supports load balancing and a redundant, fault tolerant high availability architecture. The systems have experienced no SLA unexpected downtime at DOL.

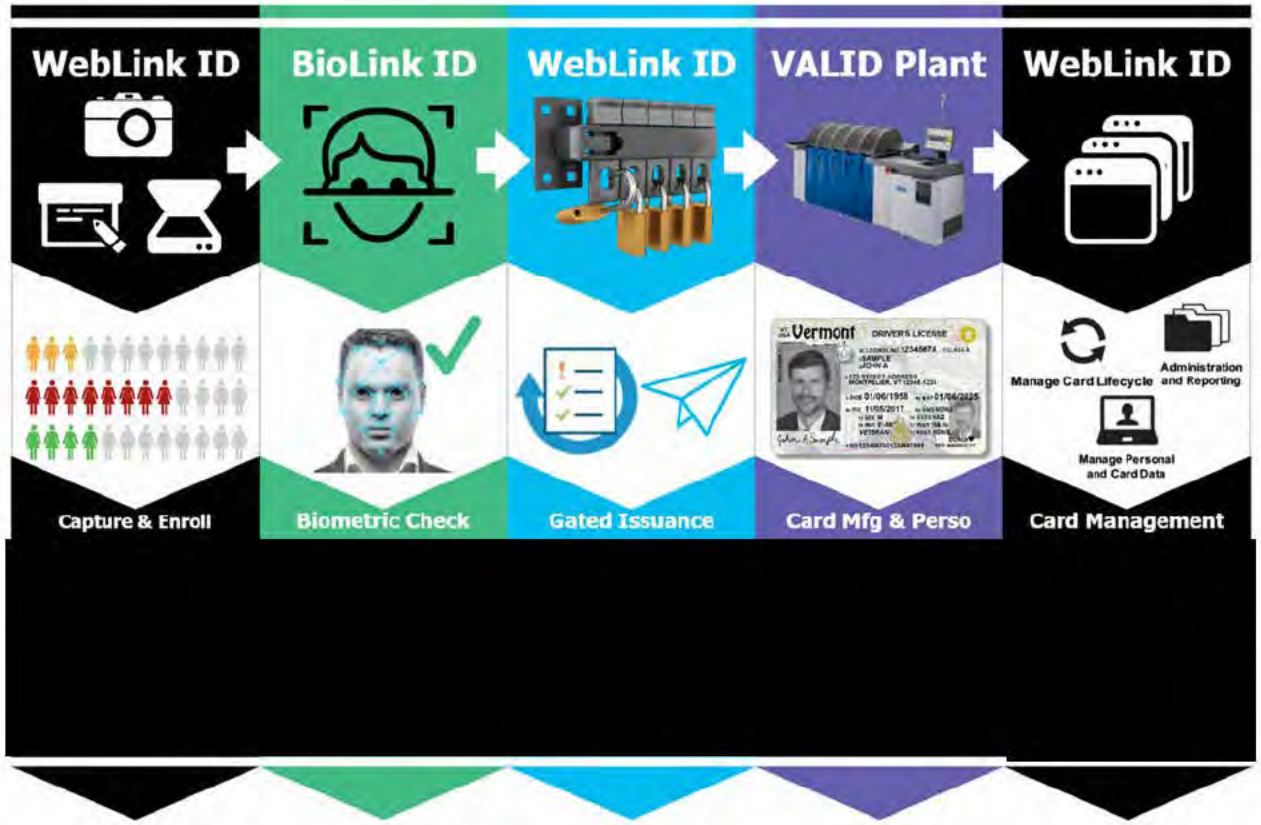
Issuance Flow and Secure Card Production Factories

WebLink ID and BioLink ID are the system pillars within the VT DMV solution. WebLink ID features flexible workflow modularity for applicant enrollment, identity vetting and adjudication including optional gated issuance with biometric review, and card management to issue credentials and manage its lifecycle. BioLink ID supports the process with its facial recognition engine and investigation tools for WebLink ID's gated issuance biometric review subcomponent.

Secure card issuance occurs from two primary VALID facilities (factories). VALID proudly offers it as the industry's most innovative solution regarding high availability and disaster recovery (DR). Each factory produces a share of the daily VT DMV volume while both facilities independently have capacity to deliver 100%+ daily volume if needed.


VT Print Requests (from WebLink ID)
2-Site Daily Production Factory Allocation Manager
Ultimate Disaster Recovery
- Identical equipment & trained teams
- High Security Area (HSA) at local factories
- Configurable business rules allocate volume:
Site #1 = Daily X%; Site #2 = Daily - X%
- Capacity at each factory: 100%+ of VT volume
Daily VT Production Process
Step 1
Step 2
Step 3
Trained Team
Secure Card Invetory
Local HSA/Job Control System
Factory #1 Identical Production
High Speed Card Printers
Physical/Logical Compliance
High Speed Mail Machines
Vault & Secure Handling
VT Capacity: Over 100%
Daily VT Production Process
Step 1
Step 2
Step 3
Trained Team
Secure Card Invetory
Local HSA/Job Control System
Factory #2 Identical Production
High Speed Card Printers
Physical/Logical Compliance
High Speed Mail Machines
Vault & Secure Handling
VT Capacity: Over 100%

The typical issuance process:



- DMV users execute WebLink ID enrollment workflows to capture data, images, and documents.
- BioLink ID performs the biometric analysis, and updates WebLink ID with the result.
- WebLink ID moves the issuance through a series configurable gates checking for exception flags and data accuracy.

- WebLink ID sends the print request with data payload after passing all gates to the two VALID factories for daily printing and mailing. The factory process integrates tightly with WebLink ID and sends it real-time updates providing better insight into card issuance timing for VT DMV back office WebLink ID workflow users. The factory sub-process to the issuance flow is shown below.

[redacted]

- The back office WebLink ID card management workflows enables users to view front and back card images captured by the printer's QC camera module representing the final produced card vs. a rendered image of its theoretical appearance. Other optional card management functions driven by roles and permissions: view, download, print, and email the final card images and other templates (example temporary documents or certification letters); expedite, hold, reissue, and return cards; and many more tasks.

WebLink ID & BioLink ID Hosted at Amazon Web Services (AWS)

Most government agencies face the ongoing challenge to reduce costs while also raising customer service levels to align with expectations demanded by its user base. Hosted or Software as a Service (SaaS) applications help reduce the overhead cost burden for agencies. On-premise (customer data centers) applications require server hardware; storage infrastructure; add to network complexity with load balancing, firewalls and network access control lists; and place additional burden on the agency infrastructure that serves many other applications to its stakeholders. Hosted applications transition that burden to the software provider which unlocks agency resources and infrastructure to manage other activities and services vs. supporting and maintaining software deployed to the local data center.

The VALID proposal includes a hosted WebLink ID and BioLink ID. These are web-based applications available to VT DMV users only. Users access and authenticate to WebLink ID and BioLink ID through their local PCs' web browsers (i.e., Chrome, Firefox, Internet Explorer or Edge). VALID applications mimic the model of secure banking: users access and authenticate to software running on a server by using a PC browser to connect with a secure website. The DMV application itself will sit on infrastructure hosted by VALID through the Amazon Web Services (AWS) GovCloud region. VALID staff apply security and maintenance patches and upgrades at the operating system, web server, application server, and database server levels for the guest servers operating VT DMV applications. The host servers (the Amazon infrastructure and virtualization layer itself) are maintained and patched by Amazon automatically. VT DMV applications operate on up-to-date servers without the maintenance burden on DMV IT staff; it shifts to VALID and Amazon (the Infrastructure as a Service (Iaas) provider).

The IaaS market is currently a 2-horse race between Amazon (offering AWS) and Microsoft (offering Microsoft Azure). Google, IBM, and other providers exist but trail the leaders significantly in market share, services offered, and strategic vision. The clear leader between Amazon and Microsoft is AWS. It dominates market share compared to Azure and offers a more complete total solution. That should not surprise anyone because Amazon entered the IaaS business over 11 years ago. It spent $16.1 billion (largest amount for any corporation in the world) in its last fiscal year on research and development, and employs thousands of developers and security/network engineers to secure its IaaS through software applications and services, server infrastructure, and network security and segmentation.

IaaS enables streamlined patching for the VT DMV infrastructure, and the hosted VALID model similarly simplifies updates to the WebLink ID and BioLink ID applications which are services oriented applications. Specifically, its architecture features microservices. Generically speaking microservices are small, independent functions of a software application which are componentized and decoupled from each other but work together through a defined application programming interface (APIs). An API is simply a set of definitions and protocols that two software applications use to communicate. In other words, these services are small, optimized to perform very specific tasks, and segmented from other parts of the application. Any configured software code related to VT DMV's specific implementation or custom integration with other VT DMV systems is componentized into a set of microservices. This makes application updates safer; core WebLink ID and BioLink ID services update without affecting VT DMV specific system integrations.

Hosted WebLink ID and BioLink ID updates are not forced. VALID will communicate the updates to VT DMV and outline the release implications and the update's benefits. VT DMV ultimately chooses if it wishes to receive the updates after it passes VALID's quality assurance process though the DEV (development) and QA (quality assurance) environments.

AWS Security and High Availability with VALID Network Topology

AWS GovCloud (US) is a specific region within the broader AWS infrastructure that adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations, the Federal Risk and Authorization Management Program (FedRAMP) requirements and Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Levels 2 and 4. Its design enables U.S. government agencies (and contractors) at all levels to run sensitive workloads on the AWS cloud IaaS.

WebLink ID and BioLink ID reside in the certified AWS government cloud within its own virtual private cloud (VPC) environment. VALID implements a multi-layered approach to guarantee protection of VT DMV software applications, server infrastructure, and cardholder data. The layers include these definitions:

- **Elastic Load Balancer (ELB):** A massive, high availability load balance server(s) within the AWS infrastructure. Public ELBs accept and load balance requests including internet traffic and internal ELBs accept local requests only. This improves redundancy and high availability of load balanced application services.

- **Virtual Private Cloud (VPC):** A segmented elastic network within the AWS infrastructure and platform that shares common security and interconnection.

- **Subnet:** A collection of virtual servers. Public subnets have internet access while private subnets have local (non-internet) routes only which prevent inbound/outbound internet traffic.

- **Route Tables:** Subnets use route tables to direct traffic between servers.
- **Network Access Control Lists (NACLs):** Operates at the subnet level with route tables to control inbound and outbound traffic to servers. It acts as a firewall to create rules for server communication: accepted protocols, allowed ports, inbound and outbound IP ranges, and more.
- **Security Group:** Additional protection that operates at the server level. It allows inbound and outbound network connections for a server. Each security group consists of a list of protocols, ports, and IP address ranges.
- **Web Application Firewall (AWS WAF):** A firewall service that controls access to software and servers by allowing or blocking web requests based on criteria: header values or the IP addresses that the requests originate, protocol, and more. AWS WAF helps protect web applications from common web exploits that affect application availability or compromise security.
- **Virtual Private Gateway (VGW):** The Amazon side of a VPN connection that maintains connectivity.

The next diagram displays the logical system architecture for WebLink ID and BioLink hosted in the AWS IaaS cloud. It also displays the VPN connection from the AWS VPC to the VALID card production factory's data center.

[redacted]

There are several recurring themes in the diagram to note:

1. It features **encryption everywhere** for data at rest and in motion.

2. VALID layers security from internet requests to the application servers and database servers through a series of routing, rules, and firewalls that combine the native segmentation tools offered by AWS. Following is a high-level description of the model:

   The public load balancer resides in the only public (internet facing) subnet within the VPC. Its rules create an https listener to handle secure traffic only; it features other security configuration which protects it from bad actors and forwards requests to the WAF layer.

   The WAF layer is a private subnet and does not face the internet. The WAF servers only accept requests from the public ELB through routing, NACLs, and security groups. It receives requests from the load balancer and applies additional filtering. For example, it requires an originating IP range from the whitelisted VT DMV network. The request is forwarded to the web server only if it meets all rules and conditions.

   The web server layer is a private subnet and does not face the internet. The web servers only accept requests from the WAF servers through routing, NACLs, and security groups. The web servers' proxy requests to the application servers.

   The application server layer is a private subnet and does not face the internet. The application servers only accept requests from the web servers through routing, NACLs, and security groups. The application servers execute requests and access the clustered database servers.

   The clustered database server layer is a private subnet and does not face the internet. The database servers only accept requests from the application servers through routing, NACLs, and security groups.

3. The entire solution is redundant and fault tolerant. Additionally, each layer is load balanced by the massive and high availability AWS Elastic Load Balancer. Each layered tier within the stack is distributed across two segmented availability zones, within the segmented VPC, within the broader AWS GovCloud region. The layered tiers have multiple virtual server instances and belong to AWS auto scaling groups which are logical collections for the purposes of instance resource scaling and management. The database is a highly performant database cluster managed by the Amazon relational database management service. The data is replicated to a second cluster for high availability. The application servers are configured to check database server health before routing requests to it. The application servers auto-failover to the replicated database cluster if the database service becomes unavailable.

4. The environment integrates with the AWS Key Management Service (KMS). It is an HSM-based (Hardware Security Module) solution to protect and control keys used to encrypt data, and protect form man-in-the-middle attacks.

   The database features two-tier encryption key architecture. The tablespace keys are managed using the KMIP standard and the master encryption key is stored in AWS KMS. It enforces clear separation of keys from encrypted data and automates key rotation and storing historical keys.

The following diagram outlines communication from the VALID data center to the WebLink ID issuance application hosted in the AWS GovCloud VPC. The two networks connect through a virtual private network (VPN). The Virtual Private Gateway (VPG) maintains connectivity to the VPC on the Amazon side of the VPN. The VALID side features an AWS Gateway which is a VPN appliance tested by Amazon and compliant with its VPC VPG within GovCloud.

The WebLink ID issuance manager in AWS sends print requests to the factory allocator manager hosted by VALID. It travels through the encrypted VPN tunnel. Additionally, the traffic between issuance manager and factory allocator is secure TLS 1.2/https communication.

[redacted]

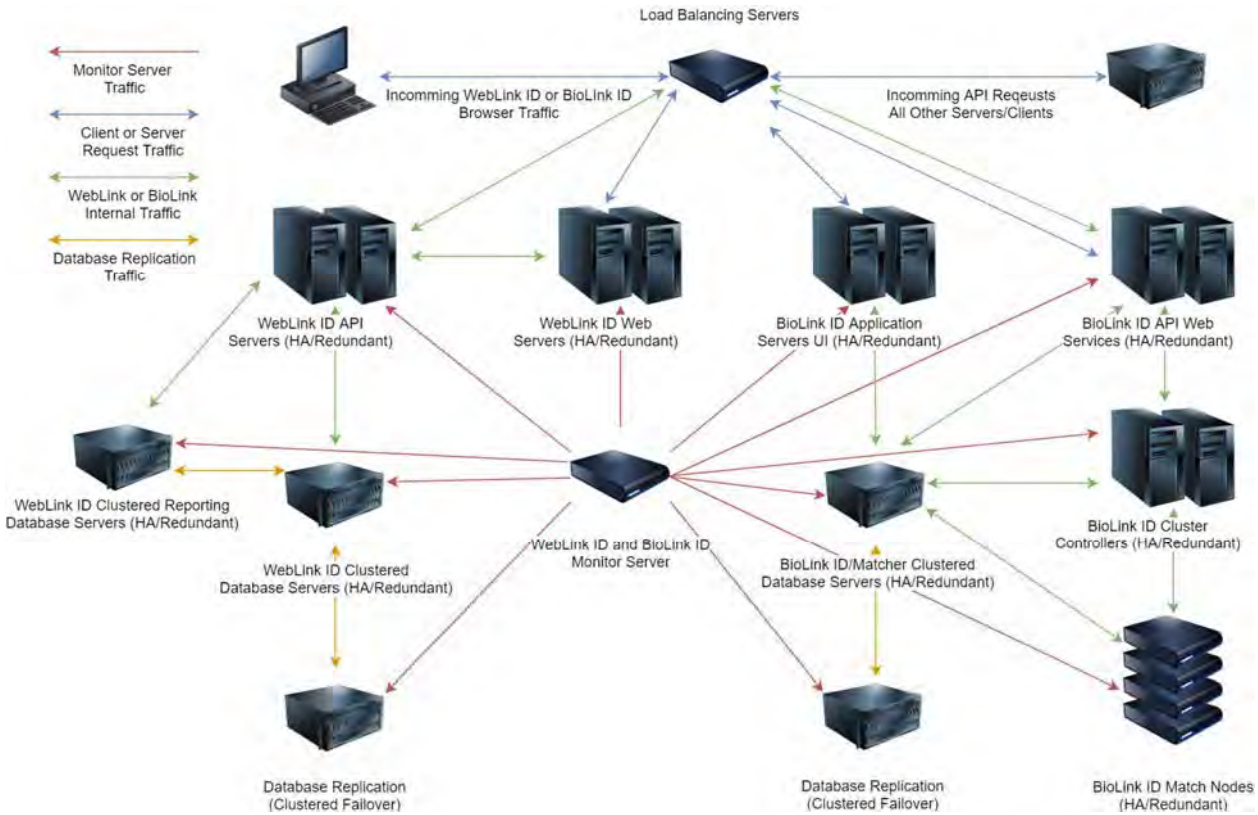
[redacted]

The VALID server layout for the WebLink ID and BioLink ID engines is shown in more detail below. The solution includes the native AWS load balancing. VALID also provides a monitor server that provides a dashboard to display real-time health for all servers and application endpoints.

The load balancing server manages all traffic between web browser clients, applications consuming the APIs, or any other server data request such as a Motor Voter engine, or other state systems requesting driver's license or ID information. The load balancer ensures no single web application server is over- or under-utilized. The monitoring server constantly checks the utilization and status of each server in the environment, and will manage sending reports or warnings to any staff on the approved distribution lists.

WebLink ID and BioLink ID application servers are installed in clusters, each will have traffic managed by the load balancing server, and will communicate with their appropriate database or services servers. The WebLink ID and BioLink ID database servers are redundant and utilize the AWS managed relational database service to keep data consistent between each instance. WebLink ID and BioLink ID can utilize either of the redundant servers for any transaction.

BioLink ID additionally utilizes redundant cluster controllers for managing the match nodes used for the facial recognition match requests.



The above diagram is of the proposed Production environment. Additionally, VALID will provide a Disaster Recovery and a separate QA environment.

2. Provide a description of the capabilities of the technology solution you are proposing.

VALID's proposed solution's capabilities can best be summed up as technologies selected to provide the DMV with a modern, scalable, extensible, secure and fault-tolerant solution for Driver's License, Photo ID and additional secure credential production. The proposed solution is fundamentally designed and architected to meet the DMV's custom needs, while integrating with both existing and future systems, allowing the environment to grow as the DMV and other departments grow their need for Identity Data. The solution contains four applications developed by VALID, WebLink ID, BioLink ID, Factory Allocation Manager, and the Job Control System.

WebLink ID

WebLink ID is a secure, web-based identity enrollment, application and credential management platform. Any authorized PC with Internet or Intranet access can transform into a feature-rich, WebLink ID card processing workstation. WebLink ID targets both the small ID card clients that demand basic data entry and credential issuance, as well as the complex, multi-process clients that require the highest standard of photo and signature capture, document collection, verification services such as AAVMA portals, and biometric verification services for a highly-secure centralized card issuance or over-the-counter card printing solution.

The WebLink ID application uses a web browser solution to scale usability and adaptability requirements to meet all identification software customers' needs. At its core, WebLink ID is a workflow engine, executing a series of tasks building and modifying a stream of data pertinent to issuing a driver's license or identification credential. The flexibility of WebLink ID enables the collection of tasks to vary greatly from credential to credential. The enrollment workflow may be a simple capture photo and print card single-page workflow or a multi-step workflow representing a series of tasks.

With centralized system management and an unlimited range of possible workflow designs, WebLink ID can offer exceptional adaptability to the unique aspects of the state's credential issuance and management requirements: administrators design and configure workflow tasks; roles and permissions; user groups; users; and card, form, and report designs.

The web-based architecture lends itself to an organic process of application refinement and feature enrichment that is continually driven by successful experiences in meeting real-world challenges and innovation. In this way, WebLink ID virtually eliminates identity software obsolescence with frequent updates and upgrades available to the customer if a client prefers to upgrade its instance.

BioLink ID

BioLink ID is a web-based biometric analysis, storage and case management solution for photos and fingerprints. Together the BioLink ID and WebLink ID servers replace the central issuance server previously used. BioLink ID stores the desired biometric information for 1:1, 1:N, 1:R, and

N:N biometric matching and verification. BioLink ID serves as both the biometric analysis engine as well as the application to view, manage and solve biometric cases created during the enrollment or migration process. BioLink ID uses the best-of-breed algorithms for its biometric analysis and verification, for this proposal, that is NEC's Neoface.

As it is a web based application, any workstation can become an investigation station allowing for image analysis, ad-hoc facial recognition queries, and suspected fraud case investigation. This removes the need to acquire costly, single PC investigation solutions.

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

VALID Add-ons: Value Above DL
- Integrated VALID products extendable to VT: mDL w/ FinTech & eSIM capability
- Data aggregation & cleansing for analytics and business intelligence
- Standards-based identity software & card process extensible to neighbor jurisdictions
- Vast production in NJ: Driver's License & EMV credit/debit mfg & perso

Trusted Solution
- Commercial-off-the-shelf apps: ongoing roadmaps of new features/tech.
- Available to VT: ongoing optional updates to WebLink ID, BioLink ID, & NEC algorithm
- Low risk application version updates: custom VT integration APIs are segmented
- Massively scaled AWS-hosted apps built w/ native fault tolerance & high availability
- Reporting engine & performance monitoring

Dynamic Production
- Vertical integration magnifies chain of custody through USPS
- Card agnostic: align card features & cost to budget
- Dual primary mfg & perso plants yield ultimate DR solution
- Real-time expedited handling, pulls, and updates w/ WebLink ID
- High-speed QC camera installed at printer: captures actual card images viewable in WebLink ID

Embedded Security
- 3rd party security & vulnerability tests of all software & data centers
- Manufacturer of EMV credit & debit cards for major US issuers
- SIM card manufacturer for large telecom wireless carriers
- Obsessed with physical and logical security in all facilities
- Secure manufacturer and perso bureau for two US DL jurisdictions

NEC NeoFace
- Facial recognition (FR) algorithm
- #1 rank in 2013 NIST FR tests
- Rated fastest AND most accurate
- Case workload reduction eliminates cost (lowest FPR %)
- Prevent fraudulent IDs w/ max. accuracy (lowest FNR %)
- VALID/NEC FR partnership: 5+ years including 18MM WA images

WebLink ID
- Hosted or on-premise
- Integrated workflow-based app: Capture& enrollment | Gated issuance Card lifecycle management
- Real-time biometric & factory production status
- Browser-based available to authorized VT PCs
- Configurable workflows: photo first & other
- REAL ID workflow: erify data w/ ext. services from AAMVA and other sources

BioLink ID
- Hosted or on-premise
- Browser-based available to VT authorized PCs
- Verify identity (1:1) or (1:R) real-time
- Real-time or batch fraud detection (1:many)
- Scalable architecture: 243 billion daily transactions in WA with growth capacity
- Fraud case management & investigation tools
- Configurable match thresholds for varying transaction types: 1:1, 1:N, ad hoc (and more)
- NEC integration since 2013

3. If a proprietary software is being proposed, provide a description ofthe:

A. Standard features and functions of the software:

B. The software licensing requirements for the solution:

C. The standard performance levels:

- **Hours of system availability:**
- **System response time:**
- **Maximum number of concurrent users:**
- **Other relevant performance level information:**

WebLink ID and BioLink ID are applications developed by VALID and sold by VALID or its dealers. These applications are the core components of the solution being provided to the DMV.

A. Standard Features and Functions (High level):

WebLink ID Features	BioLink ID Features
• Web based customizable workflow application • Built using Service Oriented Architecture • Cross platform support for web application (Windows, Linux, IIS, Tomcat) • Multi-browser support (IE, Edge, Chrome, Safari, Firefox)	• Web based facial recognition, case management and adjudication application. • Multi-browser support (IE, Edge, Chrome, Safari, Firefox) • API interface for additional integration
Supports Customized Enrollment and Lifecycle Management Tools for:	Multiple match type queries supported
• Data Capture • Image Capture ○ Photos	• 1:1 for matching • 1:R for matching • 1:N for matching

○ Signatures ○ Documents • Vetting • AAMVA Web Services ○ US Passport ○ SSOLV ○ VLS ○ Document Authentication ○ Address Verification	• N:N for migration • Ad-Hoc Investigation Queries ○ Images not previously enrolled ○ Additional Queries using new match values
Credential Issuance Lifecycle	Includes real time image processing dashboard for system usage monitoring
• Renew • Reprint • Cancellation before Issuance	• Includes reporting tools for image processing analysis
Customizable Gated Issuance	Automatically creates cases for potential fraud investigation
• Gates, Flags, and Statuses and Logic are all customizable to meet client's processes and requirements	• Allows operators to adjudicate cases, using image analysis tools in a web application (turning any workstation into a facial recognition investigation location)

• Visible or Team specific 'buckets' of applications needing investigation or additional review	• Manages the ownership, assignment and management of cases • Export of investigation materials as needed for Law Enforcement or Judicial System.
Integration with VALID's BioLink ID biometric analysis engine for facial recognition	

• Card Design and printing
  ○ In application card design tool
  ○ Integration with OTC printers for instant issuance
  ○ Integration with VALID's factory print (CIS) tools	

Administrative Tools	Administrative tools

• User, Group and Role Managers
• Can integrate with MS Active Directory
• Form Designer
• Report tools
  ○ Canned
  ○ Ad-hoc
  ○ Advanced
• Audit Log Tools
• System Messaging Tools
	• User, Group, and Role Managers
	  ○ Can integrate with MS Active Directory
	• Advanced system settings
	  ○ Thresholds and system tuning
	• Reporting
	  ○ Utilization
	  ○ Case Management
	  ○ Auditing
	• System Messaging Tools

B. Software Licensing
   1. WebLink ID
      a. For this proposal all WebLink ID instances needed are fully licensed for the term of the contract and maintenance periods. This includes licenses for development, QA, and production environments. We have configured and sized what is needed for our Production and QA environments, and included growth. Licensing needed for 3rd party integrated components such as address verification, document authentication or image analysis tools will be included in this proposal.

      b. Licensing by 3rd party verification services such as AAMVA portals is not included, and requires a separate relationship between the jurisdiction and AAMVA.
   2. BioLink ID
      a. For this proposal, all BioLink ID instances needed are fully licensed for the term of the contract and the maintenance periods. This includes licenses for development, QA, and production environments. Licensing needed for integrated components, such as Facial Recognition Algorithms have been defined and included in this proposal.

C. Performance Levels
   1. All VALID applications will perform at a minimum of 99.9% uptime, discounting any scheduled and approved maintenance periods.
   2. The scaling of the proposed solution's hardware specifically targets acceptable response times for application usage and expected concurrent users. Image analysis (quality) and image verification (1:1 matching) are conducted in real time, and the analysis of each is measured in fractions of a second. Data transport from the client workstations to the servers in the data center, is streamlined and minimized, such that only required elements are sent, to minimize traffic.
   3. The proposed solution will accommodate up to 300 concurrent users of the system, which exceeds the number of expected enrollment operators, managers and administrators which will be utilizing the system daily. This can be easily scaled to accommodate an almost unlimited number of users.
   4. Part of the VALID Proposed Solution is a performance monitoring engine, which will monitor the performance of each server, and primary services running, and will message the appropriate staff when performance reaches defined threshold, well before performance failures would be experienced.

4. Give a brief description of the evolution of the system/software solution you are proposing. Include the date of the first installed site and major developments which have occurred (e.g. new versions, new modules, specific features).

VALID's proposed solution includes WebLink ID 2.0, our third generation of web-based carding software. VALID has been designing and implementing web-based enrollment and carding solutions since 2005.

VALID's ID solutions group's experience with web based carding software began in 2005, when development began on CardsOnline. CardsOnline was originally designed as a web based card printing solution, and through its versions and implementations became a fully featured enterprise carding solution targeting multi-site carding applications. CardsOnline was designed to replace desktop carding software, and to eliminate the client-server management overhead, by removing 'thick client' desktop software. Desktop software requires local configuration, local version control and local support. By removing the desktop client, and replacing it with a web client, CardsOnline eliminated the need to update hundreds of machines with version updates, and then updating each of those machines with a configuration change. Its largest implementation, handled 65 different universities, running over 200 concurrent users, in a single server environment, peaking during college enrollment periods (school start in the fall, winter and summer) doing production of over 20,000 cards per day.

CardsOnline went through multiple versions and upgrades, but when faced with handling a complex workflow like what is required for driver's license issuance, VALID needed to create a configurable workflow web application capable of multiple steps, with multiple required connections for data transfer and validation, and the solution needed to be scalable for implementations larger than what CardsOnline could support. VALID began development of its second generation of web based carding software, WebLink ID, in the fall of 2012.

WebLink ID 1.0 was designed from our previous platform, specifically to allow for custom, complex, workflow solutions including integration with AAMVA portals and facial recognition engines. Along with WebLink ID, VALID began development of BioLink ID, its biometric enrollment, matching and analysis application. Both applications were developed to work with each other, and utilize API and web service communication layers for integration with each other and other systems clients needed our solution to work with. The first implementation of WebLink ID 1.0 and BioLink ID occurred in 2014. WebLink ID 1.5 is still being used and installed for cloud based clients, and is a premier product for the ID solutions group.

[redacted]

[redacted]

5. List the total number of installations in the last 3 years by the year of installation.

WebLink ID 1.5 and WebLink ID 2.0 installations over the past years are listed below. These numbers are a mix of each version, and represent installations into different verticals, not just Driver's License and State ID markets, but also Business Enterprise, School Districts, and other Government installs.

Year	Count
2015	10
2016	14
2017	17

6. Provide the total number of current users for the proposed system and indicate what version they are using.

- For WebLink ID 1.5 installations, we have over 1050 current users.
- For WebLink ID 2.0 and BioLink ID installations we have over 550 current users.

7. Have you implemented the proposed solution for other government entities? If so, tell us who, when, and how that implementation went?

As described in Part 1, References, we have many government customers, including but not limited to Wisconsin DNR, the RTA, Guam DMV and Washington DOL. Their implementations went well, and they remain excellent references.

- The system solution used for Wisconsin DNR tracks on a single, secure card the various DNR licenses purchased by individuals rather than having to carry multiple paper licenses – one for each activity. This has been an ongoing success.
- Regional Transportation Authority (RTA) VALID prints approximately 15,000 photo ID transit cards per month, in addition to processing all paper transit card applications. VALID manages the RTA card lifecycle, including application, approval, expiration notices and special programs.
- Guam DMV deployed their current version of WebLink ID in June of 2016, and BioLink ID in October of 2017, migration of legacy data and implementation of new software solutions have been accomplished on time and under budget. The REAL ID compliance project started in February of 2017 and is projected to be complete in April of 2018. At that time, we will continue to support the Territory of Guam.

- The State of Washington Department of Licensing deployed WebLink ID and BioLink ID in May of 2017, migration of legacy data and implementation of new software solutions has been accomplished on time and under budget. In the last seven months of 2017, we produced 1.5 M identity documents. VALID is now working on Release 2 to integrate with the DOL's vehicle system being implemented by FAST Enterprises.

- VALID currently produces secure smart cards for multiple WIC state agencies across the USA, including Texas, Missouri, Arkansas, Louisiana, New Mexico, Wyoming, Ohio, Pennsylvania, Cherokee Nation, and Isleta of Pueblo.

8. Provide a Roadmap that outlines the company's short-term and long-term goals for the proposed solution / software and label it Attachment 2.

Please refer to **Attachment 3** for VALID's Product Roadmap.

9. Provide a PowerPoint that provides an Executive level summary of your proposal to the State, Label it, Attachment #2

Please refer to **Attachment 2** for PowerPoint executive summary.

10. Describe any infrastructure, equipment, network or hardware *required* to implement and/or run the solution.

The following hardware is required for the implementation of the VALID proposed solution. The items listed are needed for the Image Capture and Enrollment stations, as this is a hosted solution, no server hardware is required.

Camera Tower	
Offering exceptional speed, quality and ease of use for moderate to high-volume image capture. Includes:	

- **Secure Capture tower**: A secure, durable design housing an 8-megapixel digital camera and high-intensity flash.
- **Photo software:** Intuitive software application that automates capture and cropping processes.

Specifications	
Physical Dimensions	• Tower: 13" x 32" • Base plate: 8" x 8"
Weight	22.0 lbs. (10.0 kg)
Flash Life	Designed for 250,000 flashes
Flash Recycle Time	• 5-second maximum for retakes • 20-second enrollment cycle
Effective Flash Distance	6 – 15 feet
Camera Resolution	8 megapixels
Non-skid Base Surface	Security mounting at base of unit for bolting to countertop or desk
Power Source	100/120 VAC 60 Hz
Connectivity	USB 2.0 high-speed compatible
Operating Conditions	• 60° F to 95° F • 20% to 80% relative humidity (non-condensing)
Safety	• National Recognized Test Lab (NRTL) for US • Safety Counsel for Canada

Topaz T-LB57GC	

The Topaz SigGem® Color 5.7 is an advanced electronic signature pad with 5.7 inch, full-color TFT VGA (640x480) LCD that captures and display. With the Topaz SigGem® Color 5.7 we can provide interactive text, graphics, and pen-tap hotspots and checkboxes to enable citizens to navigate screens, read agreements, and select preferred options before signing. This is an advanced electronic signature pad with a large, rugged signing area for long life; it has full-color LCD display to support customization; has high quality biometric and forensic capture features; and it captures and displays 'electronic ink' under the pen tip to produce a natural signature.

VALID selected the Topaz SigGem® Color 5.7 for this project in order to combine an interactive LCD signature capture system with the rich color text and graphics, because we believe DMV will need its citizens to be able to view text, data and graphics as well as gather from them accurate information and signatures.

Specifications	
Sensor Type	• Tempered glass surface • Rated to 2 million signatures • High-performance E/M digitizer

Pen Type	• Active low-power, rugged E/M • Battery-less • 1024 pressure level option
Resolution & Conversion Rate	• Exceeds industry standards • Programmable PPI
Data Encryption	AES optional, FIPS-197 compliant
Dimensions	Small Footprint (7.2" x 6.6" x 2.1" sloping)
Signing Area	4.6" x 3.4"

Xerox DocuMate 3125 Scanner	
The Xerox® DocuMate® 3125 color desktop scanner Automatic Document Feeder (ADF) handles everything from business cards to A4/Letter size documents. The small footprint and fits comfortably on any desk (especially when folded closed).	
Specification	
Image Enhancement Technology	Visioneer Acuity
Weight	5.1 lbs.
Simplex or Duplex	Duplex (two side scanning)
Interface	USB 2.0 (3.0 compatible)
Optical Resolution	600 dpi

ADF Capacity	50 sheets (20 lb paper)
Visioneer OneTouch Technology (PC)	Yes
Duty Cycle	3000 pages/day
ADF Maximum Paper Size	8.5" x 38"
Dimensions	11.2" x 6.5" x 6.7"
Output Bit Depth	• 24-bit color • 8-bit grayscale
Light Source	LED
Drivers	• PC: TWAIN, WIA, ISIS • Mac: TWAIN, ICA
Supported Operating Systems	• Windows 10, 8, 7, Vista (OneTouch 4) • Windows XP (SP2)
Imaging Sensor	Contact Image Sensor
Paper Thickness/Weight	13 to 32 lbs.
Power Supply	External
Power Consumption (active)	≤ 30 Watt
Power Supply Input Voltage	100 – 240 V~
Power Supply UK/Europe Plugs	Yes
Power Consumption (standby)	< 10 (<5.3 in power-safe mode) Watt
Speed @ 300 dpi, b&w, grayscale, or color	25 ppm / 46 ipm
Speed @ 200 dpi, b&w or color	40 ppm / 70 ipm

11. What is your recommended way to host this solution?

VALID is proposing a hosted solution, there is no hardware required in the DMV's data centers. The hosted solution's application, database, and services engines will be hosted utilizing Amazon Web Services, in secure data center which meets the following certifications and regulations:

Certifications/Attestations	Laws, Regulations, and Privacy
C5 [Germany]	CISPE
Cyber Essentials Plus [UK]	EDU Model Clauses
DoD SRG	FERPA
FedRAMP	GLBA
FIPS	HIPPA
IRAP [Australia]	HITECH
ISO 9001	IRS 1075
ISO 27001	ITAR
ISO 27017	My Number Act [Japan]
ISO 27018	U.K. DPA – 1988
MTCS [Singapore]	VPAT/Section 508
PCI DSS Level 1	EU Data Protection Directive
SEC Rule 12-a-4(f)	Privacy Act [Australia]
SOC 1	Privacy Act [New Zealand]
SOC 2	PDPA – 2010 [Malaysia]
SOC 3	PDPA – 2012 [Singapore]
	PIPEDA [Canada]
	Spanish DPA Authorization

12. Describe how your solution can be integrated to other applications and if you offer a standard-based interface to enable integrations.

WebLink ID and BioLink ID have been designed to integrate with other applications. Both support multiple modes for integration via published API's. Both applications support SOAP and JSON /Rest methods for communication. Additionally, WebLink ID supports the creation of micro-services which can handle any form of integration not covered by the existing APIs. Direct to database communication, or communication with legacy RPC based services are viable methods for WebLink ID to gather or push data to other engines.

Both applications can export information into a flat file designed for consumption by a legacy application that does not support real time communications identified above.

13. Describe the workflow and specify the status data that is tracked and available to user

As WebLink ID is designed as a customizable workflow and gated issuance application, there is not standard workflow or gated issuance process. The workflow will be designed with the DMV, to ensure it matches the expected enrollment process, communicates with the needed back office solutions, and moves the applicant requests through the gated issuance process required by the DMV. In the image below, the steps for the defined workflow are shown in the left-hand column. The operator can easily determine where they are in the process, and navigate to a previous step to make modifications as necessary. This image is a sample, and the design of the screen and workflow steps are dynamic and will be tailored to meet the DMV's business rules, processes and operator ease of use.

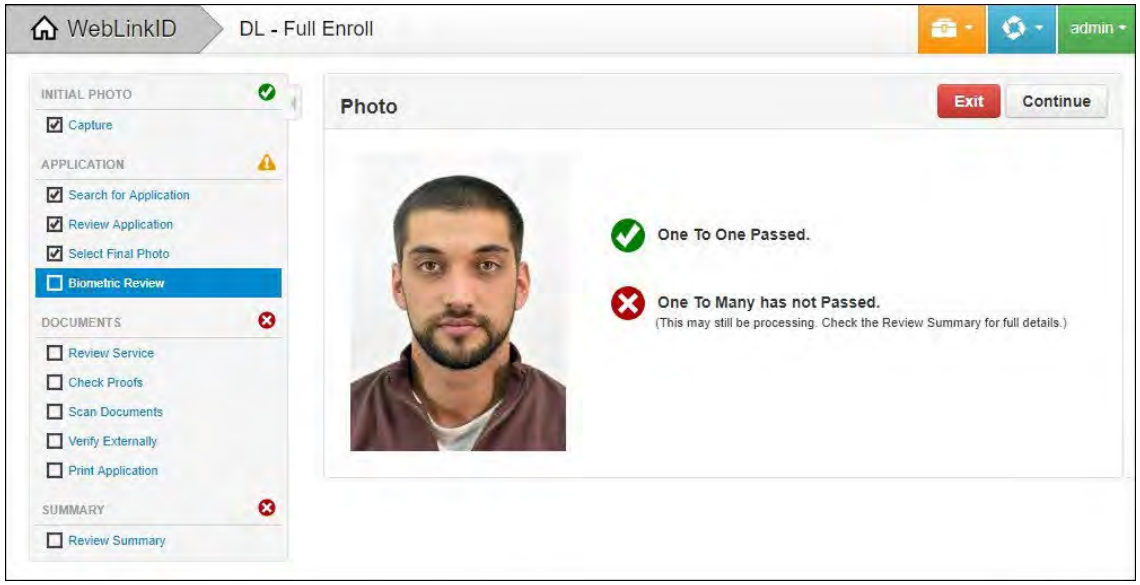


Figure 2: Sample Workflow

When defining the gated issuance process and workflows, application statuses are necessary to move the application through the process as well as provide information on where the application is in the gated issuance procedure. WebLink ID does incorporate some standard statuses when BioLink and our factory printing applications are used. Below is a quick list of the statuses possible between the VALID applications, but this is not inclusive of statuses needed to match the DMV's required processes.

Facial Recognition Statuses:

1) Enrolled
2) Queued for Verification (1:1)
3) Passed Verification
4) Pending Fraud Analysis (1:N)
5) Passed Fraud Analysis
6) Pending Investigation
7) Investigation Closed – Fraud
8) Investigation Closed – Accepted

Factory Printing Statuses

1) Sent to Factory
2) Received by Factory
3) Queued for Printing
4) Being Printed
5) Print Failure (reason code)
6) Queued for Mail
7) Mailed

14. Describe how you would close out this contract. For example, how would a transition to a new Bidder be structured, should you not win a rebid at the end of the contract term.

At the end of our contract, VALID will provide to the DMV the termination/expiration assistance to enable the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the DMV or its designee (including a competitor of VALID's). This will commence within 12 months of contract expiration or a date selected by the DMV. Additionally, VALID will provide Termination/Expiration Assistance in the event of any partial termination of this Contract (e.g., termination of an element or other component of the Services) by the DMV. VALID agrees to the following:

- At the DMV's request and subject to the terms of the termination agreement, VALID can continue to provide Termination/Expiration Assistance for a period of up to six (6) months following the effective date of termination/expiration, based on an established agreement to cover any costs associated with this service.
- VALID will provide the DMV an inventory of resources then performing work under the Services statement of work to assist the DMV. This resource inventory will include full-time or part-time equivalent resource models; skill and experience levels; education or technical skill certification levels required; and other mutually agreeable and pertinent information for the DMV to assemble or source the capabilities to perform the work post transition of services.
- In the event of a transfer of services back to the DMV and at the DMV's sole discretion, VALID will design and implement a training program for DMV employees designed to convey operational and technical knowledge associated with the ongoing operation of the in-scope applications and systems, conduct knowledge and documentation transfers for the then current operational processes and tasks, and work to ensure an overall continuity of services, until such time as DMV employees can reasonably perform their roles. These services will be priced using the Vendor rate card at the time of the request and as approved by the DMV.

- Notwithstanding any term to the contrary, contained in this provision, VALID will have no greater responsibilities under this provision than is required under the Contract as a whole, except such services provided at the then current DMV-approved Vendor rate card.

- Once a decision to terminate the Contract between the DMV and VALID is made, VALID will prepare a **Termination Assistance Plan,** which will cover the following:
  - ✓ Documentation of existing and planned support activities.
  - ✓ Identification of the services and related positions or functions that require transition and a schedule, plan and procedures for the DMV or its designee assuming responsibility.
  - ✓ Description of actions to be taken by VALID in performing Termination Assistance.
  - ✓ Description of how the transfer of (i) relevant information regarding the services, (ii) resources (if any), (iii) operations and (iv) contracts (if any) will be achieved.
  - ✓ Detailed description of any dependencies necessary for VALID to perform the Termination Assistance Services (including an estimate of the specific VALID staffing required).
  - ✓ An inventory of documentation and work products required to facilitate the transition of responsibilities.
  - ✓ Assistance in the identification of significant potential risk factors relating to the transition and in designing plans and contingencies to help mitigate the risk.
  - ✓ Establishment of a timeline for the transfer of each component of the terminated Services (including key milestones to track the progress of the transfer).
  - ✓ Preparation of a schedule and plan for VALID's return to the DMV of (i) the DMV Service locations then occupied by VALID (if any), and (ii) the DMV confidential information, the DMV data, documents, records, files, tapes and disks in VALID's possession.

15. Respond to the following questions about the solution beingproposed:

Question	Yes or No	Bidder Response / Explanation
A. Does the solution use Service Oriented Architecture for integration?	Yes	WebLink ID is based on Service Oriented Architecture explicitly for integration.
B. Does the solution use a Rules Engine for business rules?	Yes	WebLink ID utilizes the Microsoft Business Rules Framework.
C. Does the solution use any Master Data Management?	Yes	If the DMV has a Master Data Management Engine, and wishes VALID to integrate with it, VALID will gladly integrate into the DMV's solution, otherwise VALID will utilize Semarchy's xDM product available to AWS solutions.
D. Does the solution use any Enterprise Content Management software?	No	VALID will integrate with the existing Enterprise Content Management solution the DMV has implemented. If the DMV needs an ECM, VALID can work with the DMV to select an appropriate ECM which will handle the DMV's content management needs from the DL/ID/EDL enrollment perspective.
E. Does the solution use any Case Management software?	Yes	BioLink ID has its own case management components for investigating potential fraud.
F. Does the solution use any Business Intelligence software?	Yes	The AWS solution we are proposing does include a BI engine that VALID utilizes for processing, analytics and reporting.
G. Does the solution use any Database software?	Yes	Both WebLink ID and BioLink ID have databases. WebLink ID stores the applicant's data and images used for card production, history and auditing information concerning the secure credential production. BioLink ID stores the applicant's facial images and select data to be used for fraud detection and investigation.
H. Does the solution use any Business Process Management software?	No	If the DMV has a Business Process Management Engine, and wishes VALID to integrate with it, VALID will gladly integrate into the DMV's solution.
I. Is this a browser based solution and if so what browsers do you support?	Yes	IE, Edge, Chrome, Firefox, Safari

J. Does the solution include an API for integration?	Yes	Both WebLink ID and BioLink ID have APIs for integration. WebLink ID consumes the BioLink ID API and vice versa. Both WebLink ID and BioLink ID support RESTful and SOAP APIs and are capable of others as necessary.
K. Does the solution use a facial recognition software and if so explain how this works? For example, are real- time or overnight results provided?	Yes	Facial recognition engine offered is real-time for verification (1:1) and can be real-time for 1:N, given a workflow which will facilitate the few seconds needed for 1:N verification
L. Does the solution provide tracking options and if so explain how this works?	Yes	The applicant request can be tracked from inception through mailing. WebLink ID has workflows able to display this information, or this tracking information can be accessed through an API.
M. Does the solution provide an automated process for DL/ID production, including standard processing times? If so provide high level description of this process.	Yes	The creation of the credential, once the application has been approved, will be accomplished in an automated process. When the application for a credential clears all gated issuance checks, data is routed automatically to the VALID card production factory, queued for production, printed, analyzed (inline automated QA) to ensure no transposition of applicant data or images occurred, attached to a mailer, placed into a properly addressed envelope, and sealed for mail pick up. This chain of processes is automatic. The estimated time needed for this process to run is 24 hours, however most issuance requests are processed the same day.
N. Are there automated and manual processes available for expediting distribution and providing special handling for DL/ID? If so explain how this works	Yes	Expediting a credential distribution request can be set via an API call, or manually during the production process prior to delivery to USPS. Expedited credentials are handled in separate print runs, changing the mailing portion of the distribution process. The print management software checks for expedited credentials between print runs to ensure timely handling of new expedite requests.

O. Is there an automated and manual processes available for stopping DL/ID from being produced and distributed - both before and after the transaction has been transmitted to the factory? If so explain how this	Yes	The VALID solution includes the ability to 'pull' a print job, or stop a particular record from being either printed or mailed, within the WebLink ID software. Operators with permissions can request a 'pull' or a stop, up until the card is queued for mail. If the card has been queued for mail, but has not been mailed, it can be pulled, but the window for that opportunity is time sensitive.
P. Does the solution have auditing functionality that exists within the system? If so describe how the data can be retrieved and/or reported on.	Yes	WebLink ID and BioLink ID log all access to any record by both users and system processes. These logs collect the access type, user, time and reason (if optional) for any change to an applicant's record. Furthermore, all historical information is saved and not overwritten, so changes to a record can be reverted as needed. Access to these logs is protected, and read only access is the only access permitted through the application. The logs can be sorted, filtered and reported against, and the reports can be exported in a user friendly format (PDF, spreadsheet, etc.)

Part 3: Functional Requirements

The table below lists the State's Functional Requirements. Indicate the "Availability" for each requirement for your proposed solution. Use the "Bidder Comments" column to provide any additional information or explanations.

A - Feature is available in the core ("out-of-the-box") solution.
D - Feature is currently under development (indicate anticipated date of availability in the Bidder comments column).
C - Feature is not available in the core solution, but can provided with customization.
N - Feature is not available.

Requirement Number	Functional Requirement Description	Availability
1	The Bidder shall describe the typical duration and process for the login process upon first boot and when switching between users. VT DMV's goal is to maximize efficiency and deter multiple users from sharing one (1) user session to minimize downtime.	**A**
Bidder Response	[redacted]	

2	The Bidder shall provide a list of search parameters available with the proposed system, for example: DL/ID number, First name, Last name, DOB, Zip Code etc. and should also include wildcard searches for partial data entry.	**A**
Bidder Response	WebLink ID's search fields are part of the custom workflow design, as such any field of information tied to an applicant's record could be used to find the applicant. Searches can be conducted against all identified fields on a workflow, or narrowed to a specific field manually. In the image below, if a particular field is not chosen, the value, with wildcards, will be looked up in each of the fields shown.	

	[redacted] **Figure 3: Advanced Search Parameters**	
3	The Bidder's solution shall provide both the ability for automated and manual flagging functionality. Flagging a record should trigger an automated email to the designated staff, preventing permanent card request from being sent to the central issuance facility until further review and approval by authorized users.	**A**

Bidder Response	WebLink ID supports both automated and manual record flagging. Flagging a record can send email notification to a defined group, as well as place that record into the appropriate gate-review container, which will be "addressed by the appropriate gate review team." The screenshot below shows the manual flag option. The flags that can be applied and at what steps they can be applied will be defined with the DMV during the design phase of the project.

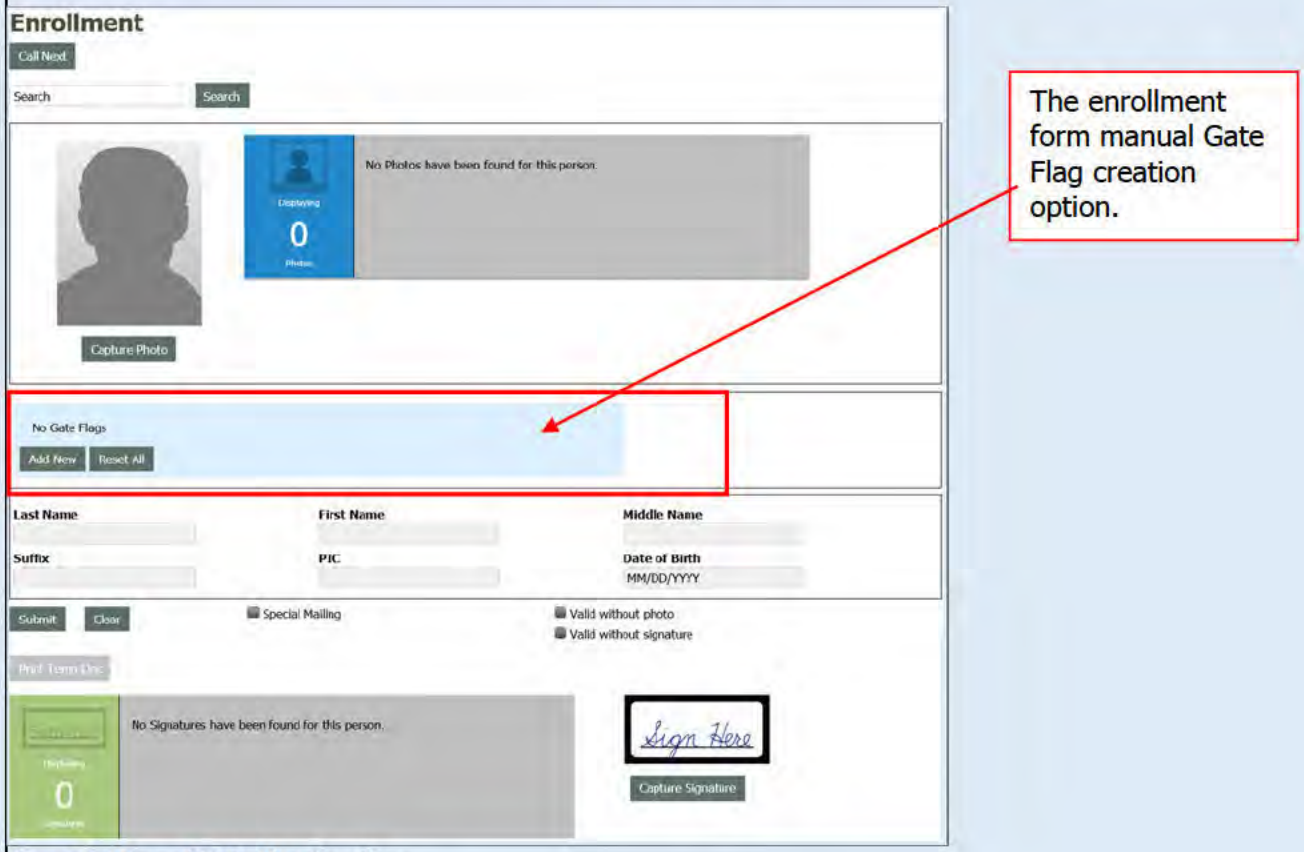


Figure 4: Manual Gate Flag Creation

	Certain flags like facial recognition failures, AAMVA portal failures, and data errors, will occur automatically and the applicant's record will be placed in the appropriate gate-review container for the appropriate team to handle. Below is an image of the gate-review containers (referred to as buckets) inside the WebLink ID application. Users with appropriate permissions can see these buckets, and work records appearing in each. **Figure 5: Buckets**

4	The Bidder's solution shall provide the ability to display messages and check boxes for customers to make selections such as, Organ donation, voter registration (yes/no Q's).	**A**
Bidder Response	Using the signature panel, which has a large color screen, the applicant can be presented a series of DMV-defined questions with either defined (check box or yes/no) answers, or a free form answer box where they would use the stylus attached to the signature panel to write the answer.	
5	The Bidder's solution shall provide an option allowing employees to select "Unable to Sign" for those applicants who are unable/not required to provide a signature.	**A**
Bidder Response	VALID commonly deploys a 'Valid without Signature' or 'Unable to Sign' check box, enabling the operator to bypass the need to collect the signature for those citizens unable to sign.	

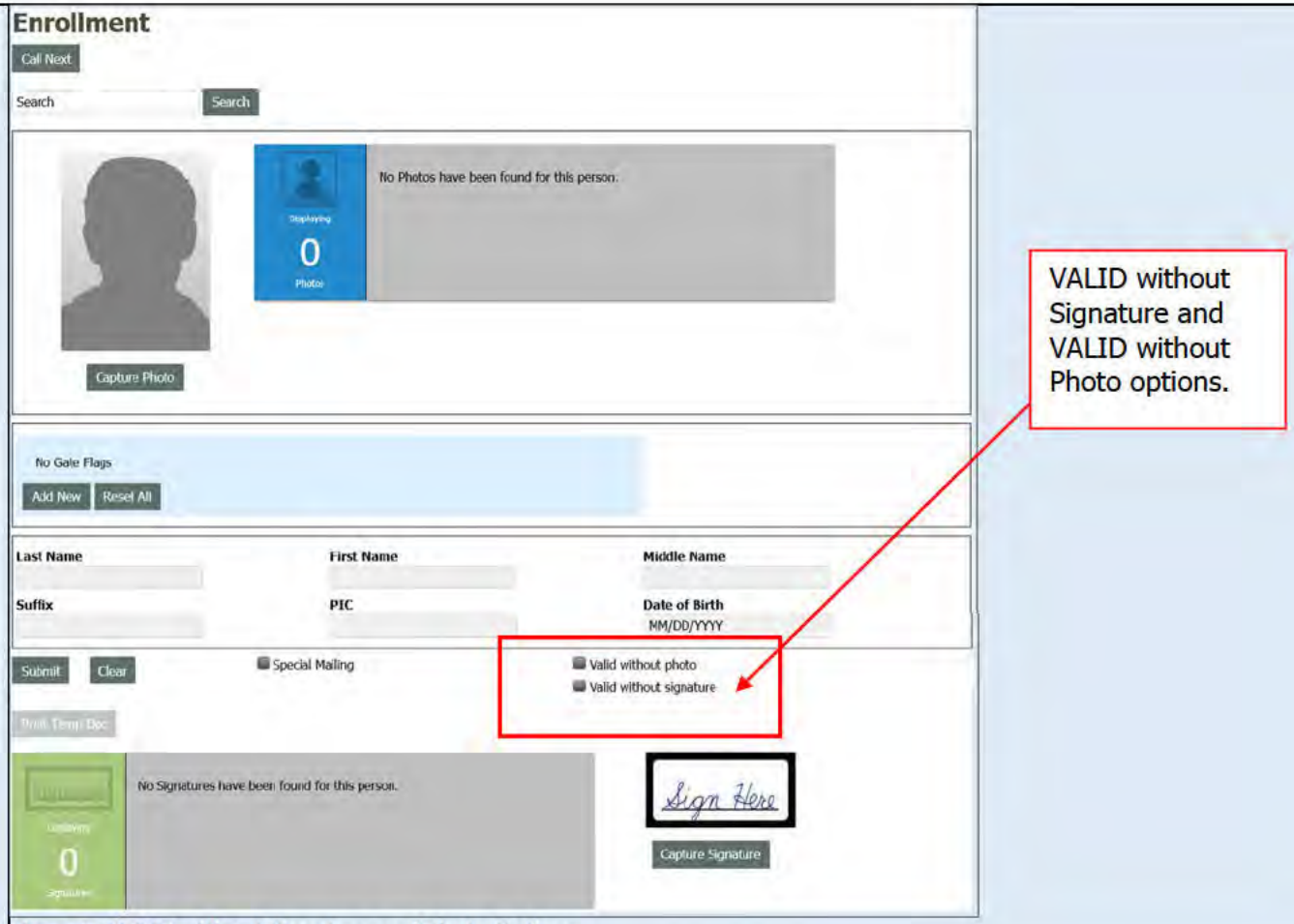


Figure 6: VALID without Signature and Photo Options

6	The Bidder's solution shall allow for images to be exempt from FR checks (i.e., When undercover DL/IDs are produced).	**A**

Bidder Response	VALID's solution enables images to be exempt from facial recognition events. The images can be prevented from enrollment into the engine, or prevented from ever being returned as a match. Vermont DMV can decide how it wishes to handle these exceptions. VALID's proposed solution supports both methods. Similarly, previously-enrolled images can be flagged to prevent being listed as a match, despite their previous enrollment. As an example, a new undercover police officer gets a fake ID made for his undercover credentials; however, he is previously enrolled in the system through his learners permit dating back to when he was a teenager. The teenager photo, and all subsequent photos, can be flagged as "invisible" so his cover is not compromised.	
7	The Bidder's solution shall initially enroll all existing legacy images for FR comparison prior to UAT.	**A**
Bidder Response	VALID understands that migration of legacy images and data is expected as part of a solution project. We will ensure the project plan includes migration of legacy information as a predecessor to UAT. VALID will migrate the data and images collected between initial migration (before UAT) and Go Live. We will ensure the project plan accounts for a differential migration, to cover the time between initial migration and Go Live, as a mandatory predecessor to Go Live.	
8	The Bidder must confirm that they will migrate all existing customer historical data and images from our legacy solution into the system prior to testing and again before going into production.	**A**
Bidder Response	VALID understands that migration of legacy images, and data, is expected as part of a solution project. We will ensure the project plan includes migration of legacy information as a predecessor to UAT. VALID will migrate the data and images collected between initial migration (before UAT) and Go Live. We will ensure the project plan accounts for a differential migration as a predecessor to Go Live.	
9	The Bidder's solution must provide both standard and ad hoc reporting capabilities; Bidders shall provide sample reports as part of their proposal as well as describe capabilities for ad hoc reporting.	**A**
Bidder Response	**Report Introduction** WebLink ID features multiple reporting methods that cover the needs of entry-level system users to more advanced power users. This includes two ad hoc reporting tools and canned reports. Access to reports is role-based, and is managed WebLink ID and BioLink ID reports modules. Figure 7 shows the WebLink ID reporting module. The reports supported can be generated on-demand or for scheduled generation.	

Figure 7: WebLink ID Reports Module

Tables below summarize the report types available and services used in creating them. For convenience, we have organized these reports into Standard Entry-Level, Mid-Level, and Advanced-Level.

Standard Entry-Level Reports	
Type	Canned
User Interface	WebLink ID which opens into an integrated SQL Server Reporting Services (SSRS)
Service	SQL Server Reporting Service (SSRS)
Database (DB)	WebLink ID SQL Server Database (or a separate reporting database, view, or Data Warehouse).

System operators access canned reports through a WebLink ID user interface available to them based on their roles. The reports in this list access the system through SSRS, a Microsoft service tool.

Figure 8 is an example of a canned SSRS report configuration page that would return a list of records that failed to enroll into the facial recognition engine. Results can be sorted and organized by data column headers, e.g., office location and issue date. The results can be viewed on the screen and can be exported for future reference in one of several formats.

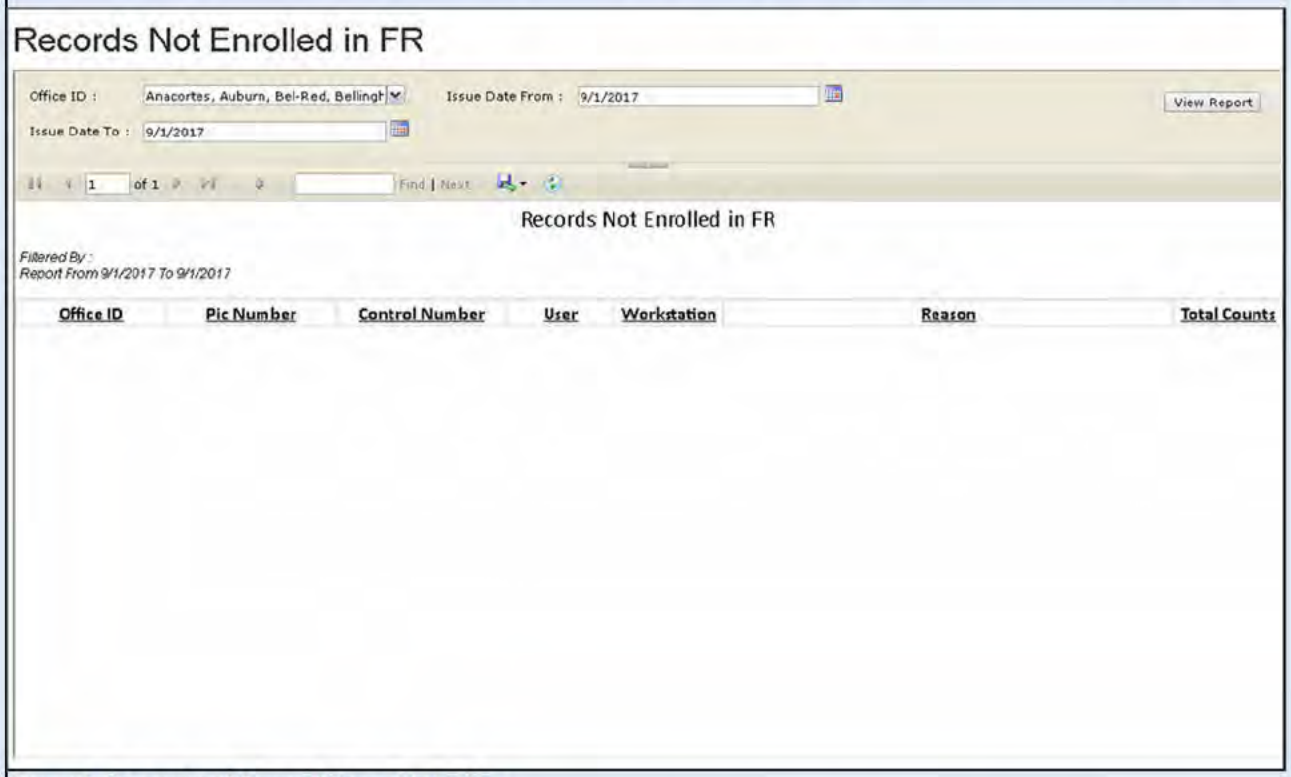


Figure 8: Example of Canned Report Interface

As shown in Figure 9, BioLink ID Reports Configuration, BioLink ID reports are similar in look and feel (columns may change from report to report).

Investigator: (Unassigned)

Date	Case ID	PIC	Control Number	Last Name	First Name	Middle Name	Date of Birth	Status
06/28/2016	30341	SMITHDD204PS		SMITH	JENNIFER	ELIZABETH	10/10/1980	Pending
06/29/2016	30343							Pending
06/29/2016	30344							Pending
06/29/2016	30345							Pending
06/29/2016	30346							Pending
06/29/2016	30347							Pending
06/29/2016	30348							Pending
06/29/2016	30349	6969696969	6969696969	Walls	Beau	M	09/08/1992	Pending
						Quantity		8

Investigator: VALID Administrator

Date	Case ID	PIC	Control Number	Last Name	First Name	Middle Name	Date of Birth	Status
06/29/2016	30350	1212121212	1212121212	McCrory	Sean		01/01/1990	Cleared
						Quantity		1
						General Summary		9

Figure 9: BioLink ID Report Configuration

Mid-Level Reports	
Type	Ad hoc
User Interface	WebLink ID which opens an integrated ad hoc tool based on Kendo UI (Excel pivot tables also supported)
Service	SQL Server Analysis Services (SSAS)
Database (DB)	VALID-developed multi-dimensional SQL Server Cube data warehouse

For these reports WebLink ID user interface utilizes Microsoft's SQL Server Analysis Services (SSAS) to mine data from a SQL Server Cube data warehouse. The report interface opens in WebLink ID, and users add filters on columns and rows of data of interest. The user interface for these reports does not support Structured Query Language (SQL) statements or scripts. The report toll supports an Excel pivot table for even more advanced mid-level power users.

Figure 10 shows the ad-hoc report user interface and an example of list of data fields available for customized filtering of the results. Typical data fields of interest to DMV include License Number, Transaction Type/Code, Issue Date, Expiration Date, Office (District, Region, HQ), User ID, Flags entered on record, Endorsements and Restrictions, License Indicators, Permit Expiration Date, Production Status, DOB, First Name, Last Name, Address, City, State, Zip code, One-Time Special Mailings, HGT, WGT, and Eye color.

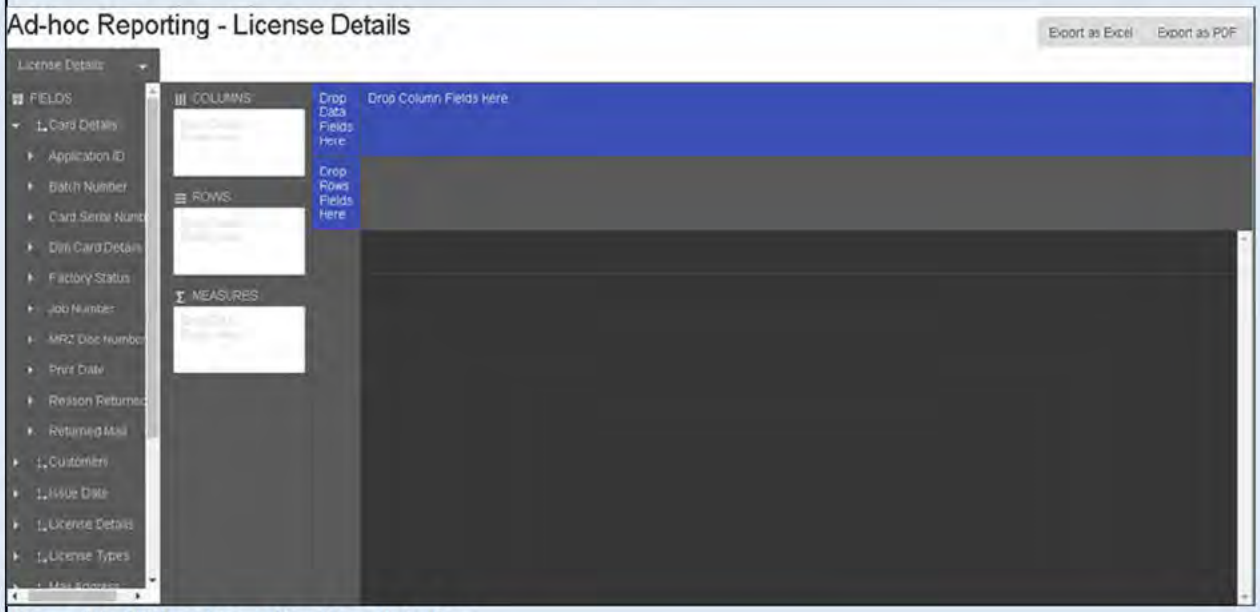


Figure 10: Ad-hoc Reporting User Interface

Advanced-Level Reports	
Type	SQL Query Editor (ad hoc)
User Interface	Accessed/authenticated through the WebLink ID user interface (opens a web browser tab for the Query Editor called SqlPad)
Service	IIS (or DMV-preferred web server platform) WebLink ID site
Database	WebLink ID SQL Server DB (or a separate reporting DB, view, or data warehouse

Advanced-Level reports can be created by directly executing SQL queries. VALID recommends DMV deploy a separate, optimized SQL Server database for advanced-level reports. This segments the production database from the reporting database if report users execute poorly structured SQL.

Users create and save queries for the specific reports of interest. The results can be viewed on the browser page and can be exported in one of several file formats. The Query Editor (Figure 11) provides a tool to create SQL statements and scripts to run against the reporting database. Tool functionality includes creating SQL, saving scripts, and sharing scripts with other users.

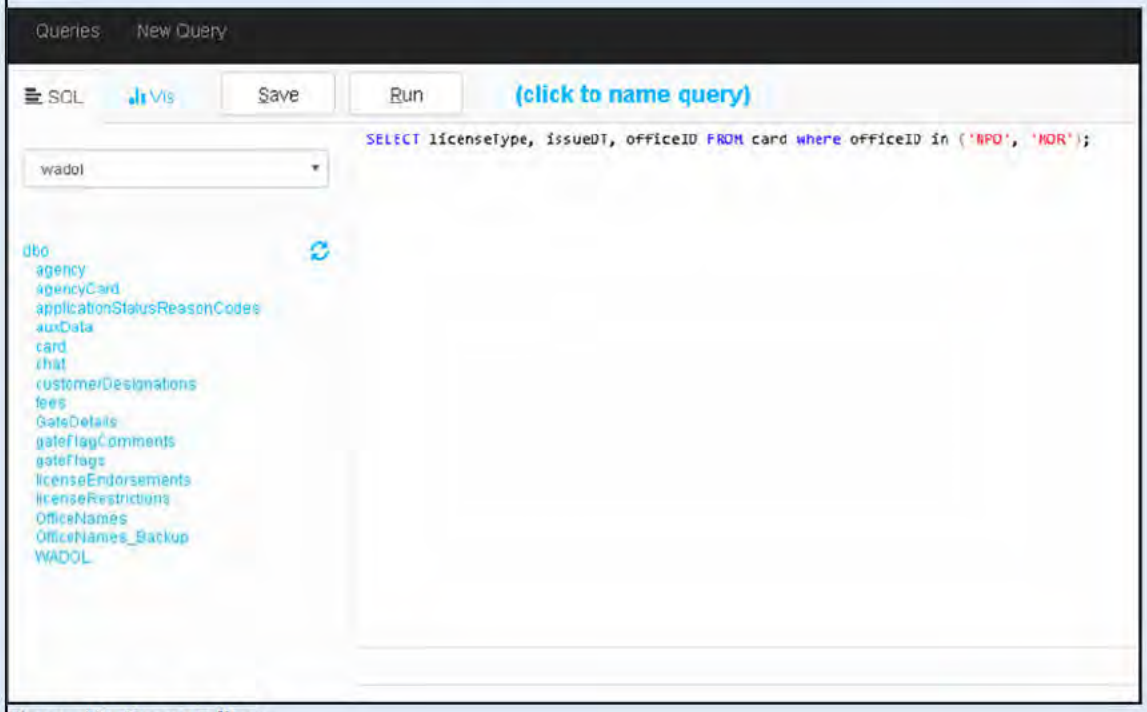


Figure 11: Query Editor

	Sample Report List VALID will expand WebLink ID standard reports to include DMV's canned reporting requirements. Below is a list of reports in a typical DMV implementation: • 1:1 Override Report • Agency ID Card Report • Enhanced Driver's License 5 Percent Audit Report • Enhanced Driver's License Renewal Statistics Report • Enhanced License Statistics Report • Identity Not Verified Report • Issuance Transactions Statistical Report • Original CDL CLP Documents Report • Records Not Enrolled in FR Report • Gated Issuance Check Detail Report and Gated Issuance Statistical Report **BioLink ID standard reports include:** • Internal Upload Image Report • External Upload Image Report • Enrollment Statistics Report • Case Resolution Report • Ad-Hoc Transactions Report • Investigation Cases by Queue Report

	Security [redacted] [redacted]

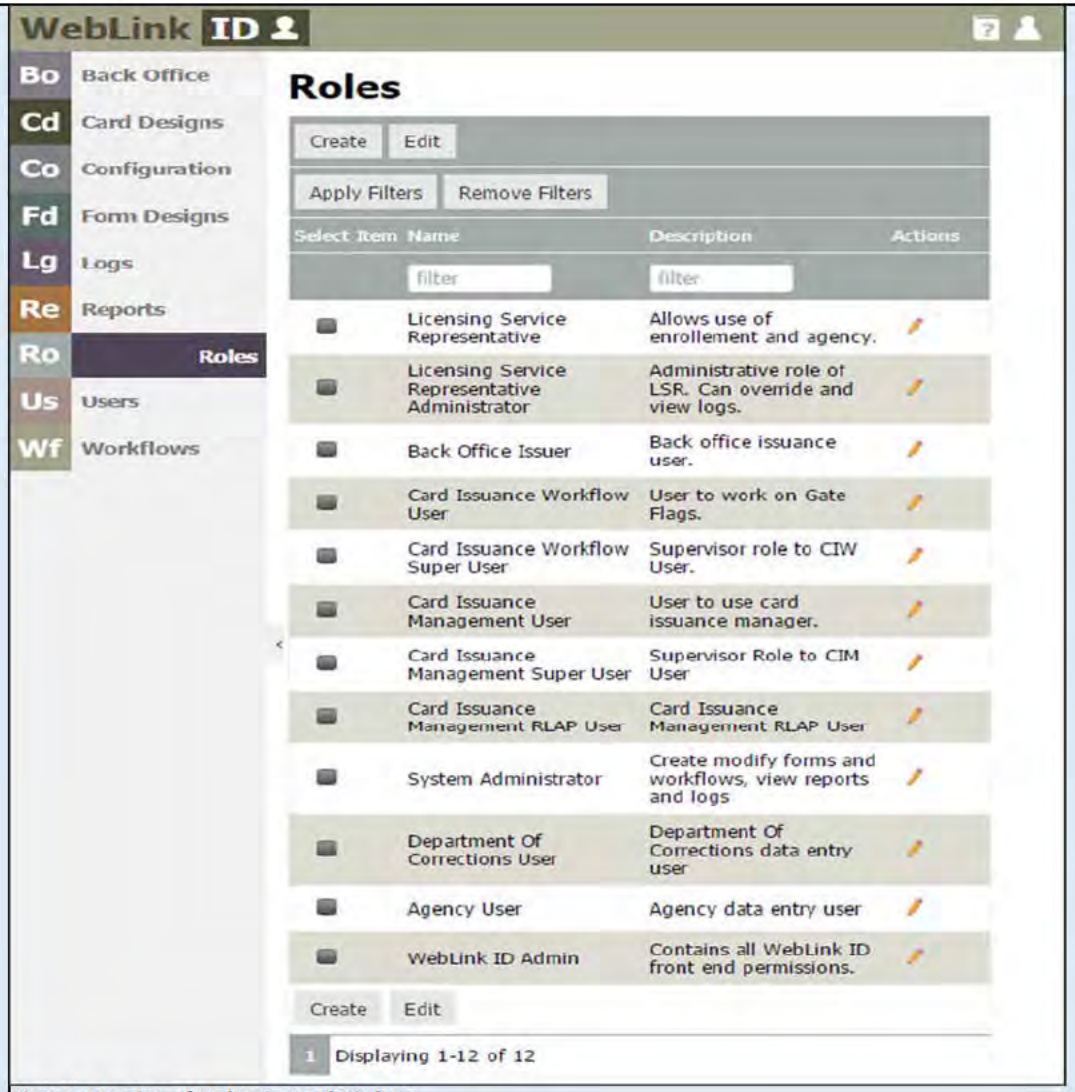


Figure 12: List of Roles in WebLink ID

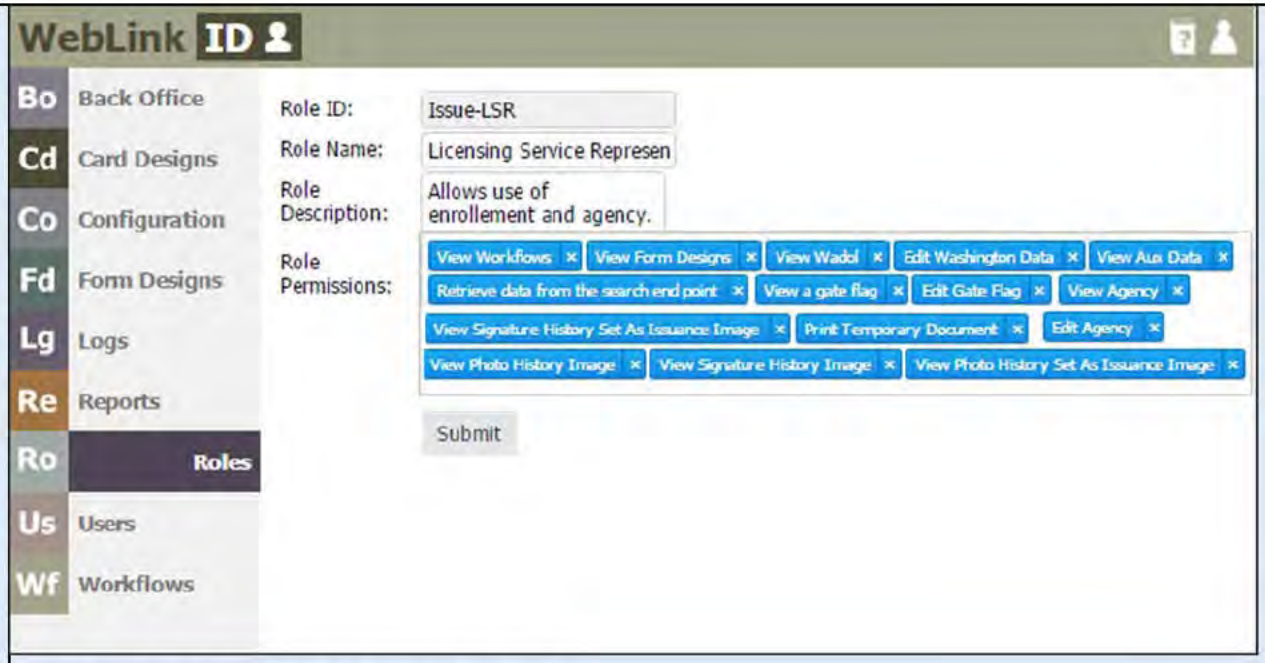


Figure 13: Permissions Given to a WebLink ID Role

Dashboard

VALID will create customized dashboards for DMV to display key statistics and project items of importance (IOIs).

The analytics tool is configurable and will be optimized for DMV's stakeholders (technical or system administrators, business users, and others). The dashboard portal supports System Dashboards and Personalized Dashboards with flexibility to optimize for the targeted audience and information sharing

Please refer to Figures 14 thru 18 for examples of customized dashboards.

Figure 14: Sample Project Dashboard Displaying Transactional Data

Figure 15: Sample Project Dashboard Displaying Overview and Reconciliation of Facial Recognition Activity

Figure 16: Sample Project Dashboard Displaying Transactional Data and Trends

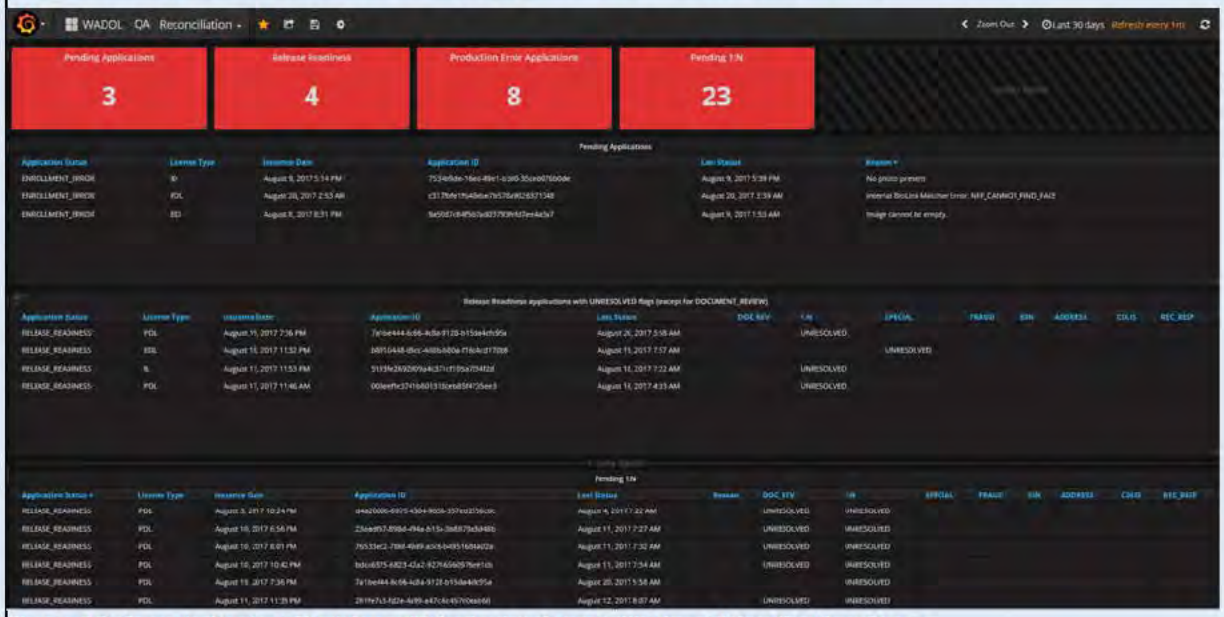
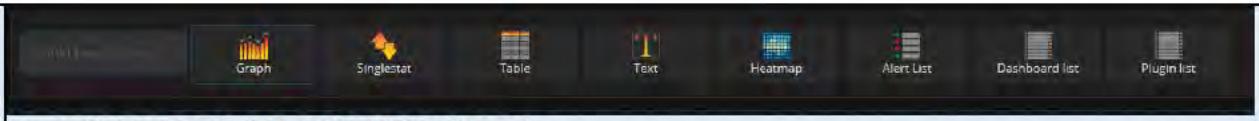


Figure 17: Sample Project Dashboard Displaying Reconciliation of Application Errors

	 **Figure 18: Toolbar to Add or Modify Dashboards** ***System Availability Report***	
10	The Bidder's solution must have the capability to produce interim (or temporary) DL/IDs at the time and point of sale. Format to be agreed upon during design phase.	**A**
Bidder Response	WebLink ID produces temporary documents (Figure 18) including DLs, IDs, CDLs, letters, and object-based (card, photo, and signature) printouts usable for investigations and law enforcement. These temporary documents can include any data from the application record including photo and signature images attached to the record (Figure 19). The Temp Doc service manages the data and Temp Doc templates organize the data into a printable display format. These templates can read data from the application record or utilize settings from WebLink ID's configuration settings. An administrator configures settings to create custom statements and/or reminders. The temporary document feature is accessible through a workflow forms and as a button on Object History Widgets. The temporary document templates are designed to look different from an actual DL/ID, so they cannot be confused with real credentials. WebLink ID temporary documents are generated as printable PDFs optimized for output on a laser printer. The ICW can be configured to connect to existing network printers to reduce additional required hardware and utilize shared resources.	

[redacted] [redacted]

This is your temporary document. Carry this with you until you receive your new one in the mail.

Your new card will show the last photo we took. If you don't receive your document in 30 days, please call us (360) 902-3900 or email Customercare@dol.wa.gov.

This Temporary Document Expires 10/28/2017

[redacted]

This document is not valid for identification unless accompanied by another piece of photo identification.

~ PERSONAL INFORMATION ~	
NAME	[redacted]
BIRTH DATE	02/05/1985
GENDER	F
HGT	5'- 06"
WGT	125
EYES	BLU
RESIDENCE ADDRESS	[redacted]

~ LICENSE INFORMATION ~	
DOCUMENT TYPE	IDENTITY CARD
LICENSE #	[redacted]
CONTROL #	[redacted]
ISSUE DATE	09/13/2017
EXPIRATION DATE	02/05/2023
RESTRICTIONS	NONE
ENDORSEMENTS	NONE
CLASS	NONE
ORGAN DONOR	NO
VETERAN	NO

~ MAILING ADDRESS ~	
Your license will be mailed to:	[redacted]

Figure 19: Temporary Document Without Photo

[redacted] [redacted]

This is your temporary document. Carry this with you until you receive your new one in the mail.

Your new card will show the last photo we took. If you don't receive your document in 30 days, please call us (360) 902-3900 or email Customercare@dol.wa.gov.

This Temporary Document Expires 10/8/2017

[redacted]

This document is intended to be used for driving purposes only. It is not valid for identification purposes unless accompanied by another piece of identification, like a recently expired driver license.

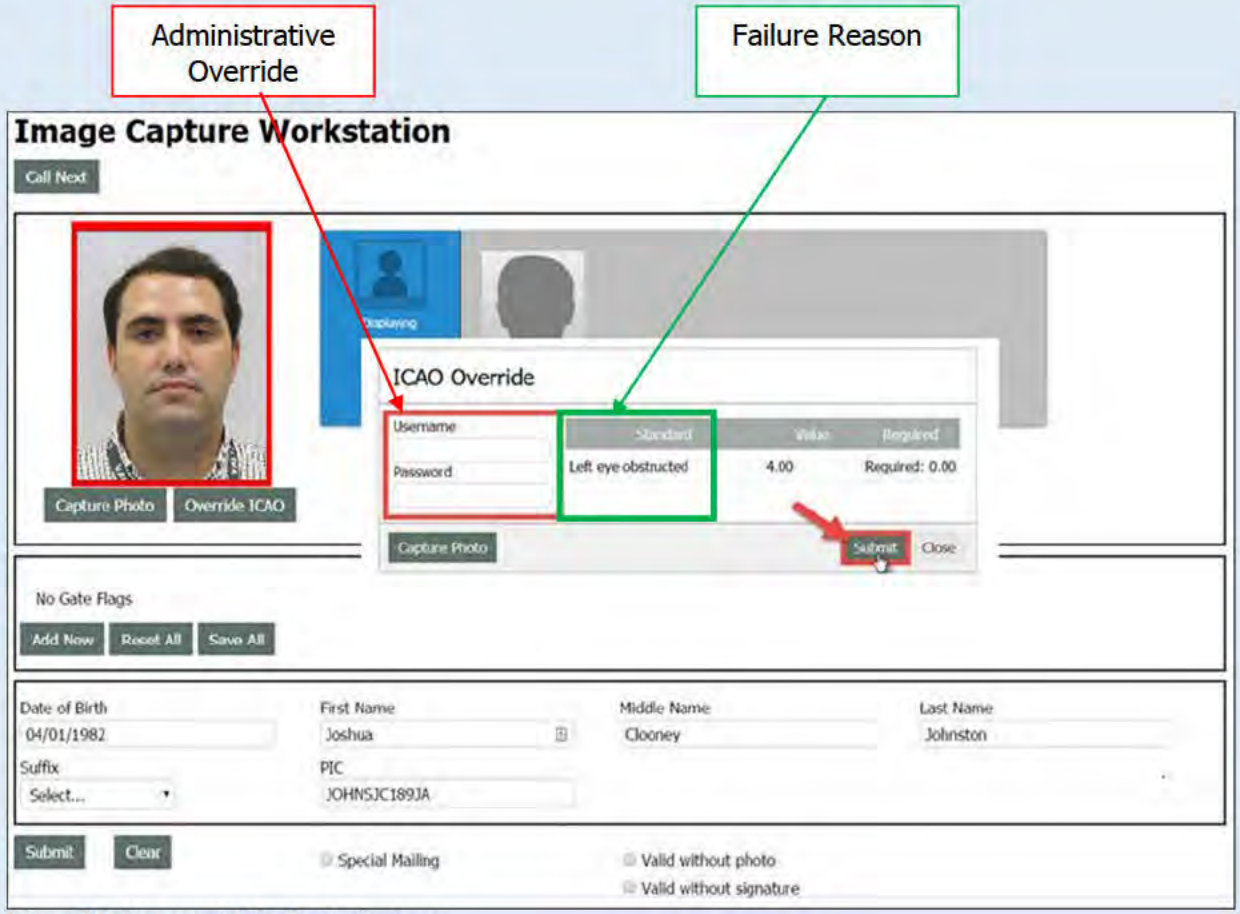
~ PERSONAL INFORMATION ~	
NAME	[redacted]
BIRTH DATE	05/18/1974
GENDER	M
HGT	5'-11"
WGT	140
EYES	GRN
RESIDENCE ADDRESS	[redacted]

~ LICENSE INFORMATION ~	
DOCUMENT TYPE	COMMERCIAL LIC
LICENSE #	[redacted]
CONTROL #	[redacted]
ISSUE DATE	08/24/2017
EXPIRATION DATE	05/18/2023
RESTRICTIONS	NONE
ENDORSEMENTS	L
CLASS	A
ORGAN DONOR	YES
VETERAN	NO

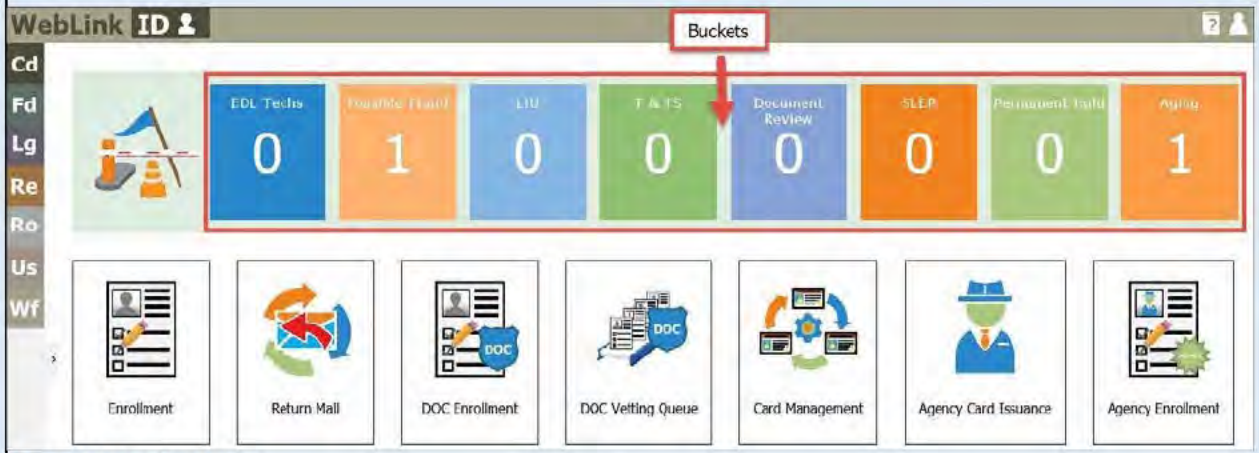
~ MAILING ADDRESS ~	
Your license will be mailed to:	[redacted]

Figure 20: Temporary Document with Photo

11	The Bidder's solution shall print and ship cards from the central issuance facility no later than three (3) business days following transmission of DL/ID card data from VT DMV to the central issuance facility. • Shipped means transferred to the shipping provider, not transferred to a third-party mail processing contractor.	**A**
Bidder Response	Approximately 90% of the jobs submitted to VALID's Card Personalization Facilities (CPFs) are completed and turned over to a Presort Bureau the same day they are received. The remainder are turned over the following day – a one-day turnaround. The Presort Bureau sorts the envelopes by zip code and commingles then with other innocuous mail. This yields the lowest postage possible while still satisfying contractual service level agreements. VALID has negotiated contracts with the Presort Bureaus used to perform this service the same day the envelopes are received. Custody of the envelopes is assigned to the U.S. Postal Service (USPS), who maintains an office inside the bureau's facility. The envelopes leave the facility on USPS trucks.	
12	The Bidder's solution shall use next day service for shipping cards that are not printed and shipped within three business days, at no additional cost.	**A**
Bidder Response	VALID will ship cards not completed within the required three-day agreement via an expedited shipping service such as UPS or FedEx for next day delivery at VALID's cost.	
13	The Bidder's solution shall provide renewal capabilities via the internet.	**A**
Bidder Response	VALID's solution includes a customer facing portal, we refer to as the 'Pre-Registration' portal. This portal can be used for a customer to request a DL/ID reprint (lost / stolen card) or renewal. In the event the card cannot be renewed remotely, due to DMV business rules, the applicant will be informed of the necessity to physically go to a DMV office for the renewal. The 'Pre-Registration' portal is a separate web server, located in a DMZ, such that it is located outside of the production portion of the DMV's network. If a DMZ is not available, VALID can work with the DMV to decide what solutions best fit their needs, including VALID hosting the Pre-Reg portal.	
14	The Bidder's solution shall inform the user on the screen when a photo failure has occurred. The error message must identify the cause of the failure in clear and non-technical verbiage.	**A**

Bidder	When using WebLink ID to capture a photo, the operator will be presented with an informative screen detailing the reason the photo captured was not acceptable. Please see a screenshot below showing an unacceptable photo capture, and what the operator is presented, as well as the option to override the error, which requires an administrator (or manager) login to facilitate.
Response	 **Figure 21: Unacceptable Photo Capture**

15	The Bidder's solution shall provide a camera system that provides maximum automation, minimum user involvement and capture high quality digital images.	**A**
Bidder Response	Cameras, signature pads, and ICW cases are available and effective in many space-saving form factors and WebLink ID is configurable to work with many different devices of varying sizes. This enables the selection of the best equipment for the space. Our capture tower houses both the camera and the flash element, conserving even more space. VALID produces or procures custom-configured backdrops of the client specified color and mounting method(s). The capture tower is attached to height adjustable legs by a free-pivoting fastener which enables the field of capture to be adjusted ranging 15° up or down from a level position. This makes taking photos of particularly tall or short subjects simple without a reconfiguration of the camera. It also helps capture children and individuals in wheelchairs. These features address the requirements of the American Disabilities Act (ADA). **Figure 22: Camera Tower**	
16	The Bidder's solution must provide multiple gates as specified by the VT DMV and must be scalable when additional gates or interfaces are necessary.	**A**

Bidder Response	WebLink ID is designed specifically for gated issuance; this ensures applications pass through the appropriate verification stages before sending the application to its final stage, either printing or termination. The gates and the staff authorized to process applications through the gates will be defined by DMV. In WebLink ID environment, applications in various stages of gated issuance appear in containers referred to as "buckets". The DMV staff will have access to these buckets in accordance with their defined roles. See Figure 23 for a sample of a bucket view.  **Figure 23: Bucket View** Each bucket shows the number of applications awaiting processing or investigation. Each bucket is mapped to a step in the gated issuance process and contain items that have failed gated issuance, such as applications that might have a 1:N facial image failure, requiring adjudication within the BioLink ID interface. The VALID project team will work with the DMV staff to identify the workflows needed, and define the gated issuance process required by DMV.

17	The Bidder's solution must allow users real-time access regarding the tracking of credential transactions that should include, but not limited to: • System process being performed • Credentials produced • Status of credential transaction • Date shipped • Process problems or failures • Data transfer failure	**A**
Bidder Response	WebLink ID includes a 'Card Management' workflow which enables users to view the status of existing applications. This powerful workflow allows access to any number of applicant data items, including but not limited to: • System Processes being performed • Credentials being produced • Status of credential transactions • Date shipped • Process or data transfer issues The image below shows a representation of the data visible on the 'Card Management' workflow, specifically the card history pane. Each data element is role-driven, so users with different permissions will see different data elements, ensuring only the data needed for the specific role is visible.	

Figure 24: Card Management - Card Life Cycle

Part 4: Non-Functional Requirements

The tables below list the State's Non-Functional Requirements. Indicate if your proposed solution complies in the "Comply" column.

Yes = the solution complies with the stated requirement as standard functionality with minimal configuration of base product.
No = the solution does not comply with the stated requirement. Or would require customization of the software. Customizations must be quoted separately
N/A = Not applicable to this offering

Describe how the requirement is met in the "Bidder Description of Compliance" column.

4.1 Hosting

ID #	Non-Functional Requirement Description	Comply	Vendor's Description of Compliance
H1	Any technical solution must be hosted in a data center.	**Yes**	VALID's solution will be hosted in multiple data centers. The primary applications for enrollment, WebLink ID and BioLink ID, will reside in an Amazon Web Services, Government Certified, Data Center. The Card Production applications, Factory Allocation Manager, and Job Control System will reside in VALID's certified data centers. Please refer to Part 4, Questions 1-4, for more detailed information on the data centers planned.
H2	Any hosting provider must provide for back-up and disaster recovery models and plans as needed for the solution.	**Yes**	VALID's proposed solution includes both the ability to back up and recover data, as well as disaster recovery environments. Both the AWS hosting provider and VALID's own data center support backup and recovery hardware and procedures, the VALID procedure is available upon request. The procedure for backup and restoration of the AWS environment will be defined during the project planning phase to ensure the DMV is accepting of the process; and we will have the ability to test and verify the procedure defined. The solution design proposes the use of multiple sites and regions to ensure the environment is capable of continuing operation in the event of a disaster at any one site. VALID proposes that the DR sites and environments are not only used in an emergency, but are

			exercised daily in production. This is a key benefit of VALID's solution, whereby we make sure that the disaster recovery environments are truly real-time, fault-tolerant production locations. In the event of a disaster, our process of utilizing the disaster recovery site as a secondary production environment eliminates the downtime often needed to convert a disaster recovery site to production.
H3	Any hosting provider will abide by ITIL best practices for change requests, incident management, problem management and service desk.	**Yes**	VALID's processes for change requests, incident management, problem management and service desk for support follow ITIL best practices, in compliance with ITIL v3. Fundamentally the ITIL best practices extend to customer account management, product development and other internal VALID processes. VALID did not initially set out to adhere to ITIL processes, as our solution needed to provide solid service and it predated ITIL. However, what VALID has developed for change, incident and problem management is in full alignment with ITIL's described best practices. **Service Strategy:** Regardless of the specific focus, VALID recognizes that the services we provide are indeed the greatest asset we can provide to our customers. Our strategy for service provisions is to fully accommodate the service request. Initially, we work with each client to define requirements, constraints, operational changes, and risks to develop a plan for solving the customer request. **Service Design:** We firmly believe the best solution is a solution which keeps the customer's objectives in focus. We work our design to ensure it meets the customer's stated and agreed upon objectives. **Service Transition:** VALID sees this as part of the implementation phase of any solution. Transition cannot occur smoothly if the design does not

			meet the requirements, and if the client is not prepared for the transition, or if the transition is rushed. A transition can be as simple as an implementation of a bug fix, or as complex as the replacement of a complete driver's license solution. Neither will occur smoothly if requirements are not met (the bug isn't fixed), the solution is not tested, and the impacted customers are not trained or notified properly of the transition. **Service Operation:** Post transition, day-to-day operations must be managed with acuity and transparency, ensuring the operations themselves are performing within the defined boundaries for acceptable performance. Service calls, development times, implementation schedules are all monitored for adherence with the SLAs, and measured for improvement, and reported through the organizations requiring insight into performance. **Continual Service Improvement:** Without a proper Service Operation, the ability to tune and improve a process becomes increasingly more difficult. Services can be improved only if they are continually measured. As such, service operation plays as important a role in service improvement as customer feedback. VALID will distribute customer feedback requests, as well as constantly monitor and analyze the solutions in place for areas of improvement.

4.2 Application Solution

A1	Any solutions vendor must provide for the backup/recover, data retention and disaster recovery of a contracted/hosted application solution.	**Yes**	Regardless of where the environment is hosted, at VALID's data center or AWS government data center, VALID will be responsible for ensuring: 1) Scheduled backups occur 2) Integrity of the data backed up 3) Restoration of the data, should it be needed 4) Recovery from a disaster 5) Retention and archival of the data, in accordance with the State's data retention and archival process VALID will work with the DMV to revise existing VALID procedures and to report the above items to ensure they meet the DMV's standards and needs.
A2	Any solutions vendor must provide for application management and design standard of all technology platforms and environments for the application solution (Development, Staging, Productions, DR, etc.)	**Yes**	VALID understands and agrees that it will provide application management for the proposed hosted solutions. VALID's proposed solution includes monitoring and analytic tools which will facilitate the management and improvement of all the proposed environment's (Prod, QA and Dev) application(s) performance by fine-tuning configuration, processes and resources required. VALID will share with the DMV the methods of our development and design standards utilized for our application development, during the contract phase of the project. Performance reports and enhancement options will be distributed in accordance with a defined maintenance SLA, for discussion with the DMV prior to any fine tuning or enhancements being implemented. In accordance with VALID's 'step-up' promotion process (discussed in depth, in Part 4, section 4 below,) implementation of any enhancements, maintenance or updates, will occur first through the Dev or QA environments, and once testing has cleared, promotion to

			production can occur. These updates will be conducted by VALID, and can be tested and verified by DMV.
A3	Any solutions vendor must engage the State of Vermont using Service Level Agreements for system and application performance, incident reporting and maintenance.	**Yes**	VALID agrees that the use of Service Level Agreements (SLAs) are beneficial to both parties, and VALID will work with the DMV during the contract phase to mutually agree on the SLAs to cover the solution's performance, issue tracking, maintenance and update processes. VALID has provided an SLA sample in Attachment 8.
A4	The State owns any data they enter, migrate, or transmit into the solution and the vendor shall allow the State to pull or copy this data at any time free of charge.	**Yes**	VALID acknowledges that all data collected, migrated or transmitted is the property of the State of Vermont. VALID will enable the DMV to access or copy any or all of the data from the various environments, as they require it, at no additional cost. VALID will work with the DMV's IT team to ensure they have access to, and the ability to pull or copy the data. VALID anticipates the DMV staff will be able to test data transfer during the Systems Integration Testing (SIT) of the project. VALID will provide to the DMV documentation regarding how to access and copy the data, as well as provide training on how this can be executed.
A5	As a contract deliverable, the vendor shall supply an up-to-date data dictionary that represents all data respective of the solution it will provide. The data dictionary must contain the following attributes: 1. The technology (RDBMS platform) that hosts the data source, i.e. Oracle, SQL Server, MySQL, DB2, etc. 2. The location where the data source is hosted 3. Thorough descriptions of each table in the data source 4. Thorough descriptions of each column within each table in the data source. In addition to business definitions, column descriptions must include the following detail: schema names; file group names (if applicable); data types; lengths;	**Yes**	VALID will provide a data dictionary for each environment database, and application interfacing with the databases. The data dictionary will contain definitions of all databases, data tables, data elements stored or used regardless of if the data is customer related, transaction-related, or meta data collected during the full lifecycle of credential. The dictionary will include the location, both logically and physically of the data elements. The data dictionary will define the data element, the application(s) which utilize the element, and any element's possible schema or values as well as any data element constraints, such as data type, length, key relationships, default values, validation criteria and formatting, calculation formulas, aggregations applied, and NULL ability. Definition of file based data sets utilized by WebLink ID will be part of the data dictionary with articulate definition of each field in the file based schema.

	primary and foreign key constrains; applied formatting; applied calculations; applied aggregations; NULL-ability; default values.		The data dictionary will be part of the Solution Design Document (SDD) set, and will be a living document. As changes are made to the proposed solution, the SDD and data dictionary will be updated and circulated in accordance with the agreed upon SLA for update and change control documentation.

4.3 Security

As a solution vendor, you must have documented and implemented security practices for the following and have a process to audit/monitor for adherence. Indicate "Yes" or "No" in the "Comply" column or "N/A" if the requirement is not applicable to this offering. Use the "Vendor Description of Applicable Security Processes" column to describe how you meet the requirement and the "Audit/Monitor" column to indicate how you monitor for compliance.

ID #	Non-Functional Requirement Description	Comply	Vendor's Description of Applicable Security Processes	Audit/Monitor Process
S1	Input validation	**Yes**	The system performs both syntactical and semantic input validations on all API calls and methods. VALID applications validate data provided by the client before the request processes: parameters, URLs and HTTP header including cookie names, and more. Additionally, its validation code whitelists only acceptable characters. The code also limits the size of input to reasonable values for a respective field, and converts it to a standard encoding scheme before it applies filters.	[redacted] to submit its applications to security

				[redacted]
S2	Output encoding	**Yes**	The system performs output encoding for HTML and URL to prevent for Cross Site Scripting. The easiest way to execute a cross-site request forgery (CSRF) attack involves performing a sensitive operation on a GET request. A common scenario embeds an image in an email with the image source being the malicious GET request. VALID mitigates these types of attack by not using the GET method for any operation other than returning data. Sensitive operations use the POST, PUT, and DELETE methods which cannot be used in a link or image. VALID further mitigates more complicated CSRF attacks that require user interaction by validating the HTTP referer header sent from the browser. VALID blocks the request if the referer header does not contain the same Fully Qualified Domain Name (FQDN) as the application. Also, VALID software uses REST operations which require a JavaScript Object Notation (JSON) request body to update or	[redacted]

			create data. It cannot be sent from HTML forms alone, and the web browser's cross origin policy prevent cross-domain ajax requests.	
S3	Authentication and password management	**Yes**	VALID applications are not available to the public. All pages and resources require authentication which is enforced on the server. The solution never features any "remember me" functionality. VALID applications use only HTTP POST requests to transmit authentication credentials from client users, and utilize the OAuth 2 framework for service to service authentication. There are options concerning how VT DMV applications authenticate to VALID systems including API keys. 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.	[redacted]
S4	Session management	**Yes**	The system uses the native ASP .NET session management implementation that maintains session variables on the server. The solution relies heavily on the server and framework's session management functions; it recognizes only these session identifiers. The session timeout is configurable in the VALID system. VT	[redacted]

			DMV and VALID will establish a session inactivity timeout that is as short as possible, and balances risk and business processes. The applications set the "secure" attribute for cookies transmitted over an TLS connection. VALID supplements standard session management for sensitive server-side operations through strong, per-session random tokens which helps prevent CSRF attacks.	[redacted]
S5	Access control	**Yes**	VALID applications store no data on the client. All requests require authorization including those made on the server. The applications are role-based. Authenticated users perform authorized actions by role(s) which is a collection of application permissions. Roles grant access to services and application data to authorized users only. The application logic and workflows conform and comply with business rules established by VT DMV.	[redacted]

				[redacted]
S6	Cryptographic practices	**Yes**	VALID applications hosted in the Amazon AWS GovCloud utilize the AWS Key Management System (KMS) which handles the cryptographic functions and key and certificate management. It is an HSM-based (Hardware Security Module) solution to protect and control keys that encrypt VALID application data, and protect form man-in-the-middle attacks. The database features two-tier encryption key architecture. The tablespace keys are managed using the Key Management Interoperability Protocol (KMIP) standard and the master encryption key is stored in AWS Key Management Service (KMS). It enforces clear separation of keys from encrypted data and automates key rotation and storing historical keys.	[redacted]
S7	Error handling and logging	**Yes**	The system captures global non-handled errors in generic messages, and logs the exception details for future analysis. VALID applications do not disclose sensitive information in error responses, including system details, session identifiers, or account information. VALID restricts log access to only authorized individuals. Additionally, VALID logs do not store sensitive information, including	[redacted]

			unnecessary system details, session identifiers or passwords. VALID logs all authentication attempts including date/time and IP address, the log attempts include failures. All VALID application services perform detailed system-level logging. VALID accumulates the data into an Elasticsearch warehouse with an analytics and monitoring tool that creates incredibly rich visualizations of system log data, and the portal features real-time alerts with configurable thresholds which will notify VALID and VT DMV system admins if there are system issues. Data and VT DMV will create retention policies for the detailed, system-level log data.	[redacted]
S8	Data protection from unauthorized use, modification, disclosure or destruction (accidental or intentional).	**Yes**	VALID applications encrypt data at rest and in transit, and GET requests do not include sensitive information. The applications store no artifacts on the client. The database servers reside in a private subnet, and the application/API servers also reside in a private subnet in the GovCloud Virtual Private Cloud (VPC), and neither subnet is accessible to the internet. The application servers only accept requests from web servers (and database servers only accept requests from application servers) through routing, Network	[redacted]

			Access Control Lists (NACLs), and security groups. VALID employees at time of hire and on an annual basis sign a computer use policy. This policy reviews unauthorized, modification, destruction and disclosure of data. The employees are required sign that they have read and understand the Computer Use Policy.	[redacted]
S9	Communication security	**Yes**	The VALID applications communicate to the client through TLS 1.2/HTTPS protocol only. The public load balancer resides in the only public (internet facing) subnet within the VPC. Its rules create an HTTPS listener to handle secure traffic only; it features other security configuration which protects it from bad actors and forwards requests to the AWS Web Application Firewall (WAF) layer. The WAF layer is a private subnet and does not face the internet. The WAF servers only accept requests from the public Elastic Load Balancer (ELB) through routing, NACLs, and security groups. It receives requests from the load balancer and applies additional filtering. For example, it requires an originating IP range from the whitelisted VT DMV network. The request is forwarded to the web server only if it meets all rules and conditions.	[redacted]
S10	System configuration	**Yes**	VALID staff apply security and maintenance patches and upgrades at the operating system, web server, application server, and database	[redacted]

			server levels for the guest servers operating VT DMV applications. The host servers (the Amazon infrastructure and virtualization layer itself) are maintained and patched by Amazon automatically. Development and QA environments are isolated from the production network. Only authorized production environment operations engineers have access to the production environment in a least privileged methodology. VALID operates a sophisticated continuous integration environment with its Git-based repository and a rigorous configuration management quality assurance (CMQA) process. It manages software changes and configuration changes to various environments.	[redacted]
S11	Database security	**Yes**	VALID applications use strongly typed parameterized queries and variables. The database servers only accept requests from the application servers. And the database does not contain any default database administrative passwords or unnecessary default schema or content. The database features two-tier encryption key architecture. The tablespace keys are managed using the KMIP standard and the master encryption key is stored in AWS KMS.	[redacted]

				[redacted]
S12	File management	**Yes**	The system uses several techniques to manage files correctly: low privilege users, strict user permissions, OS and web server paths isolated from application paths, input data validation to avoid path traversal, and more. VALID applications limit file types that can be uploaded to only those types that are needed for business purposes. Users upload files for scanned documents, photos, and signatures only (.jpg, .png, .tiff), and those are stored in the database (cannot be executed). The application removes anything that is not image data, and it rejects the file if it is not a valid image type or it exceeds a specified size.	[redacted]
S13	Memory management	**Yes**	VALID utilizes industry-standard web technologies to build its applications including .NET. The system uses the native .NET Framework Memory Management implementation, and avoids using non-managed memory pointers to prevent memory	[redacted]

			leaks. Additionally, the VALID application code truncates input strings before the copy and concatenation functions, and it avoids the use of known vulnerable functions such as printf, strcpy, and more.	[redacted]
S14	Fraud detection	**Yes**	VALID deploys Juniper IDP technology for its intrusion detection and intrusion prevention solutions. Card production data traverses the VALID server, HSA DMZ, and HSA networks. Juniper monitors the network and firewalls throughout the environment. VALID also prefers the IDS/IPS solution at the AWS Web Application Firewall (WAF) layer in the hosted GovCloud environment. VALID system analysts and infrastructure team monitor the intrusion detection system and intrusion prevention system daily. The system logs odd activity immediately and VALID investigates it. Additionally, the Security Information and Event Management (SIEM) alerts the team through email regarding events that require attention or investigation.	[redacted]

				[redacted]
S15	General coding practices	**Yes**	SHA256 Hashes for external binaries (exes) are kept in a repository managed by the release engineering team and executables are verified before being packaged into the release installer. All third-party and locally developed interpreted libraries are kept in a local private repository, and all VALID applications use services oriented architecture (SOA) built with modern web technology frameworks, languages, and libraries. Specifically VALID built its software applications using a microservices architecture which provides ample opportunity to repurpose tested and managed code rather than creating new code for common tasks.	[redacted]
S16	POA&M management	**N/A**	VALID has not identified any security weaknesses in our proposed VT DMV solution that require corrective action pursuant to the Federal Information Systems Management Act of 2002 (FISMA) that mandates a plan to track and plan resolution of information security weaknesses.	Not applicable.
S17	Risk Assessment Practices including but not limited to	**Yes**	VALID has several compensating controls in place to monitor risk. It conducts internal and	[redacted]

	vulnerability assessment and pen testing		external penetration and application testing annually, or after significant changes to the network and all findings are remediated. VALID conducts an internal network vulnerability scan quarterly and all findings are remediated. VALID also contracts PCI-qualified scan vendors to conduct quarterly external vulnerability scans.	[redacted]
S18	Incident response planning and testing	**Yes**	VALID annually tests its incident response plan concurrently with its Business Continuity Test. All documentation is updated at that time and approved by the executive committee.	[redacted]

				[redacted]
S19	System Security Plan delivery	**Yes**	VALID has extensive security processes in place, for both physical and logical security, to ensure the safeguarding and integrity of our data, infrastructure, factories, network, and computer systems. The purpose of VALID's System Security Plan is to provide an overview of the security requirements of our entire system in a comprehensive manner, and to describe our controls, define responsibilities and expected behavior of all individuals who access the system. Our plan documents via a structured process how we have planned thorough, cost-effective security protection for our entire system and all it contains. It is a living document that is periodically reviewed and updated, reflecting input from all our management team with security responsibilities as well as information owners and system operators. Our System Security Plan covers roles and responsibilities assigned by the CISO, security training, risk management, incident response plans and procedures and assessments, forensic investigation guidelines, data security both in motion and at rest, data compromise, network security, security testing and monitoring	VALID actively monitors and tests its security system, as follows: • Performs quarterly external network vulnerability scans using an Approved Scanning Vendor (approved by PCI SSC) • Performs internal and external network vulnerability scans at least quarterly and after significant changes (installations, firewall adjustments, and changes in network topology • Take immediate corrective action for any vulnerabilities • Perform internal and external penetration tests annually at each facility • Extensively make use of intrusion detection systems (IDS) for network traffic analysis • Monitor all traffic at the personalization network

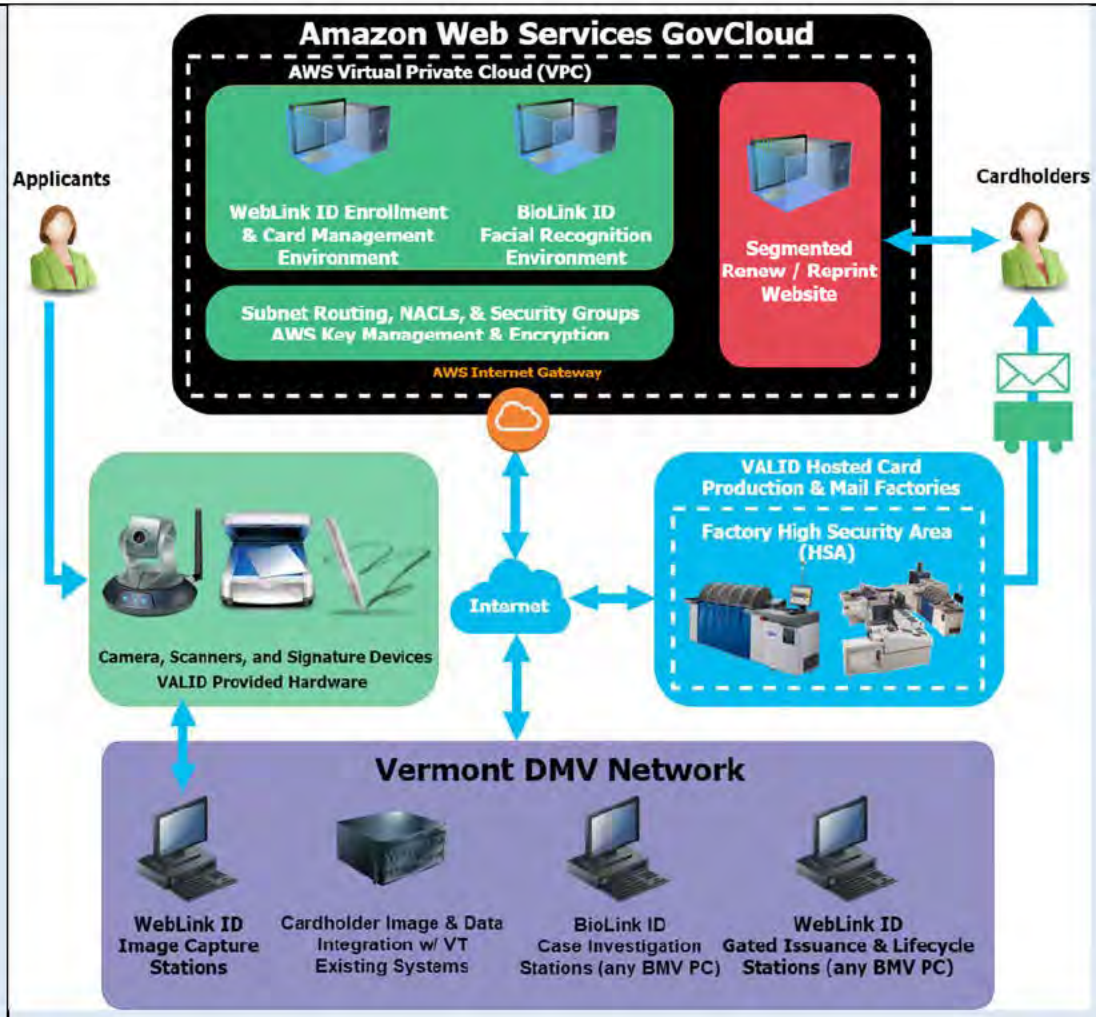
			including penetration testing, configuration management, and system access control.	perimeter as well as at critical points inside the network

4.4 Other Non-Functional Requirements

For each requirement listed, indicate if and how you comply or type "N/A" if it is not applicable to your offering.

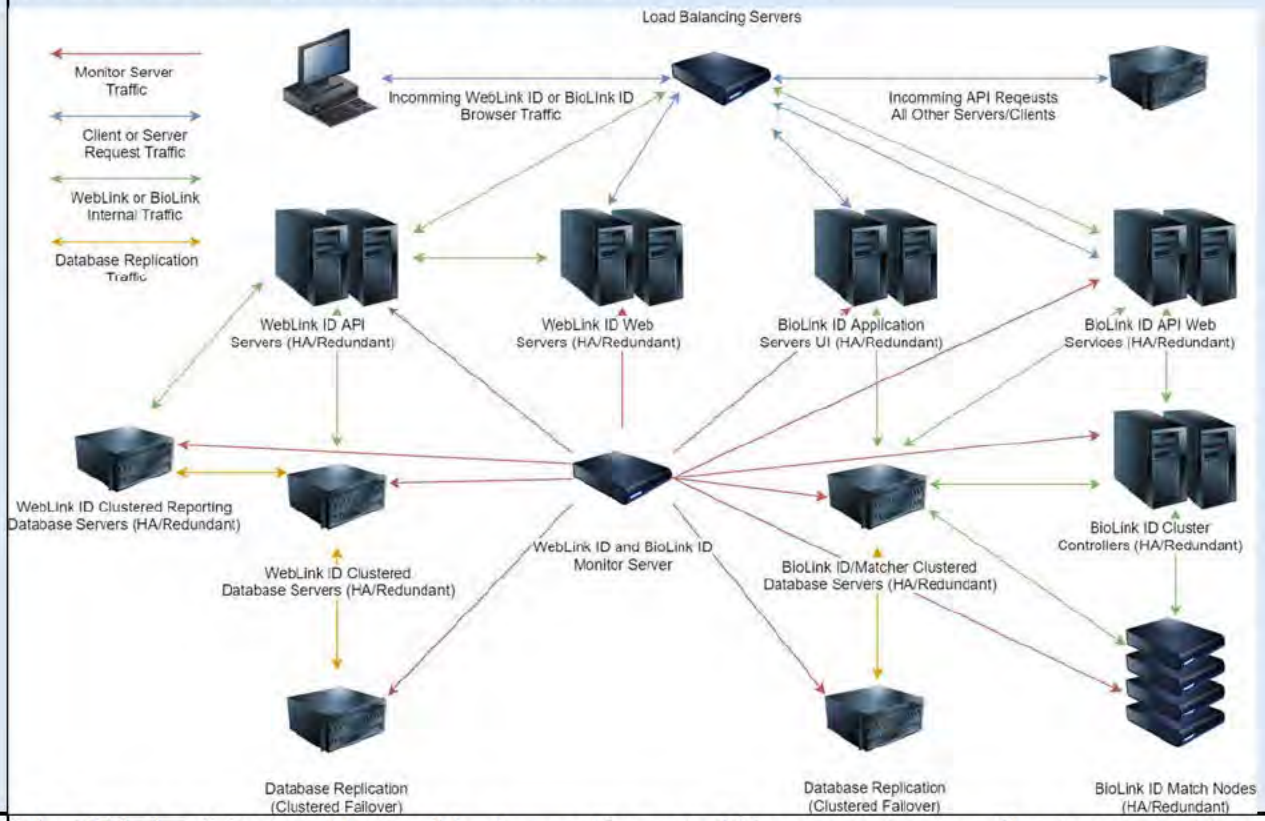
Requirement Number	Non-Functional Requirement Description	Comply
1	Bidders shall propose a solution that has the ability to securely interface with the DMV's Enterprise Data Management system and customer, credential, and transaction data.	**Yes**
Bidder Response	VALID's proposed solution will utilize WebLink ID's service oriented architecture and microservices to communicate transactional data with the DMV's Enterprise Data Management system through real-time web services or API connections. WebLink ID 2.0 was designed to facilitate this type of communication and data sharing, WebLink ID and BioLink ID communicate naturally using this type of architecture.	
2	Bidder shall propose a solution that has the ability to securely interface with external systems such as: Problem Driver Pointer System (PDPS), Systematic Alien Verification for Entitlements (SAVE), Commercial Driver's License Information System (CDLIS), Social Security Online Verification (SSOLV).	**Yes**
Bidder Response	WebLink ID can communicate with both the State's existing PDPS, SAVE, CDLIS, and SSOLV implementations. WebLink ID can also communicate with the AAMVA web services portals, should the state wish to remove its current mainframe engine. VALID was the first company to test and integrate with AAMVA Web Service Portals, instead of the traditional UNI CICS method of connection. WebLink ID consumes AAMVA web service portals for SAVE and SSOLV, as well as US Passport, and can utilize the existing AAMVA UNI CICS integration method for CDLIS and PDPS. As AAMVA opens more web service portals, WebLink ID will support those also, including State to State License verification. VALID will work with the DMV to define which integration method is preferred and how WebLink ID will communicate with the mainframe, should the State wish to keep these integral verifications static.	
3	The Bidder's proposed solution software shall support the current 64-bit Windows 10 operating system.	**Yes**
Bidder Response	WebLink ID and BioLink ID are web-based platforms with run within browsers on Windows 10 64 bit. The communication drivers for WebLink ID to talk to local hardware (Cameras, Signature Panels, etc.) are tested and certified to run on Windows 10, 64bit.	
4	The Bidder's issuance solution shall be compatible with Microsoft SQL Server and Windows Server 2016 R2.	**Yes**

Bidder Response	WebLink ID can output its data to a MS SQL server real-time. Part of the design of WebLink ID's architecture is to facilitate real-time data communication as the client requires. As transactions occur within the system, while they are stored in the WebLink ID database, they can also be written to any database, as needed or required. WebLink ID, when hosted, will utilize the AWS database designed for cloud based solutions, for its own data, processing and optimization. Both WebLink ID and BioLink ID can run on Windows Server 2016 R2 operating systems. However, for this opportunity, we are proposing a hosted solution, running on a cloud based OS (Amazon Web Services Native OS).	
5	The Bidder's solution shall provide Active Directory integration with Active Directory is 2012 R2 or higher.	**Yes**
Response	[redacted]	
6	The Bidder's solution shall provide an architecture and design specification including a network diagram.	**Yes**
Bidder Response	Shown below are the logical and technical diagrams for this proposed solution. Final architecture and designs, in accordance with the DMV's requirements, will be provided to the state in the Solution Design Document which will be developed, outlining all architecture, connections, data, data flow and processes. The designs below are discussed more fully in Part 2. Proposed Solution, Logical Design:	


Amazon Web Services GovCloud
AWS Virtual Private Cloud (VPC)
WebLink ID Enrollment & Card Management Environment
BioLink ID Facial Recognition Environment
Segmented Renew / Reprint Website
Subnet Routing, NACLs, & Security Groups
AWS Key Management & Encryption
AWS Internet Gateway
Applicants
Cardholders
Camera, Scanners, and Signature Devices
VALID Provided Hardware
Internet
VALID Hosted Card Production & Mail Factories
Factory High Security Area (HSA)
Vermont DMV Network
WebLink ID Image Capture Stations
Cardholder Image & Data Integration w/ VT Existing Systems
BioLink ID Case Investigation Stations (any BMV PC)
WebLink ID Gated Issuance & Lifecycle Stations (any BMV PC)

[redacted]

[redacted]

	Proposed Solution – Virtual Server Design (WebLink ID and BioLink ID): 	
7	The Bidder's solution must be capable of supporting up to 300 concurrent users without any impact to system performance.	**Yes**
Bidder Response	One of the benefits of the cloud model we are proposing, is the ability for the environment to auto scale. The proposed cloud solution is not merely 'co-location of servers in a data center', it is a true cloud platform. This allows the solution to scale drive space, memory, and CPU utilization as needed. The cloud solution will just as readily handle 300 or 3000+ users as the DMV requires.	
8	The Bidder's shall list any PC requirements, including memory needed to access Bidder software.	**Yes**

Bidder Response	To efficiently run the VALID proposed solution, we recommend the following hardware configuration: CPU – Core I3 3rd generation or better RAM – 4GB or better HD – 250 MB of free space (if capture station, 50MB otherwise). VALID's solution is browser based, there is very little footprint needed on the client workstations. If the workstation is to be a capture station with cameras and other capture devices, a small (250 MB) space is needed for local drivers.	
9	The Bidder's solution hardware shall be new, currently available, not refurbished, or obsolete at the time of installation and must be guaranteed for the life of the contract.	**Yes**
Bidder Response	VALID will provide only new hardware for the life of the contract. All hardware selected will be currently available, and will not be selected if the OEM has made any 'End-of-Life' announcements. In the event a failed piece of hardware does have an announced end-of-life from the manufacturer, a suitable replacement device will be sourced, tested, and delivered to replace the component.	
10	The Bidder shall provide the End of Life Cycle for proposed hardware and software.	**Yes**
Bidder Response	VALID's proposed solution's hardware is limited to the capture station devices. The could-based, hosted environment, does not require modernization or server replacements. Cameras, signature panels, and other scanners proposed are selected for their longevity. It is not anticipated that the hardware chosen will need to be replaced, due to obsolescence, over the course of this contract. The software VALID proposes is VALID developed. VALID's planned roadmap (see Part 2, item 8) does not have an end-of-life (EOL) projected for the version of software planned for implementation during the lifetime of this contract. Updates will be provided, but the software itself will not need to be replaced.	
11	Bidders are encouraged to present options that reduce the workstation footprint (the number of peripherals, cables, and required surface area for all components) while still effectively producing credentials and completing transactions.	**Yes**

Bidder Response	VALID's proposed hardware is selected for its ruggedness and quality first, as well as for its footprint. The camera tower chosen has a minimal footprint, and it was designed to free up as much disk space as possible. The scanners chosen for document collection and authentication are not flatbed designs, but are paper feeds, which consume about ½ the physical counter space a flat-bed scanner requires. Hardware list: • Camera • Scanner • Signature panel • Laser printer for temp docs (one per location)	
12	The Bidder shall propose a hardware set-up that accommodates offices with varying layouts and configurations; especially offices with multiple workstations that share cameras, document scanners, and printers.	**Yes**
Bidder Response	VALID's proposed solution for capture stations can be configured in multiple manners. Prior to installation, VALID's team will conduct site surveys, in part to collect specific site needs. Shared devices such as cameras, scanners and printers are supported by VALID's WebLink ID architecture, and should a site need to share devices among multiple enrollment stations, WebLink ID can supports this need.	
13	The Bidder's solution shall include ongoing support and maintenance for all workstations (computers, peripherals, cables, and power supplies), travel time and expenses, and other routine support costs.	**Yes**
Bidder Response	The VALID proposal includes support for the VALID installed hardware, travel time and expenses. There will be no cost to the DMV to support or maintain the hardware installed as part of this proposal. VALID is proposing that hardware support be accomplished by VALID technicians travelling to the site's requiring assistance.	
14	The Bidder's Signature pad hardware shall not require batteries.	**Yes**
Bidder Response	VALID proposes the use of a Topaz signature panel, which draws its power from the USB cable only. No additional batteries are needed for either the device or the pen.	
15	The Bidder shall produce cards at a secure US based manufacturing facility. Provide location of primary and secondary facility for the Card Production Services	**Yes**

Bidder Response	[redacted]	
16	The Bidder shall provide an overview of security procedures for protecting card integrity.	**Yes**
Bidder Response	[redacted]	

	[redacted]	
17	The Bidder shall provide a minimum of 15 on-site/in person trainings.	**Yes**

Bidder Response	VALID will provide at least 15 on-site / in-person trainings to ensure that the DMV staff are proficient in the use of the new solution. VALID will consult with the DMV on an optimal plan for a training schedule that will coincide with the installations and meet any schedule constraints. Training will occur on-site at each DMV-selected location over the course of the deployments. Training will be conducted by VALID at the designated DMV facility(ies) and should include, but not be limited to, the following: • Equipment/software driver information and operation • New processes to be followed with the new solution • DL/ID solution operation. • DL/ID solution maintenance. • Troubleshooting and monitoring. • Preventive maintenance tasks (e.g., cleaning). • Reporting VALID recommends that the installation teams install the new equipment at the DMV sites as well as test the equipment the night before they 'go live' – (immediately after the normal office hours). Some training can be provided that night, and then VALID would provide training to the local staff again the next morning prior to opening. In addition, the VALID staff would remain on site for a 4-hour period to provide hands-on assistance to all the DMV users. If issues developed and were not resolved in those four hours of hands-on assistance, VALID would remain on-site until all issues were resolved.	
18	The Bidder shall develop and implement a training plan that specifies the approach and steps to be taken by the Bidder to ensure that the knowledge, skills and abilities necessary to operate the System are transferred to VT DMV operations.	**Yes**
Bidder Response	VALID will develop and implement a DMV-approved Training Plan that specifies the approach and steps to be taken to ensure DMV personnel have acquired the knowledge and skills necessary to operate the new solution. The Training Plan would then be refined iteratively as a collaborative effort between DMV and VALID. The Knowledge Transfer and Training Plan is discussed in Part 4, item 101; and a sample Knowledge Transfer and Training Plan is provided as part of this proposal in **Attachment 10**. The following elements will be incorporated into our approach to create the Training Plan:	

- Develop an overall training strategy that meets the needs of all DMV audience levels, including the inability of some staff to participate in training for long periods of time; VALID knows that this is particularly true of the branch office staff.
- Our training will be geared for staff who reflect a wide range of computer skills, including those whose computer skills are not well developed. Our instructors will endeavor to conduct training in a user-friendly way, and all training materials and leave-behind materials will be easy to understand.
- Produce training curricula for each role-based constituency. The training curricula will outline the method of training, length of training, facility requirements, detailed outline and description of each training session, list of training materials and samples, and description of self-guided training modules. They will include a summary of the course content, and the goals and objectives of the course.
- Design customized and comprehensive training materials used to train end users and support end users after training. Materials will include step-by-step processes, and will consist of custom web-based training, electronic (fully editable and reproducible), and printed copy formats, as determined by DMV. All materials will be available to DMV to post on its intranet to support end users when using the solution.

Training Program Effectiveness

VALID's philosophy is that training is not an *event*, but an on-going process which includes an evaluation of training effectiveness. We will survey end users to determine the adequacy of the training courses and materials. Our Training Manager will prepare training course handover reports confirming that training and course materials are complete and accurate. Once completed, the VALID Project Manager will provide a certification form that all training services and materials have been provided and are considered final by DMV.

General Training Philosophy & Approach

The Credential Production System is a business-critical application. Given its complexity and importance, VALID places a high emphasis on training. Our training approach for the DMV not only addresses the training needs of current Vermont project stakeholders, but also accounts for future change of staff and refresh needs using a well balanced mix of methods.

The overall goal of the Training program is for the DMV staff to become fully proficient in a given activity or task, and to understand the core functionality of the system so that they can modify processes and flows as needed to support DMV's ever-evolving business landscape.

19	The Bidders shall provide training materials.	**Yes**
Bidder Response	**VALID will provide the following training materials** (This is further discussed in Part 6, #8) • Training plan and Training Schedule • Training Curriculum and Syllabus • Training Handouts • Comprehensive Training Manual (including one hard copy& • Online help materials • Operator's Guides / User Guides (PDF and Microsoft Word versions) • Web-based training materials (demos, videos, etc.) • Quick Reference Guides (including troubleshooting) (laminated) • Presentation materials • Training evaluation surveys • Special role-based materials for Super Users and others	
20	The Bidder's solution must include all software patches and critical updates required to meet the state's functional and technical requirements above shall be included throughout the life of the contract at no additional cost, including any Bidder or third party software. All updates and patches shall be performed outside normal business hours.	**Yes**
Bidder Response	[redacted]	

21	The Bidder shall identify all anticipated or potential future software and hardware upgrades and describe their upgrade process, specifically addressing their deployment and installation process. The Bidder shall also identify any cost-sharing benefits or policies for upgrading.	**Yes**
Bidder Response	VALID's product roadmap (Part 2, item 8) indicates continued development of both the WebLink ID and BioLink ID applications. All or none of the application updates can be applied to the DMV's implementation. As VALID releases application updates, the DMV will have the ability to assess the update, and if it is a desirable product feature, VALID will apply the update to the DMV's QA environment for their testing and acceptance. Only when a product update has been tested and accepted will it be scheduled for deployment to the production environment. VALID anticipates the need to test and validate its web-based application against ever-evolving web browsers, and Windows operating system requirements. Release of new web browsers, browser versions, and operating systems is something VALID already tests and supports. Sometimes core functionality of a web browser changes, requiring updates to either WebLink ID or BioLink ID to support the new browser version. The DMV will be notified of supported browsers, as they are created, and any impact of a new browser upon the current implementation of WebLink ID and BioLink ID. VALID provides a QA environment for the DMV to test updates and upgrades. The QA environment replicates the production environment as closely as possible (including connections to other QA environments if available). Promotion of any update or upgrade to production cannot occur unless the DMV accepts the update or upgrade on the QA environment.	
22	Bidder shall be responsible for ensuring hardware and consumables are available to meet the requirements of this contract.	**Yes**
Bidder Response	VALID acknowledges that it will deploy and install all needed hardware at the DMV locations and will maintain that hardware through its VALID Field Services teams. VALID also acknowledges that it is responsible for maintaining all its consumables at the DMV locations and at its card personalization factories. With a central issuance solution, consumables at the DMV offices are limited to printer ink and paper. There are no other consumables needed at the State offices. At the card personalization facilities, VALID maintains a rigid inventory of supplies to produce the State's credentials.	
23	The Bidder's system solution availability must be 24/7 with 99.9% uptime requirement, except for agreed upon maintenance window. Solution must provide real-time reporting and alerts of all interruptions in services and processes.	**Yes**

Bidder Response	VALID acknowledges that its solution availability will meet the 99.9% uptime requirement, 24 x 7 x 365, except for agreed upon maintenance windows. VALID will provide real-time reporting on its availability and will provide alerts for all interruptions in services and processes. This solution availability is also reflected in VALID's suggested service level agreement (SLA). To accomplish the required system uptime and availability, VALID deploys its applications and databases such that there is no single point of failure; each system is redundant, even in the cloud hosted environment. Each system is also monitored with a monitoring service, enabling immediate notification should any server or service trigger a threshold level, or experience an outage. Messaging from the system can be sent via 'in application' system messages which appear to operators, email notifications to targeted groups, or even text notifications to mobile devices. The type of messaging and the thresholds for triggering a message will be defined by the DMV and configured by the VALID team. Below is a network diagram displaying both the monitoring service and the redundant design of the proposed solution.

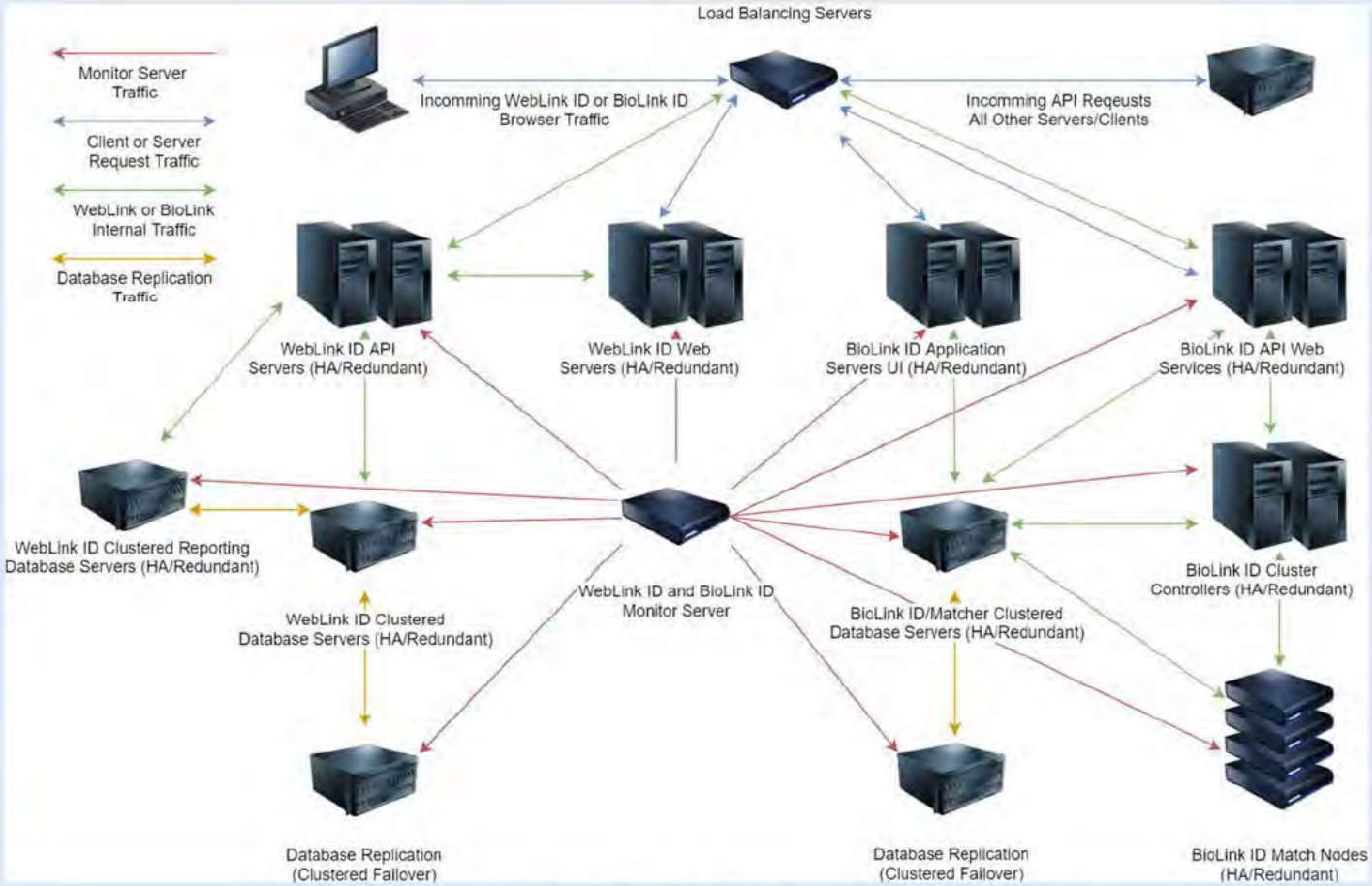


Figure 25: Network Diagram

24	The Bidder's solution shall be compliant with AAMVA standards (2016) see (Exhibit 1). Preferred security features include • UV fluorescent ink in security background printing • Tagged Ink • Phosphorescent Ink • Printing dynamic data elements using digital imaging technologies • Laminate, overlay or coating for surface printed data and portrait • PDF 417 Bar code (and MRZ on EDL) • Security background overlapping the portrait image area • Ghost image • Magnetic media fingerprinting • UV-A dull substrate material • Tamper evident card body • Embossed surface pattern • No CMYK colors and at least 2 special colors • Guilloche design • Micro printed text • Deliberate error into the design or microprint	**Yes**
Bidder Response	VALID's solution is fully compliant with AAMVA standards (2016). In its Card Design Standard (CDS), the American Association of Motor Vehicle Administrators (AAMVA) divides security features into four categories. In each of these categories AAMVA specifies one or more mandatory features as well as one or more optional features, depending on the category. The features are further divided into Level 1 features (able to be authenticated without the aid of tools or devices) or Level 2 features (authentication requires the use of simple tools or devices). One additional feature known as a Level 3 feature (authentication requires forensic assessment by skilled individuals and/or laboratory equipment) is required, but its classification is not addressed. 1. Card Body – one mandatory feature and two optional features 2. Security Design – two mandatory features and two optional features 3. Security Background Printing and Personalized Data – one mandatory and two optional features 4. Protecting Personalized Data – four mandatory and one optional features	

	A card that is fully compliant with AAMVA's minimum requirements can be made with only fifteen security features; however, no one in the DL/ID industry issues cards containing only fifteen security features – they could be more readily counterfeited or altered. In fact, counting security features has become something of an arms race. For example, consider the use of microprint (generally speaking, text whose height does not exceed 0.3 mm). If a card contains a single character of microprint does it meet the requirement? If it contains a line of microprint is that a single feature? Is four lines, four features or is it the number of characters? VALID takes the most conservative approach possible. A security feature is counted only once, no matter how many times it appears in or is used on a card. AAMVA makes no mention of the materials used in the construction of the card. Instead, in Annex E of the CDS, they describe various performance requirements considered crucial to the service life of a DL/ID. These requirements are codified in standards issued by the InterNational Committee for Information Technology Standards (INCITS) and by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). Solid PVC cards, which were once common in the DL/ID industry, are no longer offered by VALID. Their service life is not suitable. VALID does offer cards constructed of a PVC/PET composite and cards constructed of polycarbonate. Composite cards offer reasonable performance at an economical price point. Teslin, like paper, is composed of long fibers pressed into a matrix containing quite a lot of air. As such it is extremely porous and absorbent – like paper. It accepts ink well and is very flexible, which facilitates digital printing. For the same reasons, litho inks are absorbed quickly making dot gain and bright colors problematic. Further, it readily absorbs the dirt, sweat, grease and grime of everyday life. For these reasons, VALID does not offer a card containing Teslin. Finally, polycarbonate cards offer maximum performance, but are also more expensive than composite. Polycarbonate is fast becoming the de facto international standard for identity documents. Within each AAMVA category, VALID offers certain features contained in a base card as well as offers additional features. Certain of the additional features may be offered at additional cost, and if so, the cost will be called out separately in the pricing summary. The AAMVA security categories are discussed in order.

CARD BODY

[redacted]

UV-A dull substrate material – This is a mandatory AAMVA requirement, was a preferred feature by the DMV, and is included in both of VALID's base cards. A common approach to making a counterfeit card is to print a facsimile of the card on a desktop printer using ordinary copier or printer paper; however, these papers contain brighteners that are added to make the paper white. By making the DL/ID using UV-dull material, these common counterfeits can be easily detected using an inexpensive UV flashlight.

Figure 26: UV-A Dull Substrate Material

Fixed print and/or dynamic data on different layers – This is an optional AAMVA requirement, and is a standard feature of both of VALID's base cards. One method of attack by fraudsters is to split a card open between its layers to access the data contained therein. By layering the data and printing, it makes it difficult to access the entirety. In addition, because the data and printing separate if the card is opened, it is virtually impossible to realign them when the card reassembled. VALID follows this best practices method of linking and layering security features, but because our cards are fully fused, it is not possible to "open" a card without destroying it.

Tamper evident card body – This is an optional AAMVA security feature, a DMV-preferred feature, and is a standard feature of both of VALID's base cards. AAMVA defines this as a "card showing evidence of destruction or modification caused by an attack." VALID's cards demonstrate evidence of attack by tearing themselves apart if an attempt is made to intrude into the card.

Card core inclusions – This is an optional AAMVA requirement, and an optional feature offered on VALID's Composite and Polycarbonate cards. It consists of printing graphics or text on the inner layers of the card's core, such that they cannot be seen unless the card is held over a bright light. These are very popular with law enforcement personnel, because they can be easily authenticated at night by holding the card over a flashlight. If selected, the specific details of color and design will be determined during the Card Design phase of the project.

Figure 27: Card Core Inclusions

Serialized card blanks – This is an optional AAMVA requirement, and is standard feature of both of VALID's base cards. The cards will be printed (or laser engraved, if polycarbonate) with a serial number in human-readable form as well as in machine-readable form via a Code128 1D barcode. This information will be printed on the back of the card along the top edge. As an extension of this security feature, VALID uses a skip numbering scheme whereby serial numbers are not issued in order and some numbers are never issued. Thus, even if fraudsters were to produce a facsimile card, they cannot be certain that any particular serial number will be used. Serial numbers are tracked from cradle (creation) to grave (issuance or destruction).

Figure 28: Serialized Card Blanks

Embossed surface pattern – This is an optional AAMVA security feature, a preferred feature by the DMV, and is offered as an option by VALID in both of its card constructions. Most commonly, the date of birth is indent printed or embossed over the portrait, serving as redundant data (an AAMVA security feature) as well as permanently deforming the card, locking the portrait in place, making image substitution (the most common type of attack) all but impossible. Pricing for this optional feature is called out in the pricing summary.

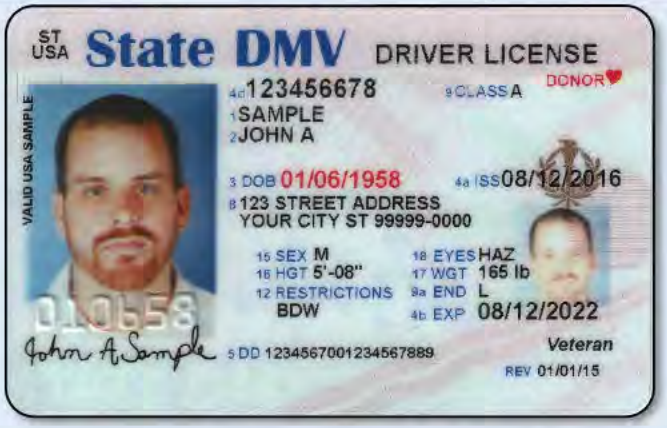


Figure 29: Composite Card with DOB Embossed over Portrait

Security Bonding – This is an optional AAMVA security feature, and a standard feature of both of VALID's base cards. This is a feature whereby the edges of the card are sealed making it apparent if gaining access to the card is attempted. Both of VALID's offerings are fully fused. The edges of the card cannot be peeled apart to gain access.

SECURITY DESIGN

[redacted]

No CMYK colors – This is a mandatory AAMVA security feature, was preferred by the DMV, and is a standard feature of both of VALID's base cards. CMYK colors are produced on inkjet and laser printers. Special or spot colors are mixed - like paint. The difference is readily apparent under low-power magnification. VALID will provide spot colors on both the front and back of the card. We believe it is important to include spot colors on the back. While it is not impossible to print color on both sides on a desktop card printer (the source for many counterfeit cards), it is difficult. Specific colors and designs can be determined during the Card Design phase of the project.

Figure 31: Spot Colors

Figure 30: CMYK Colors

Guilloche design – This is a mandatory AAMVA security feature, was preferred by the DMV, and is a standard feature of both of VALID's base cards. A guilloche is a fine line design that is impossible to exactly reproduce without the software used to originally create it and without the mathematical settings used at that time. Guilloches have been used for decades in designing and printing currency and other financial instruments. Further, VALID prints guilloche(s) on high-resolution lithographic printing presses at line widths so narrow they cannot be reproduced by photocopying or by printing on inexpensive printers. The specifics of the design will be determined during the Card Design phase of the project. A guilloche is shown in the Spot Colors illustration, above.

Microprinted text - This is an optional AAMVA security feature, was preferred by the DMV, and is a standard feature of both of VALID's base cards. Microprint is generally considered to be text whose height is no more than 0.3 mm. It is so small it cannot be printed by most commonly available printers and copiers. Typically, VALID embeds the job number of the preprint press run into the microprint. Only the DMV and VALID will know the correct job numbers for each card type. The specific details of the variable microprint – its location and content – can be determined during the Card Design phase of the project.

Figure 32: Microprinted Text

Duplex security pattern - This is an optional AAMVA security feature, and is a standard feature of both of VALID's base cards. A duplex security pattern is formed when two colors are printed in close registration such that an image is formed by their combination. In the adjacent illustration, a guilloche was formed using violet and yellow spot colors intersected by maize and azure fine line detail. Notice that the violet lines die into the yellow border of the seal. Only skilled pressmen can produce these patterns. The specifics of the pattern can be determined during the Card Design phase of the project.

Figure 33: Duplex Security Pattern

Rainbow printing - This is an optional AAMVA security feature, and is an optional feature of both of VALID's base cards. Also known as split fountain printing, rainbow printing is typically accomplished by putting two inks in the same fountain, which produces a continuous color gradient from one color to the other. The problem is that as the press runs, the inks mix and even the pure colors change, becoming ever muddier. VALID creates the same effect by overlapping two PMS color gradients. Since the colors are in two independent fountains they never mix and thus maintain the same appearance throughout the press run.

Deliberate error - This is an optional AAMVA security feature, was preferred by the DMV, and is a standard feature of both of VALID's base cards. Deliberate errors are embedded in secure cards in little-known locations. An uninformed fraudster in an effort to make the "perfect forgery" might be unaware of the error and fail to include it. Typically, deliberate errors are contained within the microprint. There is an art in determining how many errors to include and where to locate them. Too many errors, and it is obvious to everyone that they exist. Too few or too obscure and they make authentication difficult. The specific details can be determined during the Card Design phase of the project.

Figure 34: Deliberate Error

Use of non-standard font - This is an optional AAMVA security feature, and is a standard feature of both of VALID's base cards. AAMVA defines a non-standard font as one of restricted availability, but it does not define what is meant by "restricted availability". If we assume that restricted availability means a purchased font, that would still allow for thousands of fonts. VALID's Card Design team has constructed a proprietary font which is not available to the general public and which is never installed on equipment other than that used by VALID in card design, in pre-press, and in card manufacture. VALID will provide its proprietary font for use in the preprinted microprint and in certain locations of the personalization.

BACKGROUND PRINTING & PERSONALIZED DATA

[redacted]

UV fluorescent ink in security background printing - This is a mandatory AAMVA security feature, was preferred by the DMV, and is a standard feature of both of VALID's base cards. VALID stocks a variety of invisible UV inks as well as bifluorescent inks. These are inks that emit visible light of one color when illuminated with UV light at one wavelength and a different visible color when illuminated by UV light at another wavelength. Bifluorescent inks are particularly useful security features because they can be preliminarily authenticated by illuminating them with an inexpensive UV flashlight. Then, if the document is still suspect, a secondary authentication can be performed with a second UV light source. The specific design(s) and location(s) can be determined during the Card Design phase of the project.

Figure 35: UV Fluorescent Ink

Optical effect pigments (other than UV or IR pigments) - This is an optional AAMVA security feature, and is a standard feature of both of VALID's base cards. Optical effect pigments change color as the angle of the light striking the pigment changes. For example, they may change from gold to green. They are most distinctive when applied to cards using silk screen presses. VALID believes they constitute a significant security feature because (1) their appearance is quite distinctive, (2) the presses required to print them are not common, and (3) the inks used are strictly controlled. For example, the ink used in the illustration is sold only to VALID. The specific design and location(s) can be determined during the Card Design phase of the project.

Figure 36: Polycarbonate Card with Optically Variable Ink

Figure 38: OVI Showing as Gold

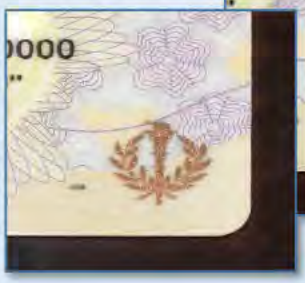


Figure 37: OVI Showing as Green

IR-fluorescent ink - This is an optional AAMVA security feature, and is a standard feature of both of VALID's base cards. Invisible infrared (IR) fluorescing inks emit visible light when illuminated by IR light of a specific wavelength. Typically, they must be revealed through IR lasers, not simply an IR flashlight. They are an important security feature because the specific wavelength required to reveal them may not be well-known, and the inks used to print them and the lasers required to illuminate them are not readily available. The specific design, location(s) and color can be determined during the Card Design phase of the project.

Figure 39: IR-Fluorescent Ink

Phosphorescent ink - This is an optional AAMVA security feature, was preferred by the DMV, and is an optional feature of both of VALID's base cards. Phosphorescent inks are commonly called "glow in the dark" inks. They contain pigments that are "charged" by exposure to UV light, and then they emit visible light that fades after the UV light is removed. VALID believes these inks are most useful in situations where the ink is routinely exposed to light and dark cycles; however, identification cards which are normally stored in a wallet or purse are not typically "charged". So, the phosphorescent effect is not observed. Nevertheless, VALID will include this ink if so desired by the DMV.

Tagged ink - This is an optional AAMVA security feature, was preferred by the DMV, and is an optional feature of both of VALID's base cards. Inks may contain one or more taggants - chemicals or other materials added to the ink to facilitate various forms of verification. Depending on the taggant(s), authentication may be accomplished by use of a simple reader or may require examination by a skilled technician in a laboratory environment. VALID uses a variety of tagged inks and offers them as an additional cost option, price to be determined based on the particular taggant selected and the coverage.

Color portrait – AAMVA does not consider a color portrait a security feature. It is a standard feature of VALID's composite card as well as an optional feature on VALID's polycarbonate card. VALID will optionally provide a polycarbonate card wherein the portrait and other key information – the date of birth and driver license number – are printed in color. The balance of the information will be laser engraved. The black component of the portrait will not be printed, but will be laser engraved. If the image is somehow removed, then the black portion of the image will remain embedded within the card (in the illustration, a hologram overlays the lower right of the portrait).

Figure 40: Color Portrait

UV fluorescent ink in personalized data - This is an optional AAMVA security feature, and is an optional feature of both of VALID's base cards. VALID offers invisible UV data in personalizing the cards as an optional security feature. Typically, the portrait and either the name and/or date of birth are used. The specific content and location(s) of the data can be determined during the card design phase of the project.

Figure 41: Composite Card with Variable UV Data

PROTECTING PERSONALIZED DATA

[redacted]

	Printing dynamic data using digital technologies – This is a mandatory AAMVA feature, was preferred by the DMV, and is a standard feature of both of VALID's base offerings. Decades ago, driver's licenses and identification cards were produced using typewriters and film. Demographic data was typed onto a paper card, a photographic image was punched out of a strip of film, and the two were laminated together in a small, pouch laminator. Printing the variable data using digital means precludes image substitution by inserting a photograph. VALID only personalizes cards using digital technology. **Laminate, overlay or coating for surface printed data** – This is a mandatory AAMVA feature, was preferred by the DMV, and is a standard feature of both of VALID's base offerings. Unprotected surface printing is subject to abrasion and may wear off. Further, it is easily accessible to removal and replacement, or alteration. VALID's Composite card, which contains surface printing is protected by an overlay and a UV-cured coating. VALID's base polycarbonate card contains no surface printing and does not require protection; however, if either the color portrait option or the variable UV data option is selected for the polycarbonate card, a clear protective overlay will be required and will be provided. **PDF 417 barcode** - This is a mandatory AAMVA feature, was preferred by the DMV, and is a standard feature of both of VALID's base offerings. The PDF 417 barcode serves primarily an administrative purpose. It contains all of the demographic data contained elsewhere on the card. Devices such as laptops and workstations equipped with the appropriate scanner can use the PDF 417 to facilitate data entry. That said, it does also constitute the inclusion of redundant data, another AAMVA security feature. **Security background overlapping portrait** - This is a mandatory AAMVA feature, was preferred by the DMV, and is a standard feature of both of VALID's base offerings. Although the PDF417 barcode provides a certain level of data redundancy, its primary purpose is administrative. It enables the use of appropriate devices to quickly and easily scan and decode the barcode. In fact, iPhone and Android apps are now available for just this purpose. All DLs and IDs issued by VALID contain a PDF 417 barcode. The barcode contains certain mandatory fields and may contain various optional fields. The specific construction of this barcode will be determined during the Card Design phase for the project.

Embedded data in portrait - This is an optional AAMVA feature, and is an optional feature of both of VALID's base offerings. Overt data is embedded in the ghost portrait, which is itself an optional AAMVA feature by superimposing a succession of letters and/or numbers whose color and density are varied so that when viewed at a distance, a reasonable representation of the image is perceived. VALID recommends this be done in the ghost image - as the portrait is the primary means of authenticating an individual's identity and the data embedding process may cause small identifying marks such as scars to be obscured.

Figure 42: Embedded Data in Portrait

Redundant personalized data - This is an optional AAMVA feature, but are standard features of both of VALID's base offerings. VALID will provide a limited amount of redundant personalized data elements as part of the base offering. Theoretically, all personally identifiable information could be reproduced, but the physical space available on the card is not unlimited. So, VALID imposes a soft limit. Typically, the redundant data includes the ghost image, date of birth, and occasionally the signature or driver license number. Additionally, all of the data contained on the card is encoded within the PDF417 barcode, which is a mandatory security feature.

Optical variable element - This is an optional AAMVA feature, and is an optional feature of both of VALID's base offerings. Optically variable elements change color or appearance as the angle of the light source varies just as do optically variable inks; however, optically variable elements are commonly understood to mean holograms or other diffractive structures. They may be hot stamped on the surface of the card, may be hot stamped on the core of the card body prior to lamination, or may be a part of the overlay, if any. They may overlap the portrait, as described above, or may be placed elsewhere on the card. These are some of the costliest security features included in card manufacture and vary widely in cost depending on the complexity and size of the included elements. Thus, VALID offers this as an unpriced option, with the price to be determined during the Card Design phase of the project, if this option is selected.

Personalized tactile elements - This is an optional AAMVA feature and is an optional feature of both of VALID's base offerings. VALID offers a variety of options for personalization with tactile elements. Embossing and indent printing may be done on both of VALID's cards. Embossing is a time-honored feature has been utilized in credit cards for decades. Both stress the card beyond its elastic limit, permanently deforming it and in either case, small alterations can be embedded within the characters that are only visible under magnification, rendering it a Level 2 feature as well as a Level 1 feature. In either case, VALID typically applies the feature over the portrait, locking it into the card. VALID's polycarbonate card may be personalized with tactile, laser engraved elements – most commonly the signature and date of birth. VALID offers embossing and indent printing as extra cost options, but offers tactile laser engraving as a no-cost option for the polycarbonate card.

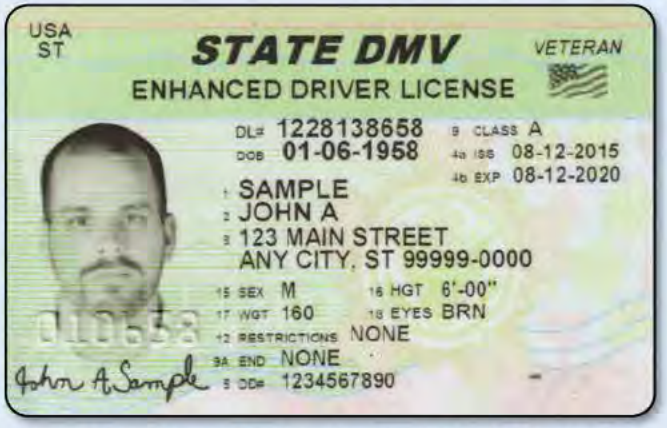


Figure 44: Embossed Polycarbonate Card also containing Tactile Laser Engraving

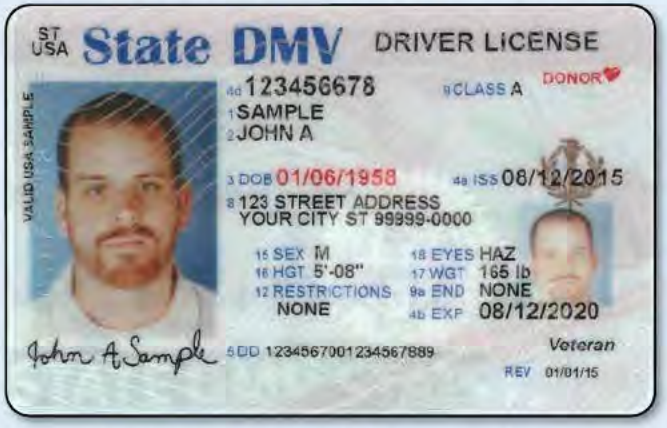


Figure 43: Indent Printed Composite Card

Figure 45: Secure Indent Print, Magnified View

	Fine line foreground - This is an optional AAMVA feature, and is an optional feature on VALID's composite offering. VALID's Composite card contains surface printing, and as such requires a protective overlay. VALID provides a clear overlay at no additional cost; however, an option for protecting the portrait and demographics, if desired, is fine line printing which can include fixed colors, rainbow colors or invisible UV inks. The cost of features like this are highly dependent on the number and type of inks and the coverage. Accordingly, the noted cost is based on a single optically variable ink and a single, invisible UV ink. Specific pricing would be determined during the card design phase of the project. VALID's polycarbonate card contains no surface printing and does not require a protective overlay. **Ghost image** - This is an optional AAMVA feature, was preferred by the DMV, and is a standard feature of both of VALID's base offerings. VALID will provide a color, ghost image at approximately half size on its Composite offering. VALID will laser engrave a ghost image on its Polycarbonate offering. VALID's general practice is to render each image contained on the card – primary, ghost, UV, etc. – at different resolutions and sizes and using different technologies. Image substitution is the most common form of card attack and by providing images at different sizes and resolutions, it becomes much more difficult to make a substitution. **Magnetic media fingerprinting** - This is an optional AAMVA feature, and was preferred by the DMV. Unfortunately, VALID respectfully declines to offer this feature – for several reasons. First, magnetic stripe technology is in decline in the banking industry and as the volume declines, the technology will become costlier to provide and to support. Second, it requires access to an external database – meaning cards can only be authenticated as long as the database connection is available. Third, this particular technology is expensive, will require significant development resources, and is licensed to a single company. Whenever possible, VALID avoids sole-source supplier arrangements. **SUMMARY** Recall from above, it was noted that a card that is fully compliant with AAMVA's current CDS could be made having only fifteen security features, not counting Level 3 feature(s). AAMVA also recommends that the security features be divided between Level 1 features, Level 2 features and requires a single Level 3 feature. Level 1 features, can be authenticated without the use of additional devices, are of most use in situations where a card needs to be authenticated quickly by many different people – typically, retail establishments and bars. Level 2 features, can be authenticated only with the use of simple tools such a magnification or UV flashlights, are of most use in situations where there is time to carefully examine the card and where only a few special devices need to be procured – typically, law enforcement.

	PREFERRED SECURITY FEATURES The DMV identified sixteen preferred security features. VALID's two proposed base cards may contain as many as twenty-two Level 1 security features and twenty-five Level 2 security features, depending on the options selected. Additionally, whereas AAMVA requires a single Level 3 security feature, VALID will include two Level 3 security features. One of the Level 3 security features can be authenticated non-destructively. The second Level 3 security feature can only be authenticated by taking a specimen from the card, thereby rendering the card in VALID. The specific nature of these security features will be disclosed to the DMV after award, during the Card Design phase of the project.	[redacted]

25	The Bidder's solution must be in compliance with federal requirements for EDL issuance, system shall incorporate address verification into the gated issuance process. Cards with invalid addresses shall be forwarded to DMV for investigation.	**Yes**
Bidder	VALID is the current incumbent for the State of Washington and as such has issued nearly 200,000 Enhanced DLs and IDs that are in full compliance with Department of Homeland Security (DHS) and Customs and Border Patrol (CBP) requirements. Every card VALID issues is subjected to address verification against the U.S. Postal Service's (USPS) data base of VALID delivery points as well as our CASS-certified National Change of Address (NCOA) database, In2View. Print requests whose addresses are found to be discrepant will be forwarded to DMV for investigation. Most incorrect addresses are created as a result of typographical errors at data entry. This is also the best opportunity to correct these errors, since the individual most familiar with the correct address is present at that time. VALID recommends use of Delivery Point Verification (DPV) tools at the operator workstation that will alert the operator when an address has been entered that is not a VALID delivery point. Most mail that is undeliverable as addressed, but which has a valid delivery point, occurs because a forwarding request has been submitted to the USPS. The majority of these instances are identified by VALID's In2View product, through which all print requests are processed prior to their being submitted to the Card Personalization Facilities (CPF). As noted, per DMV's requirement, these requests will be forwarded to DMV for investigation; however, other options exist for processing discrepant addresses. For example, DMV could allow VALID to correct the address printed on the carrier in accordance with the current NCOA database and return the updated address in the print confirmation file for DMV's use – either to update their records or perhaps to flag them for review. This has proven to be a popular option in other state programs as it reduces returned mail while still collecting the change of address notifications needed to maintain an accurate mailing address database. Finally, a small number of print requests may be processed having valid delivery points, but for which a Change of Address was submitted after the print request was processed by VALID's In2View product (presuming DMV allows in2View to make address corrections). VALID recommends that all envelopes contain the Ancillary Service Endorsement RETURN SERVICE REQUESTED, which will result in the envelope being returned to DMV with the reason for non-delivery and the corrected address, if one is known. This will enable DMV to correct the mailing address, and then mail the corrected card to the new address.	

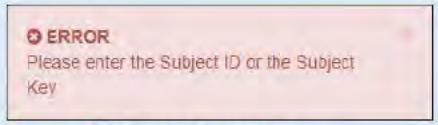
26	The Bidder shall allocate **500 hours** per year for the purpose of system enhancements, changes to card formats etc. Unused time shall be rolled over into the following year and will expire at the end of the contract.	**Yes**
Bidder Response	VALID agrees to allocate 500 hours per year to support system enhancements and other changes, such as card formatting, as needed. Further, VALID agrees that if any of the 500 allocated hours are not used in a given year, then they will be rolled over into the following year. This process of rolling over the hours will continue until the expiration of the contact.	
27	The Bidder's solution shall include Dynamic Knowledge-based authentication as part of the EDL issuance process.	**Yes**
Bidder Response	VALID's solution includes the creation of a Dynamic Knowledge-based authentication engine for VT customers to complete prior to completing the EDL enrollment process. This engine will present the customer with questions, based on data already known about the customer, from a regular enrollment. Questions will vary, and we look to the DMV to determine how many questions the customers must answer, and what are the range of topics that can be discussed – all to ensure the engine meets the DMV's expectations. Questions might range from data such as 'State your full middle name', 'Select your previous, not current, residential address street name' (from a list, where one answer is the proper previous street name, if the person has a previous), select the location of your last DL issuance (from a possibility list). The Dynamic Knowledge-based engine can be presented to the users on any workstation or self-help kiosk the DMV might have already, or it can be presented to the customers on the digital signature panel they will need to use to sign the application. How the Dynamic Knowledge-based authentication engine will be utilized is flexible, and will be defined in the Design phase of the project, between VALID and the DMV.	
28	The Bidder's solution for Facial recognition software shall include: • 1:1 verification where the most recent photo taken is compared against other images stored for that specific • 1:N matching • Data storage • Data archiving • Ability to be turned off without negatively impacting operations of the other system components	**Yes**
Bidder Response	BioLink ID is a web-based biometric analysis, storage and case management solution for photos and fingerprints. BioLink ID stores the desired biometric information for 1:1, 1:N, 1:R, and N:N biometric matching, verification and de-duplication. BioLink ID serves as both the biometric analysis engine as well as the application to view, manage, and solve biometric cases	

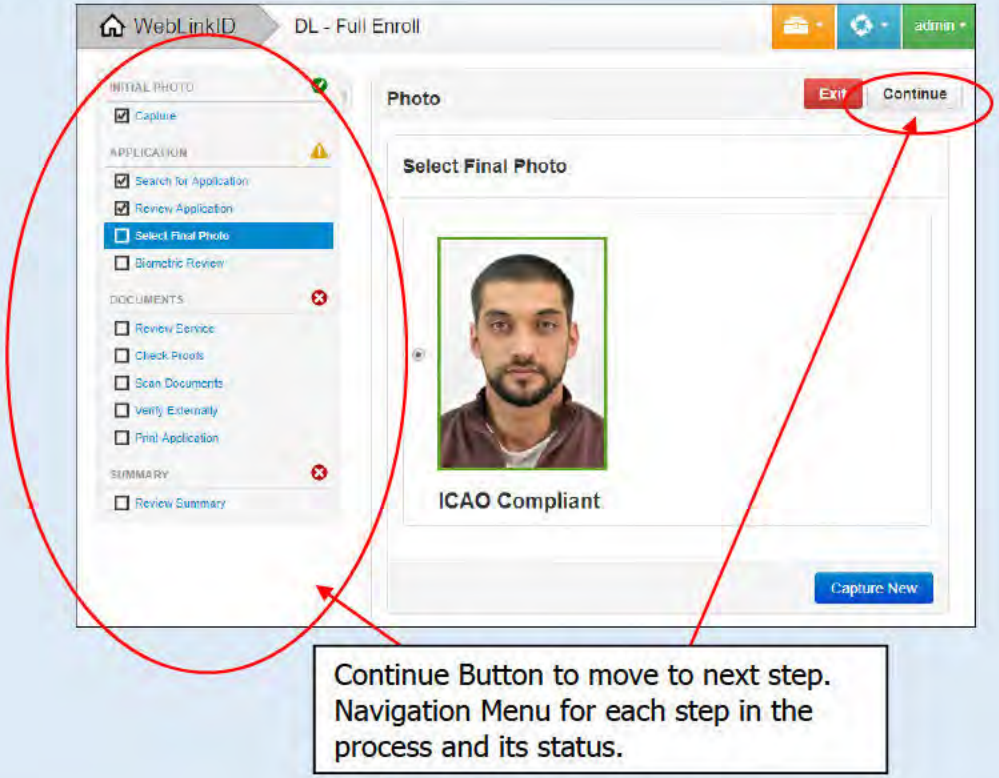
	created during the enrollment or migration process. BioLink ID uses the best of breed algorithms for its biometric analysis, verification, and de-duplication. [redacted] VALID's proposed solution utilizes WebLink ID to pass the images to BioLink ID as part of the enrollment process. During the enrollment process, and in accordance with the DMV's desired workflow, 1:1 verification will be accomplished at image capture, and 1:N as part of gated issuance, meaning the credential will not be cleared to be printed until it has passed 1:N verification. See Figure 46 below for a screen shot displaying 1:1 image success. All biometric enrollment and verification can be removed from the workflows should the DMV need to 'turn off' facial recognition. BioLink ID is not required for WebLink ID to conduct enrollments, communicate with other verification portals such as AAMVA, and can be removed from the environment without affecting other credential issuance processes, should the need arise.

Figure 46: WebLink ID screenshot displaying 1:1 Image success from BioLink ID.

29	The VT DMV is interested in exploring the ability to integrate directly with State to State (S2S) to ensure compliance with Real ID requirements. Please explain how the Bidder solution shall meet these requirements.	**Yes**
Bidder Response	As AAMVA's State to State offering is based on CDLIS integration, implementation of the S2S interface, when it is generally available, will be attainable by the DMV through WebLink ID integration. AAMVA is also considering direct web portal access through its web services offerings, but these are not yet available. VALID will work with the DMV to gain access to the S2S interface, and will modify the enrollment workflow to execute calls to the S2S interface should an applicant provide another state's ID or DL. Depending on the S2S systems' responsiveness, this verification can happen real-time, or it can happen as part of the gated issuance process, where the applicant continues with the request for a credential, and before finalization of the request, the operator can view the results of the S2S verification before letting the applicant depart.	
30	The VT DMV is interest in exploring Mobile Driver's License. Please explain how the Bidder shall meet these requirements.	**Yes**

Bidder Response	[redacted]

	[redacted]	
31	The Bidder's System's error messages will be expressed in plain language, precisely indicate the problem, and constructively suggest a solution.	**Yes**
Bidder Response	Both WebLink ID and BioLink ID display error messages in human readable text, clearly explaining the issue to the operator. The text strings used for the error messages are definable, and they are easily adjustable to meet text the DMV would prefer to use, should they wish to change the default text VALID's applications utilize. Below are screenshots of error and general system messages inside WebLink ID and BioLink ID. The red message is a sample of an error message which pops up on the screen; the green message is simple information for the operator that their last task, in this case a "Save", succeeded.	 **Figure 48: Error Message** **Figure 49: Save Message**

32	The Bidder's System will alert the User with information relevant to required next steps.	**Yes**
Bidder Response	The design of the WebLink ID enrollment workflow(s) are detailed enough such that information needed, or steps which need to be undertaken, can clearly be identified to the operator. With the design of a multi-step enrollment, as the operator advances through the enrollment, completed sections can be collapsed and other sections expanded automatically. Alternatively, a multi-page design can be implemented, as shown below. As the operator completes one section, a 'Next' or 'Continue' button can take him to the next section, and the workflow can display the progress through the steps, shown on the left side of the image below.  **Figure 50: WebLink ID Navigation Panel**	
33	The Bidder's System will provide drop down and list boxes for all key entry, and text entry will display existing values for selection (system based auto fill) (but specifically disallow User browser based autofill).	**Yes**

Bidder Response	WebLink ID workflows can be designed to utilize edit boxes, static dropdowns, and dynamic dropdowns (from system based autofill). Browser based autofill can be disabled on the pages, preventing the intentional or accidental population of invalid data into an applicant's enrollment. The image shown here displays a mini form for special mailing address entry, not the * for required and the drop down boxes for static values. **Figure 51: Special Mailing Address Entry**

34	The Bidder's System will accommodate point and click selection and check box entry for all relevant data entries to ensure that the User does not have to enter textual data that may already be available to the Bidder's System.	**Yes**
Bidder Response	VALID solutions analysts will work with the DMV staff to ensure the enrollment form is as streamlined as possible, utilizing text combo boxes, check boxes, populated drop downs, and edit boxes to reduce the typing and keyboard entry required to accomplish an enrollment. Converting as many options to defined values as possible, increases speed and reduces the potential for mistyped data entry.	
35	The Bidder's System will provide field level on-screen edits with limited User override capabilities.	**Yes**
Bidder Response	WebLink ID's workflow forms can provide field level permissions, enabling edit, change, view or hide, based on user permissions or role. Fields can be marked as read only, allowing for an administrator to override (requires admin password verification, without logging existing operator out) as shown below. Each field, check box, or data entry object can carry different permissions as needed. The next two images display the 'override' capabilities. The first is for overriding a failed ICAO image quality check, the second image displays a facial recognition 1:1 override option. **Figure 52: Failed ICAO Quality Check Override**	

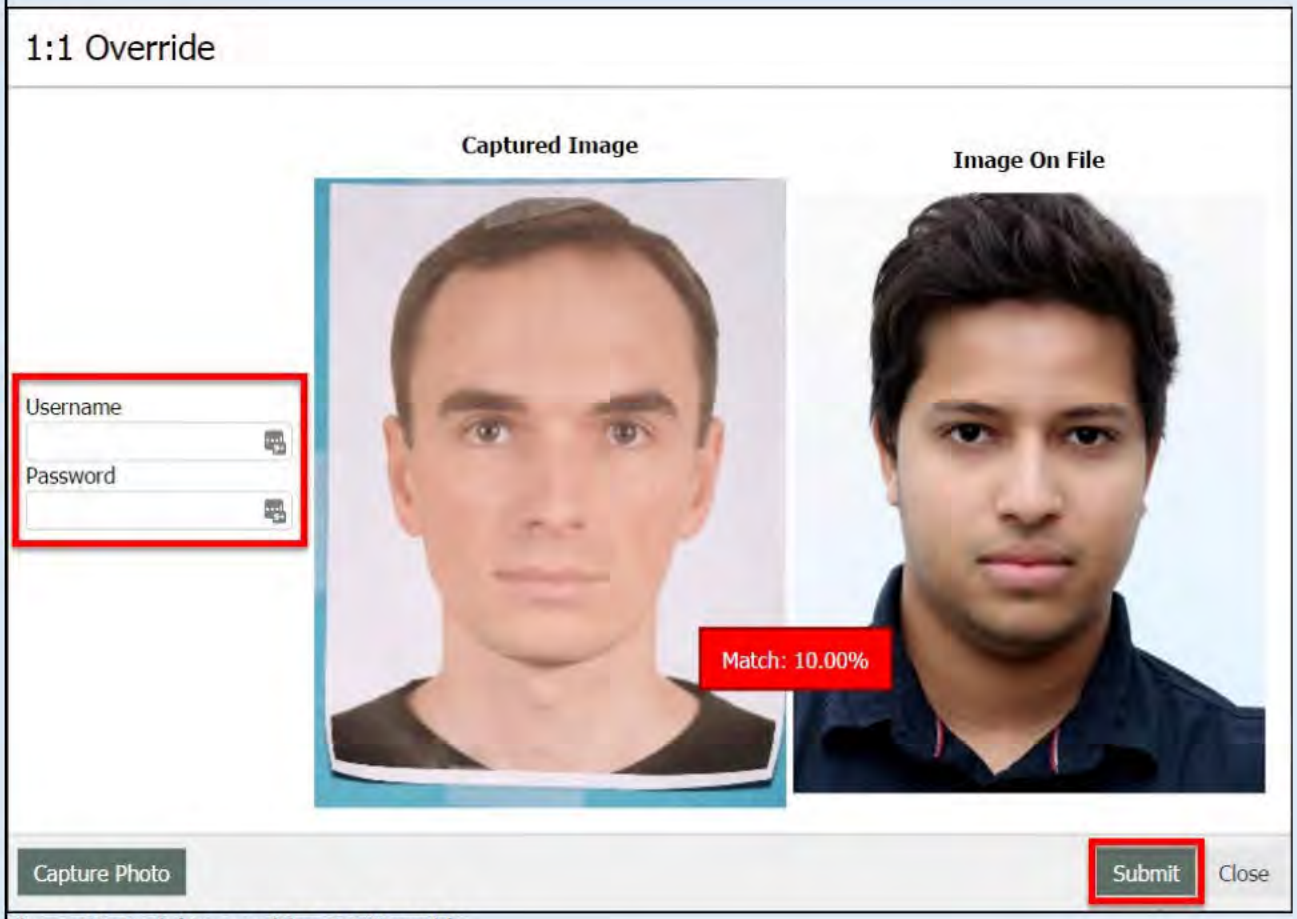
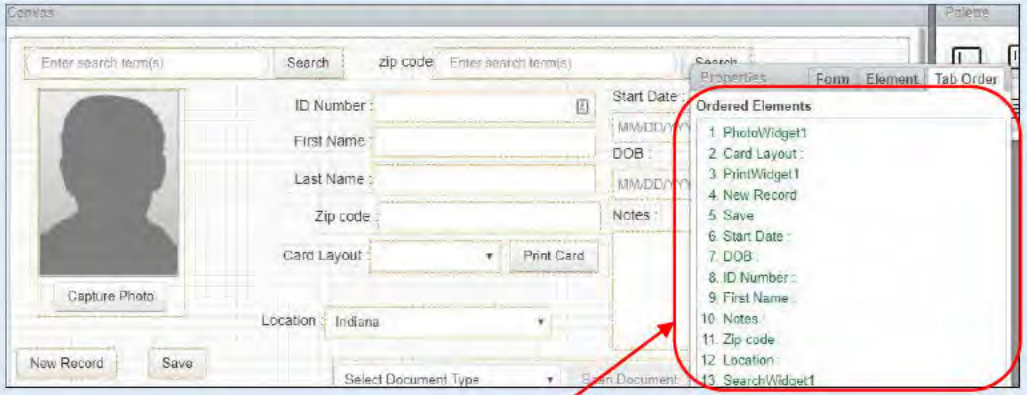


Figure 53: Facial Recognition 1:1 Override

36	The Bidder's System will not show fields not accessible to a given User based on access rights, member consent, nor will the Bidder's System show fields not in use.	**Yes**

Bidder Response	WebLink ID's workflow can be designed to hide fields that the standard user should not be able to view, but administrators need. Fields not in use will not need to be displayed on the workflow. VALID's Solution Analysts will work with the DMV to ensure the fields presented to each operator roll are appropriate for that operator roll's needs.	
37	The Bidder's System cursor will automatically advance to the next logical input field when the maximum allowed numbers of characters have been entered for the keyed field or when the User presses the "Enter" or "Tab" key.	**Yes**
Bidder Response	Intelligent navigation of the enrollment workflow is paramount to data efficiency. The workflow will be designed to maximize operator ease-of-use. This is accomplished by logically laying out the enrollment steps, enabling auto movement of the cursor when a field is complete, and defining 'tab stops' and 'enter key functions'. WebLink ID supports these functions in its form designer, allowing for the proper ordering of data entry, and rapid access to the entry fields. The screen shot below displays the 'tab stop' order within a defined workflow. This list is easy to modify, with a simple drag and drop to change the order of the tab stops, add a field to the tab stop order, or remove a field from being 'tabbed' to.  **Figure 54: 'Tab Stop' Order** This image displays the 'Tab Stop' order in the forms designer, allowing for easy navigation of the form.	
38	The Bidder's System will provide validation checks at the time of each field entry as the default mechanism.	**Yes**
Bidder Response	WebLink ID utilizes field level validation; as such, each field can be individually checked for proper data entry. Validation for text entry fields is accomplished with regular expressions (regex). Below is a screen shot of a field validation regex.	

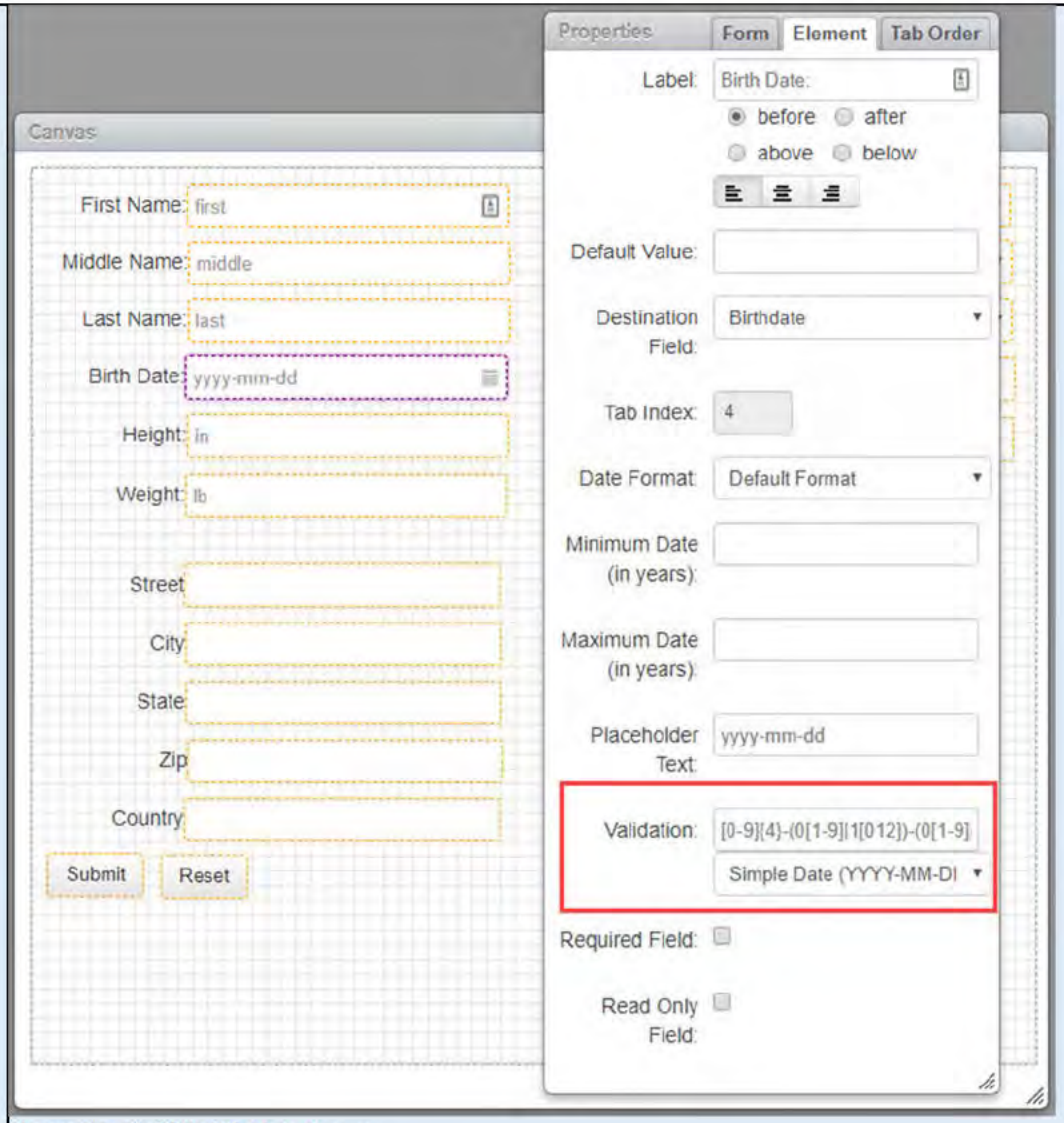
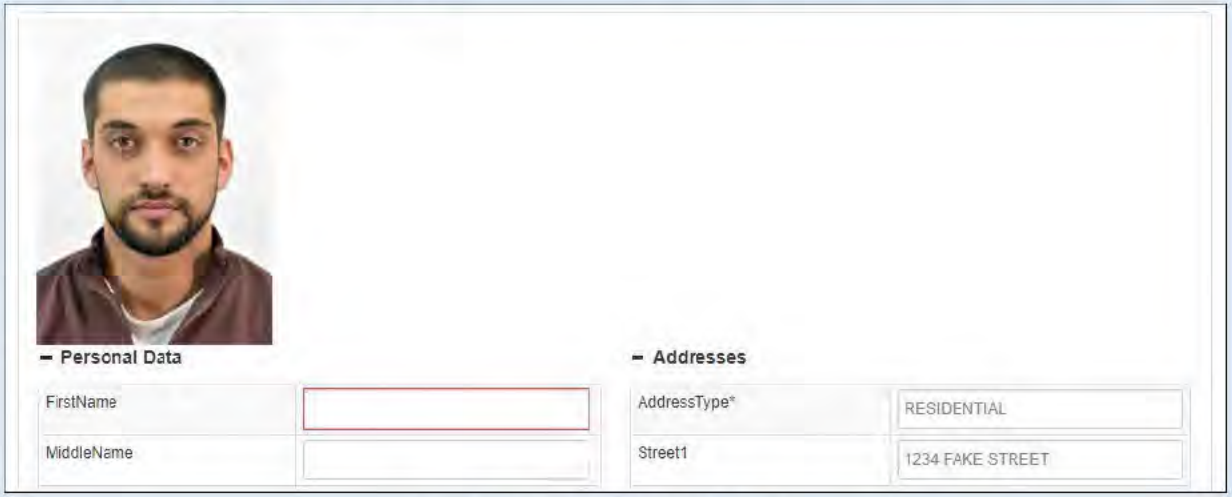


Figure 55: Field Validation Regex

39	The Bidder's System will identify invalid entries to the User as immediately as possible.	**Yes**
Bidder Response	In the event an entry does not match its validation criteria, as soon as the operator tabs or moves off the field, the field can display either red text, or a red outline around the field to notify the user that the field does not pass its validation criteria and the form or step will not be able to be saved.  **Figure 56: Invalid Entry Notification**	
40	The Bidder's System will be designed to include only the necessary information and functionality on screens and will be based on the User's access level and the User's configuration.	**Yes**
Bidder	VALID will work with the DMV staff to identify the fields needed for each credential type, as the types of credentials will require different collection of information. The enrollment workflow will dynamically display the fields needed for the specific credential being requested. Fields not needed for the specific credential will be hidden from the operator.	
41	The Bidder's System will provide templates for data entry with identified mandatory and optional data fields.	**Yes**
Bidder Response	WebLink ID supports the display of sample data for each field, as well as notifying the operator as to which field is required, and therefore which fields are optional. In the image below, the sample text displayed in grey is informative, and not data saved to each record, the mandatory fields are displayed with an *. The mandatory field marker can be changed from an * to another character, or the edit box itself can be set to a color notifying the operator it is mandatory, as the DMV requires.	

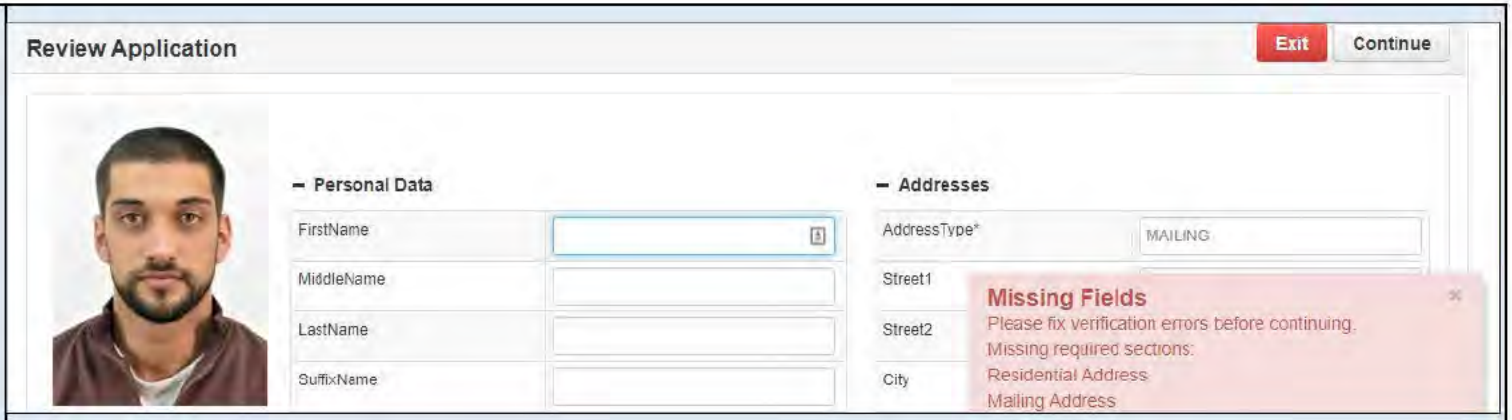


Figure 57: Missing Field Notification

42	The Bidder's System will allow incomplete data sets to be saved for completion of the workflow at a later time.	**Yes**
Bidder Response	At any point in time, an applicant's data can be saved for later retrieval. However, data on the form that does not pass validation criteria will not be saved. This process prevents the accidental saving of malformed or inaccurate data. Should the applicant need to leave the enrollment process and return later, the application will remain available up to a time frame decided by the DMV. Applications that have not been completed by the determined time span can be removed or archived, in accordance with the DMV's data retention policy.	
43	The Bidder's System will highlight and flag required and incomplete data fields.	**Yes**
Bidder Response	Fields on the enrollment form which are not complete (do not pass validation) or are required will be flagged in a manner for which the operator can readily identify the fields needing an update or completion. In the image below, fields that are improper and mandatory are displayed via a highlight.	

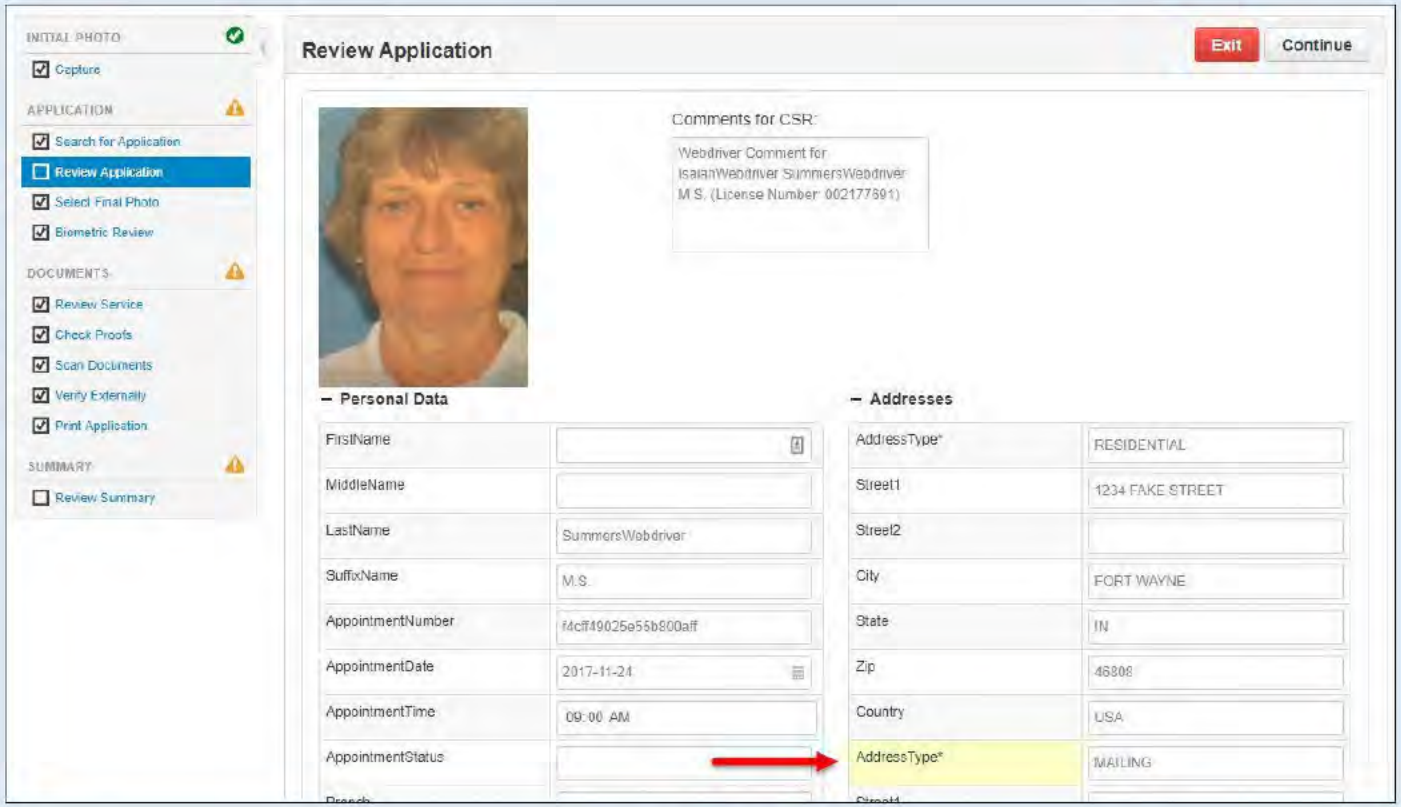


Figure 58: Required Field Flag

44	The Bidder's System will allow for the request of or entry of data from external devices (e.g. tablets, signature pads).	**Yes**
Bidder Response	During the enrollment process the applicant could be presented with questions or data entry items for which they must fill out directly during a questionnaire or 'sub-workflow' displayed to them on the Topaz signature panel. The result of these data entry options will be properly marked in the enrollment workflow, on the screen for the operator to verify. Some common options might be whether the applicant wishes to be an Organ Donor, or whether they wish to receive a Mobile DL/ID. These responses would be shown on the enrollment form.	

45	The Bidder's System will maintain a record (e.g. audit trail) of all additions, changes and deletions made to data in the system. This should be readily searchable by user ID or member ID. This must include, but is not limited to: a) User ID of the person who made the change, b) date and time of the change, c) Physical, software/hardware and/or network location of the person while making the change, d) Information that was changed, e) Outcome of the event, f) Data before and after it was changed, and g) Which screens were accessed and used.	**Yes**
Bidder Response	WebLink ID and BioLink ID maintain robust audit logging functions. All creation, change, and viewing of applicant's information is logged. The audit logs can be made visible or exposed to the appropriate administrative staff, within the applications. Additionally, audit log reports can be created for viewing and exporting of audit information. The audit logs are filterable or searchable by multiple fields, including applicant ID, operator or user ID, time range, and task or function executed. Coupled with WebLink ID's version control, all information entered or edited, can be investigated. Every change to an applicant's data set is maintained including the start value and end value of the transaction, who conducted the transaction and the timestamp of the transaction. Audit logging and historical version control allow the DMV to readily identify 'who' did 'what' during each revision of the applicant's request for a credential.	
46	The Bidder's System will allow an authorized administrator to request the inclusion or exclusion of auditable events based on organizational policy & operating requirements/limits.	**Yes**
Bidder Response	VALID will work with the DMV staff to ensure all events required by the organizational policy and operating requirements and limits are properly part of the audit engine within the applications in this solution. By default, WebLink ID and BioLink ID audit all creation, viewing, and change of applicant data.	
47	The Bidder's System will be able to detect security-relevant events (as defined in NIST 800-53 moderate baseline, rev 4) that it mediates and generate audit records for them. At a minimum the events will include, but not be limited to: a) Start/stop b) User login/logout c) Session timeout d) Account lockout e) Member record created/viewed/updated/deleted f) Scheduling g) Query h) Order I) Node-authentication failure j) Signature created/validated, k) Personally Identifiable Information (PII) export l) PII import m) Security administration events n) Backup and restore o) Audit Event Types listed in IRS 1075.	**Yes**
Bidder Response	Standard audit log requirements as defined by NIST 800-53 and IRS 1075 are already part of the WebLink ID and BioLink ID application audit logging. These include, but are not limited to logging the following actions: [redacted]	

	[redacted]	
48	The Bidder's System will provide authorized administrators with the capability to read all audit information from the audit records in the following two ways: 1) The Bidder's System will provide the audit records in a manner suitable for the User to interpret the information. The Bidder's System will be able to export logs into text format in such a manner as to allow correlation based on time (e.g. Coordinated Universal Time [UTC] synchronization provide the capability to generate reports based on ranges of System date and time that audit records were collected. 2) The Bidder's System will be able to export logs into text format in such a manner as to allow correlation based on time (e.g. Coordinated Universal Time [UTC] synchronization).	**Yes**
Bidder Response	Both WebLink ID and BioLink ID enable the viewing, searching and filtering of Audit log data to operators, administrators or other roles defined by the DMV. Exporting the data in a .csv or similar format, complete with UTC timestamps of events, is an available option. The image shown below displays the 'Search Log' tab of the Audit Logs visible inside WebLink ID. This particular log displays every search executed in the system, can easily be filtered and exported.	

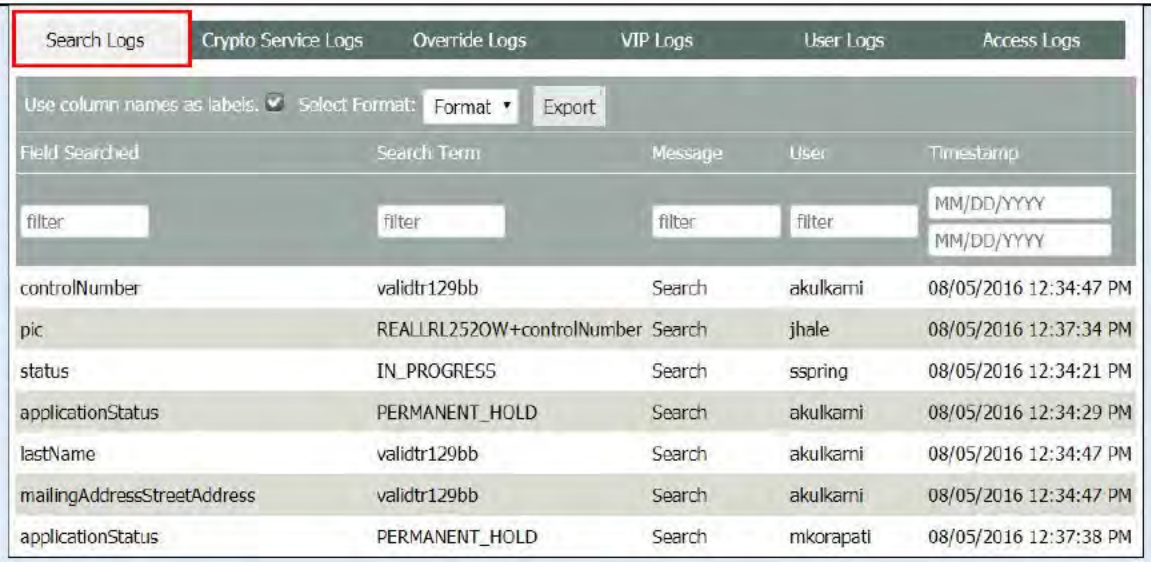


Figure 59: Search Log

49	The Bidder's System will be able to perform time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.	**Yes**
Bidder Response	All of the applications in the VALID proposal utilize NTP time synchronization to ensure each application is recording valid and accurate timestamps for all transactions and events. If the DMV has an NTP server, the VALID solution can sync with it, otherwise it will use the NTP server of the hosting provider, Amazon Web Services (AWS).	
50	The Bidder's System will prohibit all Users read access to the audit records, except those Users that have been granted explicit read access.	**Yes**
Bidder Response	Access to audit log information is permission-driven; and it is granular. VALID will work with the DMV to define appropriate roles for audit log access and the DMV will have the ability to affect who is granted the audit log roll.	
51	The Bidder's System will protect the stored audit records from unauthorized deletion.	**Yes**
Bidder Response	WebLink ID and BioLink ID do not allow any deletion of the audit log data, there is no tool or option inside the application to delete the audit records.	
52	The Bidder's System will prevent modifications to the audit records.	**Yes**

Bidder Response	WebLink ID and BioLink ID do not allow any modification of the audit log data; there is no tool or option inside the application to modify the audit records.	
53	The Bidder's System will be architected with no single point of failure, supporting a high-availability enterprise.	**Yes**
Bidder Response	VALID's proposed solution utilizes the best of today's technologies. It uses auto-scaling and fault-tolerance strengths only available through cloud-hosted solutions, while guaranteeing data security and monitoring beyond what most IT shops can realistically provide. In traditional 'on premise' solutions, heavy investment is required in hardware, even if using virtualization, to provide a truly fault-tolerant solution. Duplicates of each environment (production, QA, development) must exist in at least two different data centers to allow for true fault-tolerance, as one physical site might go down due to environmental issues. Inside each data center, each server must be made redundant to allow for single server or application failure. Given this paradigm, any single component is essentially replicated 4 times, at least 2 in the production and 2 in the disaster recovery data center. While there are ways to minimize the need to duplicate every server or virtual machine, the net cost is still large. By developing an application designed for true hosting environments, utilizing a large cloud-based provider becomes viable and in many ways the superior option. Amazon Web Services enable VALID to build a properly redundant set of environments, which are monitored real-time, 24 hours a day, 365 days a year. In the event of a single node's failure, additional nodes can be automatically brought online, without any human intervention. Additionally, AWS allows geographically different data centers to be used, separating each data center by hundreds of miles, such that one outage would not affect the next data center. This option is simply uneconomical for the traditional, on-premise model. All systems needed are effectively replicated among different data centers, and as such, data storage locations, while being instantly replicated among locations. More important, the multiple data centers are real-time primary systems, so that the load is shared between primary and the traditional 'disaster' site, ensuring the environments are not out of sync or not being utilized.	
54	The Bidder's System must be built so that there is a near linear relationship between each additional server added, and the additional load that can be accommodated (load vs. capacity added), up to specified limit.	**Yes**
Bidder Response	Another benefit of a hosted solution is the ability to auto scale resources as needed, in the event of a high traffic or high-volume timeframe, additional resources are automatically added to the application (more cpu, more ram), resources not being needed are removed or disabled.	

	In the traditional model, adding another 100 users might require adding additional VMs or hardware, which comes at both a human and a hardware cost, which the hardware might only be utilized for 1/3 of the day (operating hours), but the full price burden must be absorbed. Auto-scaling of the hosted environment eliminates this inherent waste of resources. Resources are only accessed as they are needed, and do not sit idle during off peak times.	
55	The Bidder's System will use fully redundant network and hardware. Hardware components (such as processor and memory) should have built-in redundancy to allow a second component to take over in the event of a failure in the primary component. Similarly, redundant paths should also exist for networks.	**Yes**
Bidder Response	VALID's proposed infrastructure requires only that the DMV host a Hardware Security Module (HSM) for establishing the hardware created VPN between the DMV's network and the hosted data center. VALID will provide redundant HSMs to ensure there is no single point of failure for the VPN needed.	
56	The Bidder's System will leverage virtualization to expedite disaster recovery. Virtualization enables system owners to quickly reconfigure system platforms without having to acquire additional hardware.	**Yes**
Bidder Response	The hosted solution employs virtualization. The application servers, database servers, web services servers, match nodes and cluster controllers are all virtualized. Additionally, within the hosted business rules, additional nodes and servers can be brought online automatically if any one node or server fail, or if the environment require more resources.	
57	The Bidder's System will have the ability to support either a Production and hot (real time replication) disaster recovery design or a multi host site Production design that would allow one site to seamlessly be offline and the other site would maintain service without interruption.	**Yes**

Bidder Response	VALID's issuance system was designed from the ground up to be robust and disaster proof. Experience has shown that secondary Disaster Recovery (DR) facilities that are only operated in the event of a disaster or for test purposes usually cannot adequately respond to an actual disaster. First, every disaster is different and they rarely comply with scenarios developed to design and test the system. In a genuine disaster situation, the best response occurs after carefully considering the circumstances – something for which there is little time and often fewer resources. Second, initiating production in the DR facility assumes that all IT equipment, data tunnels and physical materials are fully functional and ready to go "at the flip of a switch". This isn't usually the case – processes and card constructions have simply become too complex. Finally, initiating production at the DR facility assumes that that facility's personnel are familiar with the day-to-day nuances of production – the minor, undocumented procedures that make daily production flow smoothly. Without actually running the program every day, the DR facility doesn't develop these. The truth is, bona fide disasters are often accompanied by a second – hopefully smaller – disasters when the DR facilities are activated. [redacted]

58	The Bidder's System will include a disaster recovery plan and provide contingency plans for State lookup capabilities and online collaboration in the event of a disaster.	**Yes**
Bidder Response	[redacted]	

59	The Bidder's System will provide the ability to perform archival/incremental backups and the ability to perform open/closed database backups.	**Yes**
Bidder Response	VALID's proposed solution includes both backup and archival functions for the whole environment. A hosted solution, such as the one proposed, can conduct open database and server backups. Data retention of backups and archival of data will be defined with the DMV in accordance with the State's data retention policy and any federal requirements, if applicable.	
60	The Bidder's System will provide tools for managing an environment that supports both high availability and disaster recovery.	**Yes**
Bidder Response	VALID will provide access to the appropriate management tools for the hosted environment. As VALID is proposing a hosted solution, it will be VALID's responsibility to manage the environment's fault-tolerance and disaster recovery options and configurations. DMV staff can access the performance and resources tools to view system and resource utilization.	
61	The Bidder's System will include the capability to maintain all data according to state defined records retention guidelines (i.e. record schedule). General schedules can be found at: http://vermont-archives.org/records/schedules/general/. Specific retention disposition orders can be found at: http://vermont-archives.org/records/schedules/orders/. In general, document retentions range from 3 to 10 years.	**Yes**
Bidder Response	VALID's proposed solution will maintain all data according to the State's defined records retention guidelines.	
62	The Bidder's System will include the capability to maintain all images and electronic documents according to state defined document retention guidelines (i.e. record schedule). General schedules can be found at: http://vermont-archives.org/records/schedules/general/. Specific retention disposition orders can be found at: http://vermont-archives.org/records/schedules/orders/. In general, document retentions range from 3 to 10 years.	**Yes**
Bidder Response	VALID's proposed solution will maintain all images and documents according to the State's defined document retention guidelines.	
63	All software developed and delivered by The Bidder must be free of viruses, malware, backdoors	**Yes**
Bidder Response	VALID's software is guaranteed to be virus-, malware-, and backdoor-free. VALID will maintain the production, QA and development hosted environments, and for both maintenance and support will have access to the applications.	
64	The service provider must resolve Severe (defined as those issues or defects which completely prevent users from processing drivers licenses/identification cards) requests within 4 clock hours.	**Yes**

Bidder Response	VALID understands and agrees with this requirement. Software and hardware issues preventing the issuance of any credentials will be addressed within 4 clock-hours of report.	
65	The Bidder must resolve high priority defects within an average of 1 (one) days, but no more than a maximum of 3 (three) days.	**Yes**
Bidder Response	VALID understands and agrees with this requirement. Software and hardware issues deemed to be high priority will be resolved with an average resolution time of 1 day, with all high priority issues being resolved within 3 days. VALID and the DMV will define the which types of issues fall into which priority level.	
66	The Bidder must resolve medium priority defects within an average of 4 (four) days, but no more than a maximum of 7 (seven) business days.	**Yes**
Bidder Response	VALID understands and agrees with this requirement. Software and hardware issues deemed to be medium priority will be resolved with an average resolution time of 4 days, with all medium priority issues being resolved within 7 days. VALID and the DMV will define the which types of issues fall into which priority level.	
67	The Bidder must resolve low priority defects or request within an average of 10 (ten) days, but no more than a maximum of 14 (fourteen) days, unless mutually agreed upon.	**Yes**
Bidder Response	VALID understands and agrees with this requirement. Software and hardware issues deemed to be low priority will be resolved with an average resolution time of 10 days or less, with all medium priority issues being resolved within 14 days. VALID and the DMV will define the which types of issues fall into which priority level.	
68	The Bidders system shall be capable of integrating with active directory.	**Yes**
Bidder Response	[redacted]	
69	The Bidder's System will authenticate Users before allowing access to functionality requiring a login	**Yes**
Bidder Response	No function within WebLink ID or BioLink ID is available to users without them executing a login and authentication. There is no application function that exists outside a login and authentication session backed by an Active Directory server acknowledging the authentication.	

70	The Bidder's System will provide a mechanism to limit access to view/update information, based on User role, access rights, member consent, and program rules.	**Yes**
Bidder Response	Access to all functions, workflows and administrative tools within the proposed VALID solution's applications are roll-driven. VALID will work with the DMV staff to ensure the creation of all the roles needed for secure operation. Roles dictate what access an operator has to a workflow or tool, and within the workflow or tool, what permissions they have to the data or to the tool's functions. The DMV will maintain access to and administration of the existing users and the roles they are granted.	
71	The Bidder's System's interfaces will secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective.	**Yes**
Bidder Response	The VALID proposed solution protects the data, its integrity confidentiality, and availability. It does so by requiring authentication for every transaction, while encrypting data-at-rest, and in transport methods. No application, VALID or otherwise (API) communicates with the data without an authentication of the requesting users and server or system accounts. The design of the environments ensures system, and therefore, data availability when properly authenticated.	
72	The Bidder's System will provide the functionality that provides reliability for applications, services or message flows: ' Load balancing ' High availability ' Fault tolerance ' Failover ' In-order delivery ' Transaction support ' Execution prioritization ' Message prioritization. Tests for High Availability and Failover must be completed prior to the release to UAT.	**Yes**
Bidder Response	VALID's proposed solution is designed to provide true fault tolerance and reliability for each environment (Prod, QA, Dev), please refer to Questions 53 and 54 for further detail as to how VALID's solution meets these requirements. VALID understands that prior to User Acceptance Testing (UAT), a Systems Integration Testing (SIT) phase must be concluded, and agrees that stress testing for load balancing and reliability should occur during SIT testing. VALID's project team will work with the DMV team to ensure the test plans for SIT include Stress and Reliability tests.	
73	The Bidder's System will have the ability to use standards-based communication protocols, such as TCP/IP, HTTP, HTTP/S and SMTP. 'Protocol bridging: The ability to convert between the protocol native to the messaging platform and other protocols, such as Remote Method Invocation (RMI), IIOP and .NET remoting.	**Yes**
Bidder Response	Both WebLink ID and BioLink ID utilize standard communication protocols such as TCP/IP, HTTPs and SMTP for communication. Both applications also have an API for direct communication via JSON/Rest or SOAP utilizing HTTPS. HTTP is not utilized due to its non-encrypted nature.	
74	The Bidder's System will seamlessly work with the technology and programs that act as glue, transforming among protocols, connecting to databases and linking pre-SOA Application Programming Interfaces (APIs) to the SOA backplane.	**Yes**

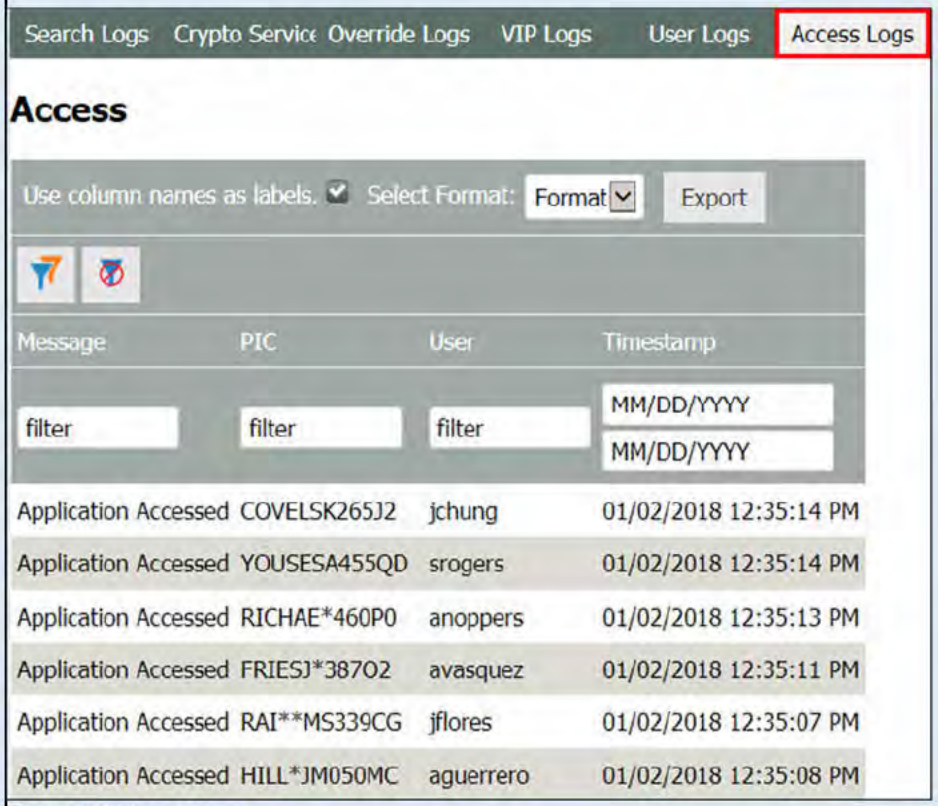
Bidder Response	[redacted]	
75	The Bidder's System will comply with all applicable State security policies and adhere to all legal, statutory, and regulatory requirements, as determined by Vermont leadership. See also standards mentioned in State of Vermont IT Attachment D.	**Yes**
Bidder Response	VALID's proposed solution complies with all applicable State security policies, and adhere to all legal, statutory, and regulatory requirements.	
76	The Bidder's System will implement security controls in accordance with all Federal and State security policy and regulations.	**Yes**
Bidder Response	VALID's proposed solution implements security controls in accordance with all Federal and State security polices and regulations.	
77	The Bidder will adhere to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.	**Yes**
Bidder Response	The proposed applications that are part of the VALID solution, adhere to the 'Fail Safe' principle, such that, in the event of a failure, there is no access to protected data, utilizing a 'default-deny' paradigm.	
78	The Bidder's System will maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information.	**Yes**
Bidder Response	VALID understands this requirement, and has designed its solution and applications in accordance with the understanding that this solution is essentially creating and hosting identities. Security architectures, storage, and communication protocols are selected to ensure the highest possible level of security for data and processes.	
79	The Bidder's System will provide the ability to identify certain information as confidential (e.g. PII, PHI, etc.) and only make that accessible by appropriately authorized Users.	**Yes**
Bidder Response	Each data element used as part of the enrollment or credential production process, and meta data gathered as part of the process of enrolling, verifying or producing a credential can be deemed maskable, or hide-able, from system operators or administrators not needing access to the data itself. The DMV staff can work with the VALID project team to ensure appropriate data is protected from view or export by in appropriate staff roles.	
80	The Bidder's System will restrict access to summarized information according to organizational policy, scope of practice, and jurisdictional law.	**Yes**

Bidder	VALID's solution does not allow access to summarized information by default. Access to all data and statistics must be specifically granted, the default access is 'none'. This 'default-deny' paradigm is the basis for ensuring no one has access to data they should not be privy to, regardless of role.	
81	The Bidder's System will provide the ability for authorized administrators to assign restrictions or privileges to Users or groups.	**Yes**
Bidder Response	The appropriate DMV administrators will be given access to assign and manage user permissions and roles within each application. These roles can map to Active Directory groups, such that management of the user groups happens only inside Active Directory management tools, or it can happen in both the VALID provided applications and AD management tools. The VALID project team will work with the DMV to select which paradigm works with the states' security policy for user and group management.	
82	The Bidder's System will support removal of a User's privileges without deleting the User from the Bidder's System to ensure history of User's identity and actions.	**Yes**
Bidder Response	WebLink ID and BioLink ID are capable of restricting or revoking a user's permissions without affecting any audit log data displaying that user's history of events and transactions. The user will lose rights, but the log data will still display the user account (if applicable), as the audit log data is not relational, or a series of 'joins' requiring the user to still exist in a user table for their history to be visible.	
83	The Bidder's System will provide the capability to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the Bidder's System.	**Yes**

Bidder Response	VALID's proposed solution includes a monitoring tool which provides system administrators a real-time view of the system's integrity, user requests, traffic volume, resource utilization and health. The monitoring tool has thresholds for alerts, and activity outside normal usage, as well as messaging capabilities for approaching any defined threshold or exceeding thresholds. Access to the system will be strictly monitored, any derivation or attempted access from outside the defined 'white-list' of locations will send initial alerts, and the solution is capable of threat analysis and shutting down any access requests from unsolicited or non 'white-listed' services or locations, instead of simply reporting unauthorized access, it will prevent it.

Figure 61: System Monitoring

84	The Bidder's System will provide the capability to identify and report on inappropriate access to information in the Bidder's System, based on User defined criteria.	**Yes**

Bidder Response	VALID's proposed solution will publish usage and access reports, with suspected and blocked threats, to specifically identified administrators. VALID will work with the DMV to determine which reports go to which recipients during the Design phase of the project. During the UAT phase of the project, these users will need to verify the reports are acceptable. Another tab from the Audit Log tool inside WebLink ID displays the records accessed, by which user, and the given timestamp.  **Figure 62: Access Logs**

85	The Bidder will provide third-party conducted penetration tests on production releases of the externally accessible web application as requested by the change control board entity. The reports shall be provided to the security officer upon request.	**Yes**
Bidder Response	VALID has had no security breaches at any of its facilities at any time. VALID employs a full-time analyst who monitors the network and systems for abnormalities or access alarms. VALID's secure facilities conduct internal and external penetration testing, vulnerability reviews, and application testing/scanning. [redacted]	
86	The Bidder will not transmit or store any Personally Identifiable Information (PII) using publicly available storage over the Internet or any wireless communication device, unless: 1) the PII is "de-identified" in accordance with 45 C.F.R § 164.514(b) (2); or 2) encrypted in accordance with applicable law, including the American Recovery and Reinvestment Act of 2009 and as required by policies and procedures established by VT Information Security Officer.	**Yes**
Bidder Response	VALID is fully compliant with the Federal Driver Privacy Protection Act (DPPA) of 1994, Public Law No. 103-322 codified as amended by Public Law 106-69, as well as the American Recovery and Reinvestment Act of 2009. VALID has four major applications that will handle the Vermont DMV data: (1) WebLink ID, (2) BioLink ID, (3) the Factory Allocation Manager (FAM) and the (4) Job Control System (JCS). WebLink ID and BioLink ID are two web-based applications that can run within the Vermont data center ("on premise" software) or may be hosted in a VALID data center. VALID hosts the FAM and JCS in its Data Centers and Card Personalization Facilities (CPFs). VALID will not transmit or store any personally identifiable information (PII) using publicly available storage over the Internet or any wireless communication device. **Secure Communication between VALID and Vermont DMV Data Centers** [redacted]	

	[redacted] [redacted] **Secure WebLink ID and BioLink ID Data at Vermont DMV Data Center** [redacted] **Secure JCS and FAM Data at VALID Data Center** [redacted] **JCS Application Security**

	[redacted] [redacted] **FAM Application Security** [redacted] [redacted]	
87	The Bidder will perform Security Impact Assessments prior to releasing solutions into production.	**Yes**
Bidder Response	Prior to any production release, VALID will undergo a rigid set of checks in collaboration with the Vermont DMV to ensure that everything is ready to move into production. That effort will include a thorough Security Impact Assessment	

88	The Bidder will ensure that all credentials are produced in a highly secure facility located within the Continental United States.	**Yes**
Bidder Response	Since VALID manufactures and personalizes bank cards in addition to DLs and IDs in our Card Personalization Facilities (CPFs), the facilities are audited annually by representatives of the Payment Card Industry Security Standards Council (PCI SSC) as well as individually by certain member institutions. In fact, it is fair to say that at least one VALID facility is undergoing an audit nearly every week of the year. The PCI SSC was formed in 2006 by American Express, Discover, Japan Credit bureau, MasterCard and Visa. At this writing, the PCI SSC lists 935 Participating Organizations of which 58 were Financial Institutions. Rigorous standards exist for Data Security as well as Physical Security. An overview of the PCI Security Standard can be found at: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf.	
89	The Bidder will ensure that all employees with access to the system, system components, State data, or responsible for the production of identification cards have undergone a background check.	**Yes**
Bidder Response	VALID has planned its staffing requirements by the project phase. A full list of staff who will be working on the CPS project by phase will be made available to Vermont DMV upon request. VALID's security policies require that prior to their hiring, all employees, full-time, part-time or temporary, go through criminal and credit background checks prior to hire, at both local and national levels conducted by an independent third-party service provider. Additionally, VALID performs and reviews background checks of current employees on an annual basis. Upon review and approval of the background checks, VALID's Human Resources and Security Department provide security training for all new / temporary employees. Access policies are reviewed with all employees during the mandatory Employee Security Training. Annually, VALID's security policies are reviewed and approved by the executive committee. Mandatory Security Training is held annually for all employees.	
90	Where available and agreed between the Bidder and the State, the Bidder will use State templates for project management deliverables.	**Yes**
Bidder Response	VALID is agreeable to using the State's templates for the Project Management deliverables. The VALID project manager will review those templates with the DMV and will incorporate them into the VALID project management process.	

91	Contractor will work collaboratively with the State Project Manager to develop agreed upon project management deliverables; such as Project Management Plan, Communication Management Plan, Status reports).	**Yes**
Bidder Response	The VALID PM will work directly with the State Project Manager to develop agreed-upon project management deliverables, such as schedules, plans and reports.	
92	The Bidder will advise the State and Contractor management of progress in meeting goals and schedules contained in the work plans as well as any risks and issues during weekly progress meetings attended by the Bidder and the State. These may include walkthroughs of selected deliverables as requested by State staff.	**Yes**
Bidder Response	During weekly progress meetings VALID will provide ongoing updates, will offer advice to help meet goals and schedules, will identify the risks associated with each undertaking, and will participate in in walkthroughs of selected deliverables, as requested by the State staff.	
93	The Bidder will develop and provide written progress reports to the State Project Manager. Reports shall contain status meeting agenda items, Progress of each task/activity, Action items and decisions from the previous meeting. - Problems encountered, proposed resolutions, and projected completion dates for problem resolution. - Planned activities for the next two reporting periods. - Status of contractually defined deliverables, milestones, and walkthroughs scheduled in the project schedule. - Updating of information on a weekly basis in the State project and portfolio management tool. - Other information as needed (per Contractor or the State). Frequency of periodic reports can be adjusted during the course of project as agreed by the State and Contractor.	**Yes**
Bidder Response	VALID will develop and provide weekly progress reports which address the topics mentioned above, and they will be submitted to the DMV at DMV-designated time frames. VALID will support other report periodicities, as needed. The VALID PM will incorporate all the action items and activities mentioned above. VALID will use the State's templates and portfolio management tools.	
94	If the Bidder must substitute key staff during the project, The Bidder will submit to the State, in writing, the reason for the change and provide a completed staff experience reference form and resume for the substitute personnel. The State will either approve or reject the substitution.	**Yes**

Bidder Response	VALID acknowledges that the replacement of its designated key personnel will occur only with the approval of the State. If VALID must provide an alternative key person, then VALID will submit to the DMV in writing the reason for the change and a completed staff experience reference form and resume for the substitute person, which the State will approve or disapprove.	
95	The Bidder will describe their approach regarding the project documentation repository. The Contractor is recommended to align with the State's document repository. In case the Contractor cannot, they must provide justification as to why their proposed repository works well in the best interests of the State.	**Yes**
Bidder Response	It is VALID's intent to align its approach regarding project documentation, terminology and procedural processes to that of Vermont DMV.	
96	The Bidder will develop a technical infrastructure document which describes all of the hardware, system software and tools necessary for each of the environments proposed.	**Yes**
Bidder Response	VALID agrees with this requirement and plans to provide technical infrastructure documentation describing the system, hardware, software and tools needed for each of the Production, QA and Development environments. These documents will be part of the Solution Design Document, and will be delivered before SIT, and revised as necessary post SIT and before implementation.	
97	The Bidder will provide a Change Management Plan. The Change Management plan will detail any differences in the approach to Change Management during the various phases of the project as well as the post implementation/operations phase of the contract.	**Yes**
Bidder Response	VALID will provide its Change Management Plan to the Vermont DMV for its review and approval. VALID understands that any s differences in approach to change management by project phase and/or ongoing operations should be detailed in the change management plan.	
98	The Bidder will develop an environment configuration manual that describes the environment installation and configuration necessary for each of the environments.	**Yes**
Bidder Response	VALID agrees with this requirement and plans to provide an environment configuration document for each of the proposed environments (Prod, QA and Development) detailing the configuration of each of the hosted environments. These documents will be part of the Solution Design Document, and will be delivered before SIT, and revised as necessary post SIT and before implementation.	

99	The Bidder will provide a data dictionary, data models, data flow models, process models and other related planning and design documents to the State.	**Yes**
Bidder Response	VALID agrees with this requirement and plans to provide the following documents to the State: 1) Data Dictionary 2) Data Models 3) Data Flow Models 4) Process Models 5) Other planning and design documents These documents will be part of the Solution Design Document, and will be delivered before SIT, and revised as necessary post SIT and before implementation.	
100	The Bidder will develop (in cooperation with the State) and execute a Knowledge Transfer and Training Plan that describes roles and responsibilities of the State and Contractor and the approach for bringing managers, end Users, and technical personnel to an appropriate level of understanding with The Bidder's System.	**Yes**
Bidder Response	VALID will collaborate with the State to create and execute a Knowledge Transfer and Training Plan that will layout our joint objectives, mutual roles and responsibilities, as well as our approach to ensure that all the DMV staff – management, operational and administrative end-users and technical personnel – are proficient and confident in using VALID's credentialing system. A sample Knowledge Transfer and Training Plan is provided in **Attachment 10.**	
101	The Knowledge Transfer and Training Plan will address and describe, at a minimum: - Training goals/standards and the specific plan for training technical personnel and end Users. - Size of population and types of roles that need training - Strategy for providing training early in the project to allow the training goals to be implemented throughout the project life Phase. - Tasks, deliverables and resources necessary to complete the training effort and identify tools and documentation that will be necessary to support proposed effort. - Types of training, the specific courses and course materials, the training approach for both technical personnel and end Users, and how training effectiveness will be measured and addressed. - Deliverables to support initial and ongoing training including User manuals, System manuals, and on-line help and training materials for technical/non-technical personnel. - Knowledge Transfer to enable the State personnel to operate, maintain, configure and modify The Bidder's System including operation of the testing tools, supporting infrastructure, and security as agreed between the State and Contractor. - Metrics for tracking progress in achieving training and knowledge transfer objectives. - Reporting progress of training and knowledge transfer activities. - Additional training for technical staff on development, reporting and maintenance including processes and tools as needed.	**Yes**

Response	In collaboration with the DMV, VALID will prepare a Knowledge Transfer and Training Plan, which describes the formal processes to position the DMV staff to run, maintain and proficiently support the DL / ID system solution in a self-sufficient manner. VALID will collaborate with Vermont DMV to determine the staff groups to be trained and the types of training that is best for each group. For example, the end users at the DMV locations have limited blocks of time that they can train. Regarding KT, the most important planning is determining what skills / knowledge needs to be transferred, who should participate in the KT program, and how we will attain the KT objectives. VALID will follow the preferred DMV processes and terminology for all project plans. VALID views Training and Knowledge Transfer (KT) as two distinct processes. Training on the VALID system will provide an understanding of the processes and the skills needed to proficiently support the DL/ID system solution. KT is a process whereby experienced individuals share or distribute their knowledge, providing inputs into problem-solving. KT might be viewed as a roles-based "experience transfer" that enables the application of the skills learned during Training. Thus, VALID plans to establish a formal KT program that enables senior VALID staff to mentor selected VT DMV staff regarding the skills necessary to use, manage and support the DL/ID system solution. VALID has placed its suggested Knowledge Transfer and Training Plan in **Attachment 10.**	
102	The Bidder will submit all training packages to the State for review and acceptance at least seven (7) calendar days prior to the beginning of scheduled training.	**Yes**
Bidder Response	VALID recommends that its walkthrough off all training packages to the State occur at least a month prior to the beginning of scheduled training, so that any corrections or adjustments can be made efficiently and without rushing. Of course, should issues be uncovered later in the phase, after training has begun (e.g., the need for a special Quick Reference Guide), then that item can be retrofitted to the DMV end-users.	
103	The Bidder will provide all training materials developed for The Bidder's System to the State. Those materials will become the property of the State and may be modified and duplicated by the State.	**Yes**
Bidder Response	Everything developed by VALID for the training of the DMV staff will be made available to the Vermont DMV, which can modify and replicate as needed.	
104	The Bidder will provide electronic copies of all training materials in a format that can be easily accessed, updated and printed by State staff using software for which the State owns licenses, prior to deployment onto the staging platform. This includes but not limited to CDs/DVDs, and online.	**Yes**

Bidder Response	All of VALID's training materials have an electronic distribution component. VALID will work with the DMV to determine the optimum media and format to distribute the training materials to the DMV staff. Whichever media solution is selected, VALID will ensure that it can be easily accessed, updated, and printed by DMV Staff.	
105	The Bidder will assist the State with testing and release preparation in the pre-production environment.	**Yes**
Bidder	VALID will assist Vermont DMV with all testing and release preparation in the pre-production environment. VALID's Quality Management team heavily executes test cases before a potential release. Further, release preparation will include staging on the QA server where additional testing occurs; and VALID uses a pre-production checklist to ensure that all steps are executed prior to production switch-over. All client-specific interfaces and customizations will exist as separate source code projects with a different lifecycle managed by VALID. These use a WebLink ID API that rarely (if ever) changes, which future-proofs compatibility between the interface and future changes in WebLink ID. In the unlikely event that the production system(s) need to be reverted to a previous version, version rollback poses very little issue for WebLink ID and BioLink ID, as they are web-based products that are centrally-managed and version-controlled	
106	The Bidder must produce and execute an Implementation Support Plan.	**Yes**
Bidder Response	VALID has produced an Implementation Plan, which includes our plan for support and maintenance. It is in **Attachment 6**. VALID will work with DMV to made any adjustments needed in this plan, prior to execution.	
107	The Bidder must provide support staffing information such as the proposed number, ratios, duration, and roles/responsibilities for on-going support (as identified in previously submitted implementation approach and plan).	**Yes**
Bidder Response	VALID will provide to Vermont DMV suggested support staffing information for the implementation and ongoing operational support.	
108	The bidder shall work with the State of Vermont (SOV) to develop security and infrastructure to ensure SOV is complying with the Interconnection Security Agreement (ISA) required by Department of Homeland Security	**Yes**
Bidder Response	Yes, VALID will be delighted to assist, as we did with the State of Washington. The ISA formally records the security protections that must operate on interconnected systems, and it documents the security understandings between the DHS and the State; and it will include descriptive, technical, procedural and planning information. VALID will assist the State of Vermont in working with the DHS to establish a new ISA, and ensuring compliance.	

4.5 Data Compliance

Contractors and their solutions must adhere to applicable State and Federal standards, policies, and laws based on the type of data that will be stored, accessed, transmitted and/or controlled by the solution. If the "Type of Data" column is checked below, respond "Yes" or "No" in the "Comply" column and provide an explanation on how you comply in the "Bidder's Description of Compliance" column.

Type of Data	Applicable State & Federal Standards, Policies and Laws	Comply	Bidder's Description of Compliance
☐ Publicly available	▪ NIST 800-171		
☒ Confidential Personally Identifiable Information (PII)	✦ State law on Notification of Security Breaches ✦ State Law on Social Security Number Protection ✦ State law on the Protection of Personal Information ✦ National Institute of Standards & Technology: NIST SP 800-53 Revision 4 "Moderate" risk controls ▪ Privacy Act of 1974, 5 U.S.C. 552a.	YES	VALID does not release or use PII data provided by the state agencies for any purpose other than verification of accuracy of the information prior to issuance of DL or ID credentials as permitted by the DMV or applicable State and Federal policies. As a PCI certified service provider to some of the major financial institutions in the country, our facilities are regularly audited by independent third parties for physical, logical and penetration security compliance. VALID has instituted internal policies that we believe are aligned with the listed Standards, Policies and Laws. VALID policies for protection of sensitive data, including PII, are documented in the following policy documents, available for examination by the DMV upon request after notice of contract award. 1. IT Security Incident Response and Forensic Plan 2. Data Compromise Policy 3. Data Incident Response Policy
☐ Payment Card Information	✦ Payment Card Industry Data Security Standard (PCI DSS) v 3.2		
☐ State	• Annual SSAE 16 SOC 2 Type 2		

☐ Federal Tax Information	✦ Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies: IRS Pub 1075		
☐ Personal Health Information (PHI)	✦ Health Insurance Portability and Accountability Act of 1996: HIPAA ✦ The Health Information Technology for Economic and Clinical Health Act HITECH ✦ Code of Federal Regulations 45 CFR 95.621		

Type of Data	Applicable State & Federal Standards, Policies, and Laws	Comply	Bidder's Description of Compliance
☐ Affordable Care Act Personally Identifiable Information (PII)	✦ Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies: IRS Pub 1075 ✦ Minimum Acceptable Risk Standards for Exchanges MARS-E 2.0		
☐ Medicaid Information	✦ Medicaid Information Technology Architecture MITA3.0 ✦ Code of Federal Regulations 45 CFR 95.621		
☐ Prescription Information	✦ State law on the Confidentiality of Prescription Information		
☐ Student Education Data	✦ Family Educational Rights and Privacy Act: FERPA		
☒ Personal Information from Motor Vehicle Records	✦ Driver's Privacy Protection Act ("DPPA") 18 U.S.C. Chapter 123, §§ 2721 – 2725	Yes	VALID understands the significance of the DPPA and the sensitivity of PII data that will be entrusted with our organization in providing credentialing services through the course of the VT DMV contract. We exchange protected data with many current public and private customer entities including state governments and financial institutions. Our card personalization facilities are PCI compliant. VT resident's PII data will be processed and stored in PCI compliant environments. All PII data will be encrypted, in transit and at rest.
☐ Criminal Records	✦ Criminal Justice Information Security Policy:		

Part 5: VALID's Implementation/Project Management Approach

1. Describe the approach you would recommend for project managing this engagement

We approach ID/DL projects as a seven-phase effort. Within each phase there are a number of key activities that will take place. The seven phases are listed and discussed in detail below:

- Phase 1 – Project Initiation & Planning
- Phase 2 – Requirements Gathering (Fit / Gap Analysis)
- Phase 3 – System and Card Design
- Phase 4 – Development and Configuration
- Phase 5– Verification (Testing) and DMV Training
- Phase 6 – Project Implementation (Transition and Deployment)
- Phase 7 – Maintenance and Ongoing Delivery & Support

Phase 1 – Project Initiation & Planning

Our initial planning efforts would begin with a project management plan that integrates all the project plans from the various project knowledge areas in an integrated, consistent, and coherent set of documents. It will become the baseline against which to measure project performance. It will describe the steps associated with executing, monitoring and controlling, and closing the project. These project plans are important because they will define the work that we will do throughout the project.

Quality Management – VALID plans quality up-front. We will plan how we conduct our quality assurance and quality control activities, and we will match them to the needs of the DMV, and its QA/QC representative(s) (if applicable). It is during the project planning phase that VALID creates quality checklists, its process improvement strategies, and its performance measurements or metrics that will enable VALID to collect, measure, compare and interpret the project's performance. VALID will provide the DMV with a Quality Management Plan.

Requirements –Throughout the Fit/Gap phase, VALID will meet with the DMV to gather and refine requirements for the new DL/ID sytem. Once we have a validated set of identified requirements provided us by the DMV, we will organize them into a Requirement Traceability Matrix (RTM) to ensure that we identify each requirement, follow them as they potentially undergo change, and align them with the stakeholder needs. The RTM will trace the requirements throughout the project life cycle. The RTM add value by associating each requirement to its business objectives.

Risk Management – Every project must be aware of risks. It is during the planning process that we will identify risks to the project, will perform a quantitative and qualitative risk analysis, and will produce a risk register which establishes the likelihood and impact of each primary risk. VALID will update the risk register in concert with collaborative discussions with the DMV. We prefer to review the risk register twice per month throughout the project. Our overall goal is to progressively reduce the project's exposure to events that threaten the timely delivery of the solution.

Schedule – It is during Project Initiation and Planning that we will define our activities and will plan the project milestones. We will sequence activities, will estimate our staffing resources along with activity duration, and we will finalize the project schedule. This last effort will be finalized collaboratively with the DMV, and the result will be a baselined schedule. Throughout the project, we track the baseline schedule against the current schedule. Managing the schedule continuously helps resolve project risks. VALID has provided a sample schedule in **Attachment 4.** It is VALID's intent to finalize the schedule in collaboration with the DMV.

Communications – During this phase we will establish our communications procedures for both informal and informal communications. We will review what information is needed, when it will be needed, and in what format. Communication planning includes both scheduled and unscheduled meetings, reporting (format, content and periodicity), and information sharing with all stakeholders; we will agree on escalation procedures, document management, access, retention and archival requirements.

Change Management – Change management describes the process to identify, document, review, approve, track, and report the status of all change requests/change orders. VALID has sample change management forms it can provide to the DMV, or work with the DMV's own forms to forge a change management solution that is efficient and easy to understand. VALID would welcome the opportunity to worth with the DMV to prepare a mutually agreeable Change Management Plan.

Issue Log – VALID views issues as potential barriers to success. Because we want to deliver information to the project stakeholders in a timely and effective manner, we will establish an issue log in which all issues can be clarified – with an owner's name, a targeted resolution, and a description of the impact to the project. Moreover, all issues wll be tracked to resolution.

Training – As we plan the project, we will thorouoghly review the training needs. That entails a detailed understanding of the DMV's hierarchy of needs (e.g., end users of the system, technical support vs. administrative personnel), the composition and disposition of the staff to be trained, the modes of training needed (e.g., in-person, web-based, classroom, hands-on, etc.), and the documentation needed (e.g., user manuals, quick reference guides, training handouts, evaluation forms, etc.). Also, we can plan any special activities needed that closely align with training such as equipment installs.

Monitoring and Control – It is during this planning phase that we will define our monitoring and control processes to be used throughout the project. This obviously will include project governance, but also will describe the process for the DMV to verify and accept deliverables, as well as the periodicity and method to document lessons learned, and how we should apply best practices. Throughout the project we will monitor and control our project work by doing the following:

- Comparing actual data to baseline estimates
- Determining when corrective action or preventive action is needed
- Keeping risk data current
- Forecasting project progress
- Tracking status of approved changes as they are implemented

Procurement – Last, we will plan the procurement effort. VALID will make plans to procure all the hardware, software, and peripheral items that will be needed by VALID and by the DMV, including supplies. We have a procurement team within VALID who will order the equipment from proven vendors. Prior to the equipment being procured, VALID will send the purchase order to DMV for its approval.

This phase, like all of VALID's project phases, will end with a focus on Lessons Learned, Scope Verification and agreement by the DMV (e.g., certification of phase complete), and an update of all project documents.

Phase 2 – Requirements Discovery; Data Gathering & Fit/Gap

In any project, VALID makes a series of assumptions that need to be verified; and the DMV will have an expectation that it has selected a vendor who will efficiently leverage its experience with industry best practices, and it should guide the DMV toward a practical realization of its objectives. Given a variety of design considerations, VALID will help the DMV understand the advantages and disadvantages of <u>each</u> potential course of action. The following paragraphs describe <u>how</u> we will verify requirements and gather data, and then how we will synthesize the gathered data against our standard capabilities and develop the gap that we have to bridge.

In most situations VALID will simply configure its internal products to meet the needs of the DMV, as that is how our WebLink ID and BioLink ID products were designed. However, in some cases there may be a need for some software development such as for new interfaces, or a re-configuraiton of our WebLink ID product, or the acquisition of additional equipment. Thus, during Phase 2, Discovery and Fit/Gap, VALID gathers requirements and clarifies needs. If the DMV has pre-defined its Statement of Work with requirements and deliverables, VALID will still need to validate those requirements, and plan how it will meet its deliverables. VALID will meet with the DMV staff to verify any gaps between the DMV's needs and VALID's standard solution. Gaps can include new requirements not previously understood or recently surfaced, decisions not yet made, or the need for interfaces or extensions that are not pre-existing. VALID will identify all known gaps, and will document all functional requirements. As a result of that effort, VALID will produce a FIT/GAP document, identifying the gaps and citing ways VALID will resolve the gaps. It will continuously garner feedback from DMV, and will update this document on an ongoing basis until all gaps are resolved. Additionally, VALID will create a Requirements Traceability Matrix (RTM), which will be posted for DMV access at all times. Its update will be an onging function through Design, Development and Verification.

Phase 3 – System and Card Design

During this phase VALID will address data layouts, interfaces, extensions (e.g., development to our existing product), system reports, process flows, and data conversion and migration planning, concluding with an approved Solution Design Document. The card design will undergo an iterative series of steps that will conclude with approved card prototypes. The following describes how VALID will accomplish its design, development and configurations.

Interfaces – All needed interfaces will be identified, defined (via a functional and technical specification), developed, tested, and validated.

Extensions – These are constructs that close the functional gap between the standard solution and the business or technical requirements of VT DMV. As with interfaces, extensions will be identified, defined, developed, tested and validated. This effort includes a JAD (Joint Application Design) session or set of similar types of discussions with the DMV.

Application-Level Security – VALID has embued in its solutions a set of extensive security features. Application-level security focuses role-based access to the DMV's authorization systems. VALID might provide templates and samples, create and certify security matrices, perform security audits, and integrate existing authorizations and business processes, as needed. This process and any decisions to be made will be reviewed with the DMV.

Performance Standards Management – This will effectively establish and achieve performance criteria, primarily as measured end-to-end, and response times. VALID will prepare with the DMV the performance standards during the Design phase; and we will implement them during the Verifcation phase.

Technology Environments – This is primarily a requirement of a central-issuance environment. Its purpose is to ensure that all VALID-hosted environments (such as testing, QA, Production, etc.) have been properly established and configured. These environments will be discussed with VT DMV to ensure that the technology environments match directly to the DMV's needs.

Card Design – There is almost always the need to undergo a card design process or at least to review the current card design. There are considerations of card composition, security features, functionality, layout, and special featuers which all need a thorough review. These card design reviews tend to be iterative in nature, obtaining ongoing feedback and making adjustments accordingly. This effort typically will conclude with an approved card prototype and the trial printing of the approved card design.

During the System Design, VALID will produce a Solution Design Document (SDD), with an assessment of changes required, a data dictionary, the sources of data elements, and a list of interfaces, extensions and reports. Card design is generally not tied to other project initiatives and processes, and thus it can be methodically progressed forward. To allow for plenty of discussion and validation, VALID prefers to begin its card design effort early in the project.

VALID will update its project documents, and will review the completion of this phase with the DMV.

Phase 4 – Development and Configuration

This phase includes all build activities for the new solution, DR/BC planning, and VALID's procurement and factory preparation. During this phase, VALID will begin the data conversion and migration efforts as well as complete the site surveys.

Development (Build) – VALID will develop any necessary interfaces or extensions, build its reports, and address enterprise data integraton requirements. Everything VALID does will pass through our QA process. All interfaces, extensions and reports will be validated in alignment with the the DMV's participation.

Reports – VALID will provide a standard set of reports, including compliance, managerial, and operational reports. During the previous phase, VALID would have reviewed its reports with the DMV to determine if these reports met the DMV's needs, or if additional reports needed to be produced. If necessary, custom reports will be produced in this phase of the project. In addition, all reports that did meet the DMV's professed needs are re-examined in detail. This occurs in full collaboration with the DMV.

Data Conversion and Migration (DCM) – With any ID/DL project data conversion and migration is a critical determinant to project success. Data will originate from multiple sources, and the data will need to be consolidated into a defined file layout. In addition to consolidated records, VALID will need to obtain the business rules (logic) relating to existing systems and data. VALID must usually conduct multiple iterative sessions with the DMV staff to finalize a comprehensive list of data elements to be converted, and to agree on a conversion strategy.

Site Surveys – To prepare for an efficient and successful installation, VALID field technicians will travel to the field offices and conduct site surveys, focusing on such things as adequate electrical power, working space for the equipment to be installed, location limitations, etc. The results will be documented, reported, signed off and posted. Any deficiencies or concerns will be noted. This will occur early enough in the project so that the field offices will be given sufficient time to remedy any issues.

Disaster Recovery and Business Continuity (DR/BC) – VALID maintains an up-to-date DR/BC plan, which it can customize to meet the needs of the DMV. VALID is cognizant that the recovery point objective (RPO) and recovery time objective (RTO) varies by customer; but VALID is well within the requirements of Vermont DMV. Because it maintains multiple card processing / card personalization factories with excessive capacity for growth, VALID can provide some unique solutions to support its customers' needs. VALID will review with the DMV the DR/BC strategies to meet its needs, and will test those strategies well before the "Go Live" date. One key point: VALID maintains hot recovery sites for its ID/DL state customers; and it can send some or all of its card processing batches to an alternate site for processing in a matter of minutes.

VALID will update its project documents, and will review the completion of this phase with the DMV.

Phase 5 – Verification (Testing) and Training

This phase not only includes all the formal testing activites that must take place, but also includes parallel activities in preparing the DMV's staff and their facilities for project transition. Thus, we include training in this section. This section provides insight into how VALID performs its testing and prepares for and conducts training. Additionally, we will complete the data conversion and the data synchronization efforts. Testing – This phase includes the following types of testing:

- **Functional Testing** – To ensure that individual functions within a component of the central issuance solution perform within the DMV business and technical requirements. The functional testing is performed in order to ensure that DMV functionality requirements are met for correctness, procedural accuracy, aesthetic value, user friendliness and consistency. It also reveals how specific components will function. Additionally, VALID conducts permutation (perm) tests to verify that we have enacted the numerous business rules for handling the DMV names (those business rules will be determined during the card design process).

- **Systems Integration Testing** – To ensure that multiple DL/ID System solution modules and their associated interfaces, extensions and reports, operate as intended, and that data integration across the DMV enterprise meets the DMV's data integration requirements. Integration testing verifies that all applications and sub-systems are installable in reproducible manner, are fully and properly integrated, and the entire system works as a whole in compliance with identified functional specifications and design documents.
- **Security Testing** – To ensure all components of the DL/ID System are accessible only by authorized users, and that our DL/ID system solution is not vulnerable to outside penetration attacks, and that all interfaces, extensions and reports meet applicable secure coding and testing guidelines. The Security Test should validate that the assigned roles configured in the system provide appropriate access.
- **Equipment / Device Testing** – To ensure the equipment and devices operate in accordance with manufacturer specifications and any applicable DMV requirements. This includes the equipment to be deployed at the DMV business locations as well as equipment used by VALID at its factories to process the DMV licenses.
- **Performance (load, volume and stress)** – To confirm that the DL/ID system solution meets the performance standards and test the software design scalability of the various components of the solution. This testing will be preceded by a Performance Test Plan, and will test the scalability of the solution via load testing. This will occur in incremental stages, with the results of the testing in each incremental stage documented.
- **Data Conversion and Migration (DCM) Testing** – To occur during each event of data conversion and migration, and for the final data conversion and migration upload prior to Production. VALID will perform an initial load of a sample of folio data, including images and meta data, provided by the DMV and will analyze the data load to confirm accuracy of the data conversion.
- **User Acceptance Testing (UAT)** – UAT focuses on the critical testing of the DMV workflow and processes, security controls, and enterprise data integration requirements. UAT will be led by the DMV and VALID will participate in the tests as requested. VALID will generate a User Acceptance Test Plan and Acceptance Test Specification (Test Cases / Test procedures) after system requirements are finalized and will occur well in advance of the actual UAT. Further, VALID will provide the User Acceptance Test Plan to the DMV for review and approval well prior to Acceptance Testing.

The UAT will include, but not be limited to, all necessary criteria and tests which will be performed to ensure that the solution as a whole, and all components thereof, satisfy the requirements agreed to, provisions for the documentation of testing results, problem detection, and corrective measures taken to permanently address problems, and a description of the resources, including the DMV and VALID staffing, necessary to conduct testing.

The DMV will have the sole discretion to determine the final UAT test plan, including all details contained therein, that will ultimately be used in the determination of whether the solution, and all components thereof, satisfy the project requirements.

During this phase VALID will develop a Functional Test Plan, a Sytem Integration Test (SIT) Plan, a Security Test Plan, Equipment Test Plan, a Performance Test Plan, a DCM Test plan, UAT Plan, and will provide Regression Test Planning – all testing wiill include test scenarios with use cases, and test scripts. Generally, the customer performs the UAT, but it does so with test scenarios and test scripts prepared by VALID. In addition, VALID will work with the DMV's technical staff, explaining the purpose and process associated with the various test stages.

Training – Whenever VALID trains its customer regarding its solution(s), the training generally includes some combination of role-based training: supervisor training (or train-the-trainers), end user training, and technical or support staff training. Formal training will require an extensive set of training materials, handouts and guides, as well as a variety of training methods and evaluation techniques. It might include training materials in an electronic format or Web-based Training (WBT), if the DMV so prefers. VALID will work with the DMV to fully understand its training needs and preferences for types of training. Armed with that information, VALID will craft together plans and will develop the training materials in accordance with DMV's preference. Later, at a time convenience to the DMV, VALID will perform a walkthrough of its training materials. During that walkthrough, VALID will garner from the DMV its thoughts on revising and improving the training materials, as well as ensure that we have comprehensively addressed all the training material needs. A sample Knowledge Transfer and Training Plan can be found in this proposal in **Attachment 10.**

Our two keys to successful training are: first, to decompose the groups to be trained into common functions (e.g., admin staff, technical staff, and business office end-users, etc.), and to tailor the training to each group; second, to ensure that the training occurs just in time (JIT) for them to start using the new system. Generally, for the end users, VALID has learned it is best to install the system, train the users, and observe/remedial train, as needed – all in close time proximity. This approach can quickly result in a proficient end-user. Thus, VALID will gain agreement with the DMV as to the sequence of events for training, installation and cutover.

Phase 6 – Project Implementation

- During the Implementation phase, the focus is on transitioning from the current system to the new solution. This will entail transition planning, practice cutomver, system rollout, installation of the equipment at the DMV's field offices, and follow-up training. It will include system stabilization and optimization. The project rollout will be divided into several stages, including external services (check interfaces such as with law enforcement), back office cutover, piloting of front office(s), and then full state deployment**,** project completion, prior to moving to formal operations and maintenance (O&M).

The following sections describe how VALID moves through project transition activities.

Equipment Installation – Equipment for the field offices (usually consisting of an image capture workstation (PC) with application software, scanner, signature panel, printer and camera, etc.) will be pre-staged, inspected, tested, and inventoried and be delivered to each field office and installed on a set schedule. Immediately after (i.e., the next morning after the installation), the delivery team will return to the installed site for assistance, observation and remedial training, as needed.

Cutover to Production Planning – Cutover from the current system to the new production system is a short-term event; but planning for cutover usually takes several weeks. Cutover can occur with an entire system, or a portion of a system (e.g., for a pilot in a staged approach). Thus, we will define with the DMV the cutover strategy, confirm all responsibilities for the cutover to production, validate the outcomes, validate the data for uploading, provide an array of specified resources, and verify that all components to be cutover are ready.

The rollout itself consists of several stages, including external services (e.g., checking interfaces with such entities as VT Law Enforcement and the Department of Homeland Security), back office cutover, piloting of the front offices, and then full state deployment, and project completion.

Generally, VALID recommends a Pilot that can test of the data flow and the outcomes, as well as validate all the components to be cutover. Lessons learned during the Pilot will be aptly applied to the statewide deployment.

Post-Production Activities – These activities have as their primary objective: to stabilize / optimize the system solution.

- The Stabilization / Optimization Period is an established time interval in which all Level 1 (high importance) and Level 2 (medium importance) defects are corrected; and Level 3 (low importance) defects are remedied to the extent possible. The time period for stabilization lasts from 30 to 90 days, depending on the DMV needs.
- Transition to Card Production Services is a period during which VALID activates its operational support strategy and the DMV takes over operation of its side of the system. VALID will use this period to ensure knowledge transfer has occured with the DMV's team.

At the end of this phase that we will close the project and transition to an ongoing service, producing the identification cards / licenses for the DMV. In addition to the standard end-of-phase activities, such as Lessons Learned, VALID will provide a summary of all phases for an end-of-project review.

Although it could occur after the project has been closed, we plan for a Post-Implementation Evaluation Review (PIER) via a survey to be conducted at DMV site(s) to ensure comprehensive feedback regarding the end user's evaluation of the new processes and their proficiency in using the new system.

Phase 7 – Maintenance and Ongoing Delivery & Support

During this phase, VALID will provide outstanding service and support, will begin planning for DMV technology refreshments, and will continue to improve its solution to optimize DMV staff satisfaction. Ongoing maintenance and support are covered in detail in the Implementation Plan.

2. Provide a list of the standard project management deliverables that you would normally produce for this type of engagement.

Standard Project Management Deliverables

Throughout the project schedule (see Attachment 4) VALID has identified needed project management deliverables, which include the following:

- Project Kickoff Event
- Weekly Progress Reports
- Communications Management Plan
- Deliverables by Phase Document
- Risk Register
- Site Survey Plan
- Implementation Plan
- Post Implementation & Evaluation Report (PIER)
- Change Management Plan
- Solution Design Document
- Monthly Progress Reports
- Staffing Resource Plan updates
- Issue Log
- Site Survey Summary Report
- Quality Management Plan
- Deployment Assessment Report

VALID anticipates collaborating with Vermont DMV to adjust the above 'standard' set of deliverables to meet the needs of Vermont DMV. Additionally, VALID will work with the DMV to provide any additional PM deliverables needed by the Vermont DMV.

3. Provide a proposed list of project phases, tasks, and an implementation timeline. Label this Attachment #4.

The Project Schedule, with project phases, tasks and an implementation timeline is located in **Attachment #4.**

4. What types of difficulties have other clients experienced with implementation of the proposed solution?

We have noticed some concerns / difficulties experienced at other jurisdictions. The following are samples from multiple clients.

1. **Resource constraints caused by multiple cross-projects**. It is often intuitively appealing for a jurisdiction which is trying to improve its credentialing production to add other desirable projects to occur in concert with that effort. Such things as installing

a new queuing system, adding a new card type, changing the state's Endorsements and Restrictions policies, or fixing the internal legacy system. While well-meant and highly desirable in the long-term, these "side projects" can be highly distracting as they consume the time and attention of the same groups of staff and their leadership who not only have to focus on the new DL/ID System project, but deal with day-to-day issues. Further, the end users are being faced with learning multiple new processes and systems, rather than just one set of changes.

2. **Underestimating the effort needed to prepare stakeholders for the new system.** Because it is natural to resist change, even subconsciously, successful jurisdictions have become change masters, focusing on the organization change management (OCM) needs of their stakeholders, especially their own staff. Those who do not give full attention to the reality of a new card design, a new system and new processes tend to have a longer learning curves among their staffs and some confusion and annoyance exhibited by their external stakeholders.

3. **Underestimating the training needs of their staffs.** Some jurisdictions believe that changing DL issuance from one vendor to another is a relatively straightforward affair, since their agencies have done it a few times before. However, when also changing processes, due to the impact of Real ID (e.g., photo first), the concern is not so much the new equipment or even the new system, but the sense of total change that can be highly challenging. This could lead to a lack of confidence among some of the end-users, and that can translate over to the State's customers. There are several ways to combat this:

   a. Extensive preparation with periodic meetings leading up to the office conversion, enabling multiple opportunities for the staffs to ask questions. This can be supplemented with some online training regarding the new solution.

   b. "Borrowing" some key users from nearby DMV locations to work in QA / Testing of the new solution, at SIT and UAT, and then returning to the DMV locations to cross-pollinate their knowledge.

   c. Enabling some users to become "super users"; whereby a Vendor trains selected staff early and the participate in the transition activities, enabling them to help guide their colleagues at the newly installed locations,

   d. The training staff to remain at newly installed DMV locations for an extra day or two to guide, coach and remedially train those users who may need assistance.

e. Forming a DMV user advisor team which meets regularly to discuss the changes and how best to plan for and implement them

5. **Describe the experience and qualifications of the Project Manager you would offer as the resource for this engagement. Provide a copy of their and label it Attachment #5.**

The PM's experience and qualifications are located in **Attachment #5**. The PM's resume is located in **Attachment #7**.

Part 6: Technical Services

1. **Describe the technical services included in your proposal (e.g., business analysis, configuration, testing, implementation, etc.).**

For this initiative, VALID will leverage the following teams within its organization:

Business Analysts (Solutions Analysts) – During the appropriate phases of the project, VALID will leverage our solutions analysts. We use the term Solutions Analyst as this position is responsible for both the gathering of the project's detailed requirements, as well as working with the development and the configuration teams to ensure the requirements are met, in accordance with the design of the overall solution.

The Solutions Analysts will work with the project management team to ensure requirements for the solution are captured, expanded and documented. They will be working closely with the DMV team to identify the following items as a minimum:

1) Workflows – how the DMV wishes to have their operators conduct enrollments, view and access enrolled applicant's data, and monitor the lifecycle of the credential issuance.
2) Gates and Statuses – help the DMV define the various gates needed for their credential issuance, and the statuses for the applicant's credential requests as it flows through the gates and issuance process.
3) Reports – will work with the various DMV teams to identify their reporting needs. Needs will include types of data, format, frequency and delivery of the reports required.
4) Operator, Staff and Administrative roles – the Solutions Analyst will work with the DMV to help define the various access and permissions needed by each different role needing access to either WebLink ID or BioLink ID.
5) Integrations – The solutions analyst will work with the project team to collect and document any points of integration with existing DMV systems that are part of the solution. Detailing these connections will potentially require working with IT and 3rd party systems managers, as such, a firm technical understanding is required above and beyond the standard business analyst role.

Quality Management Team – VALID maintains a professional quality management team consisting of quality assurance and quality control staff that plans and oversees all its validation testing, which is formal, structured, and documented. VALID develops and maintains test data repositories, in accordance to the requirements of the DMV. We use comprehensive test plans with detailed test scenarios and test scripts. We will conduct quality reviews and testing progress discussions with the DMV. We will submit all test plans and testing results to the DMV, and invite the DMV to participate in our testing, if it wishes. We will provide the DMV with weekly reports which will reflect the progress of our testing. In the case of User Acceptance Testing, we will support DMV's testing. We will also provide the DMV with a services connection portal that will track the posted progress of all testing efforts.

VALID will provide formal validation testing for all supported environments. Our process will ensure that each testable element will meet the specified requirements. Our process includes identifying, tracking, and resolution of all issues. We will maintain test data repositories, as agreed upon. We will conduct periodic quality and progress reviews with appropriate DMV personnel; and we will track progress in weekly reports. We will maintain a record of solution component approvals by the DMV, and verify all applicable completion criteria.

Key activities will be performed during each stage of testing to enable successful progression to the next test stage. Each of the test stages details the activity, activity description, the responsible party, the tools and templates and the project outputs. VALID plans to provide the following test stages:

- Equipment Testing
- Functional Testing
- System Integration Testing, including all interfaces (end-to-end)
- Performance Testing (stress and capacity)
- Disaster Recovery Testing
- User Acceptance Testing
- Regression Testing

For each of the above test type, VALID's Quality Management Team will create the following:

Test Scenarios and Test Scripts – Initial drafts of the test scenarios and test scripts are created by VALID during the design stage; and they can be further refined by DMV and VALID as the design sessions continue, as well as during Build and Configuration. As applicable, test sets are a set of tests that are grouped for a specific test cycle. These may include all of the tests within a test stage (if applicable) or a subset depending on the scope of the test cycle. Test scenarios and test scripts and any test sets will be captured and maintained by VALID within the test management tool. In connection with performance testing and regression testing, the test scripts will be created within the specific toolset for that activity. DMV may supplement or modify any of the foregoing test materials as may be necessary to adequately test Vermont's DL/ID system solution.

Test Environments – A test environment sufficient to support the testing requirements will be created during the Build and Configure and testing activities. Test environment requirements include accommodating the applications, interfaces and extensions, as well as the supporting transactional data.

Test Data – VALID will provide the initial set of test data based on scrambled or de-identified data provided by DMV. DMV's SMEs can supplement the test data as needed, and would be responsible for validating the data prior to test execution. The test data plan will specify how data will be

generated (*e.g.*, new synthetic data or normalized production-quality data), updated, refreshed, and controlled. All testing documentation will be provided to DMV.

System Design and Development Team – VALID has a clear objective regarding software design and development: it aims to satisfy clients with early and continuous delivery of stable software that meets requirements and expectations. VALID's development team uses Agile methodology for all development projects, and that includes WebLink ID development, interfaces, and customizations. While VALID's solution in producing IDs/DLs is primarily configuration-based, interfaces always need development and VALID always strives to improve its software; and so when system design and development are needed, VALID can call on a highly proficient team of developers using Agile as their methodology.

Agile offers an adaptive project life cycle which is iterative and incremental, with rapid iterations (usually 2 weeks in length), and are fixed in time and resources. Agile is highly regarded and increasingly adopted from small firms to the world's largest technology companies. An Agile development environment requires total organization buy-in, and can entail a shift in the organization culture, and not simply a process change instituted by the development team. The key features of Agile include: its short-termed delivery cycles (sprints), the validated requirements, dynamic team culture, less restrictive project control, and emphasis on real-time communication. VALID's Agile environment is illustrated in the graphic below.

In order to achieve goals and planned results within a defined schedule and a budget, we have found Agile to be an optimal development methodology. As the name implies, an Agile approach provides a nimble process which enables faster turnaround and the dynamic ability to quickly adapt to needed changes or course corrections. The Agile approach tends to take a more people-centric perspective, implementing short, iterative phases called Sprints that rely on ongoing feedback that continuously reshape and refine the project path.

Agile project management focuses on adaptability to changing situations and constant, regular feedback – whether it is from our clients or from our other team members. An Agile approach is usually ideal for smaller software projects and/or those with accelerated development schedules. Agile development provides opportunities to assess the direction throughout the development lifecycle. This is achieved through regular cadences of work (Sprints) at the end of which our teams must present an incremental solution. Agile methodology becomes "iterative" and "incremental" as it focuses on the repetition of abbreviated work cycles as well as the functional solutions they yield. In an Agile paradigm, every aspect of development — requirements, design, etc. — is continually revisited and re-evaluated. In Agile development, iterations are cycles by which teams plan, collaborate and deliver business functionalities, products, etc.

The adjacent illustration graphically depicts the iteration cycle in Agile project management.

This "inspect-and-adapt" approach to development reduces development costs and time-to-market. Because a team's work cycle (sprint) is limited to two weeks, stakeholders have recurring opportunities to calibrate releases for success in the real world. Agile development helps VALID build the right solution to optimize value throughout development. Agile development approaches are founded on the process of human collaboration. The project is seen as a series of relatively small tasks conceived and executed to conclusion as the situation demands in an adaptive manner, rather than as a completely pre-planned process. Our development teams claim that this technique:

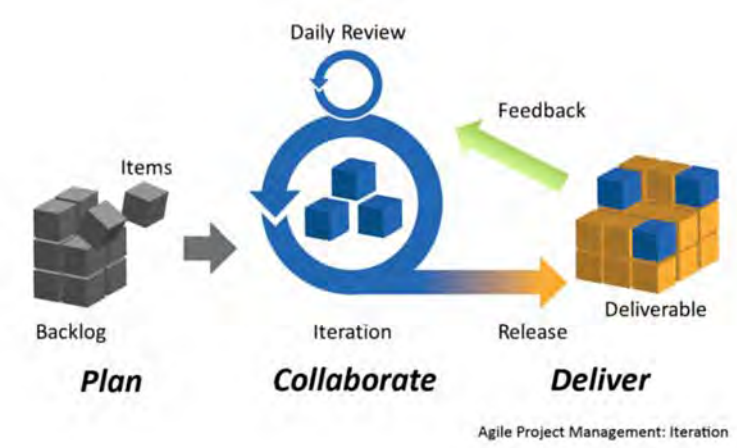


Figure 63: Iteration Cycle in Agile Project

- Is a consistent project management technique since it involves frequent testing of the project under development
- Enables active client involvement in the development process

Card Design and Delivery – VALID's Card Design and Delivery team offers over fifty (50) years of experience and highly-skilled resources to design and manufacture a secure, durable card that is fully compliant, and that exceeds AAMVA's most current requirements. Our credentials experts will use industry best practices and card engineering resources to design and produce cards that fully meet DMV's expectations. The VALID Card Design and Delivery team has placed over twenty (20) of its designs into production throughout various US jurisdictions.

Developing the new card design is often the most time consuming part of the delivery project. Reaching consensus on visual elements and validating the end product will be a collaborative effort among the DMV stakeholders. Therefore, card design activities begin soon after contract award and comprise stepwise reviews and approvals of individual card components based on an overall design concept that will be developed and approved by the DMV.

VALID's Card Design and Delivery Team will accomplish the following:

1) Its graphics designer will develop a documented card specification with at least three card design concepts for DMV review. Incorporating the DMV's feedback with each iteration, the process will continue until a consensus has been reached. The focus is on completing initial horizontal and vertical formats, and identifying spacing and locations for various messages and indicators.

2) The design concept selected by the DMV will be developed with "soft copy" proofs provided for all card types and formats. Prepress artwork will be completed for the DMV approval.

3) VALID will complete a First Article press run of core materials based on soft copy proofs approved in Step 2. All relevant card types and formats are included in their most commonly occurring forms. In other words, adult and minor driver licenses and adult and minor identification cards, if these use different artwork, would be provided as hard cards with simulated personalization, whereas less common forms (e.g., CDL) might be shown in soft copy form. Every card format will be included in either hard or soft form. A Card Design Specification containing representations (hard or soft) of all card types, descriptions of formatting, encoding and security features will be prepared, which will serve as a permanent record of the agreement between VALID and DMV. Factory software development and card rendering engines will not be created until this document has been approved by both parties.

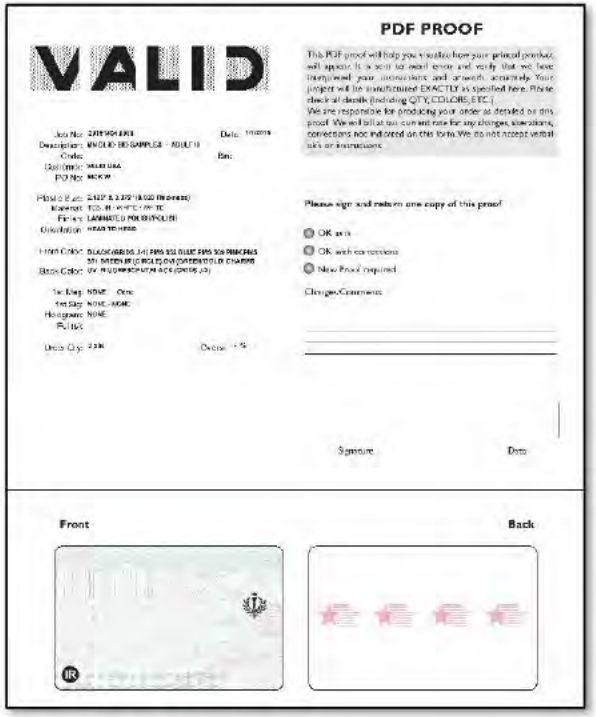


Figure 64: PDF Proof

4) Illustrator files, font callouts, and other needed artwork pieces (such as organ donor and veteran indicators) are sent to the developers as a template to write any custom code required for final card production. A standardized test job will be created that containing all possible combinations of logical data (portraits including representative genders and ethnicities, maximum length fields, combinations of endorsements and restrictions, multiple addresses, etc.). To the extent possible, the cards in this job will be self-documenting; e.g., a max length name field will contain the term "max length" in addition to the characters required to pad the length. The purpose of this job is not simply to test the software for errors, but to create a job that fully exercises every step of the factory workflow. The job will be retained so as to test equipment modifications and repairs as well as future software releases.

5) VALID will prepare multiple copies of a production card approval document containing hard cards that have been produced using final production software, equipment and materials. Copies will be provided to DMV and will be retained by VALID's Quality organization and Operations management for the Card Production Facilities. The cards included in the Production Card Approval Document are usually produced near the end of the user acceptance test (UAT), since it is not uncommon that changes are made during UAT that affect the finished card(s) design.

As described in the above-cited steps, VALID will work with the DMV to address all its requirements as detailed throughout the RFP, including meeting the AAMVA and ISO/IEC standards for image capture, sizing and placement.

If any new versions to the ISO/IEC or AAMVA standards emerge, then VALID will work with the DMV to update its DL/ID cards to the new standards. If requested by the DMV, VALID will add, delete, or modify card designs and/or formats once per calendar year at no additional cost to the DMV, pursuant to normal inventory management practices. All mandated format or design changes, including those mandated by federal or AAMVA standards, will be provided at no additional cost for the term of the contract, including extensions or renewals.

Staying ahead of card threats and potential fraud is an ongoing process and not a one-time activity. As the sophistication of fraudsters grows, so must card security. VALID will partner with DMV to assess card threats annually and on an ad-hoc basis as new threats emerge, and VALID will recommend potential options to mitigate those threats. The DMV may choose corrective action or determine that the threats do not warrant card changes.

Further, throughout the term of the contract VALID will evaluate revisions of the AAMVA DL/ID card design standard as they occur, advise DMV of their impacts, if any, and recommend potential options for incorporating any changes.

Data Analytics Team – VALID's organization includes a dedicated Data Analytics Team specialized in migrating, transforming, and managing data for clients looking only for those services. The VALID Data Analytics Team has experience managing data migration, cleansing and consolidation for commercial and government clients measuring in the hundreds of millions of records. The team has recently managed DL/ID data migrations involving approximately 50 million records and 20 million images.

During the appropriate phase of the project the DMV data will be migrated first to the QA environment, then to the production environment. Data need to be migrated into two different application databases, WebLink ID and BioLink ID. VALID will conduct an analysis of the data prior to the migration into QA environment. The analysis will highlight any possible concerns with the existing data, incomplete records, partial data sets, or records that are not complete enough to migrate. The purpose of this analysis is to enable the teams to adjust or correct the problematic data prior to migration.

Migration itself will occur on the QA and Production systems in a scheduled and organized fashion, with migration status reports available at any time during the process. Following the completion of the migration, the data will be available within WebLink ID for validation.

While the specifics of converting and migrating the DMV database may differ slightly, the VALID Data Analytics team will generally follow a six-step process for DCM, as follows:

Step 1 - Initial Card Image File (CIF) processing – This step is composed of testing and validation.

- Running SSIS (SQL Server Integration Services) Package to import CIF data
- Each job runs a month of a year; so 24 jobs in parallel running 24 months (2 years); this seems to maximize performance
- After jobs complete, another job runs to truncate log files

Step 2 - Initial historical card image processing – This is the full processing after testing and validation is completed. VALID runs stored procedures to import card images; and depending on the quality of the database, VALID can generally run an average of 100+ images per second.

Step 3 - Initial database processing – VALID will transfer the appropriate data, decrypting and re-encrypting as needed.

- Use SQL replication to keep our database in sync with DMV database.
- Transfer data as needed from the replicated database to staging tables.
- Decrypt and re-encrypt any data currently encrypted on DMV database.

Step 4 - Initial customer number processing. VALID will work with DMV to obtain a table of its records, so that it can cross-check the customer identifiers.

- DMV would supply a table for DEV and QA.
- VALID would store the Customer ID and /or other customer identifier.
- For non-matches, VALID would supply a list to DMV to create customer numbers.

Step 5 - Validate – VALID will validate with DMV sample CIF data, images and historical card images.

- Use a web-based viewer to display CIF data, images, and historical card images.
- Use the current vendor CIF viewer to open existing CIFs.
- Use VALID viewer to open imported CIFs and card images.
- Once the data is consumed by WebLink ID and BioLink ID, perform validation using those tools and the current vendors' applications.
- Provide extracts of any migrated records to DMV for comparison to original data sources.

- Validate imported data via a comparison of the DMV database and CIF data via the customer ID or other identifier.
- If overlapping data fields match identically for a given customer ID, then data integrity is considered verified.
- Compare CIF data to DMV database data to determine any discrepancies.
- For data that exists in both, DMV will determine which is the true source.

Step 6 – Synchronization – This step ensures that DMV data and the imported files on VALID are all in full alignment, and remain so going forward.

- Keep the DMV database in sync with SQL replication.
- Import CIF images via a scheduled SSIS job.
- Import historical card images via a stored procedure job.
- Update Customer ID via a service call to DMV database.
- State data for WebLink ID and BioLink ID consumption.

Configuration Team (DevOPS) – As this is a hosted web-based solution, VALID's primary configuration team is part of the VALID engineering group, named DevOPS, which is responsible for both the creation and management of the hosted environments as well as the deployment of the DMV specific configurations.

While the development team creates the specific content, the DevOPS team is responsible for ensuring the content created is installed and configured for utilization. Configurations include, but are not limited to the following:

1) Server and Virtual Machine resource allocation
2) Application and Data monitoring and backup
3) Client specific integrations with other services, databases, or enterprise solutions
4) Network connectivity, reliability and fault tolerance

The DevOPS team will work with the appropriate DMV IT staff and any 3rd party solutions staff necessary to ensure smooth connectivity to any required integration.

Field Services Team – VALID's Field Service technicians will be recruited from the Vermont area, and trained up well prior to training and deployment by our experience Field Services Management team. Later, post initial installation and user training, these technicians will be retained to provide maintenance services. Our Field Services technicians will be fully trained on and capable of diagnosing, replacing and servicing the deployed equipment, both hardware and software, as well as their operation. They will have detailed maintenance documentation at their fingertips.

VALID Field Services will maintain and distribute to the DMV all the technicians' contact information including their names, physical location, mobile telephone numbers, and email addresses. VALID will update the DMV monthly on the equipment inventory, by product/model, maintained to support the DMV's locations. All equipment required of VALID will be newly manufactured, and will be inspected to ensure excellent working order.

VALID Field Services will provide for the DMV a detailed description of all its equipment, and its parts; as well as how parts supply are requisitioned and inventory maintained. Some equipment may require depot maintenance for repair, and VALID will explain how that will occur, and with what vendors. VALID will maintain an adequate support of equipment and parts inventory so that there will be ample equipment to replace and malfunctioning equipment – to ensure availability to all the DMV locations. VALID Field Services will replace malfunctioning equipment with identical equipment, and malfunctioning parts with identical parts. VALID will ensure that it acquires enough equipment and parts to handle the anticipated needs of the DMV through the contract term, to ensure that equipment does not become obsolescent.

2. Provide a list of the standard deliverables for the technical services described above.

Throughout the project schedule VALID has identified technical deliverables, which can be segmented into QA / Testing, System Design and Development, Card Design, Data Conversion and Migration (DCM) and Disaster Recover / Business Continuity Planning.

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

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

- Security Test Plan
- Version Release Document

Data Conversion and Migration (DCM)

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

- Card Layout for DMV review
- Card Design Specifications
- Card Prototype Card Layout
- Card Core Approval Document
- Card Prototypes
- Production Card Approval Document (PCAD)

DR / BC Planning

- Disaster Recovery (DR) / Business Continuity (BC) Plan
- DR/BC Test Plan
- Test Result for DR/BC Testing

3. Provide a description of the roles/services/tasks the State will be expected to cover as part of this engagement. Describe any additional roles/services/tasks that are optional, but would be beneficial for the State toprovide.

VALID anticipates the State provide the following roles to facilitate implementation. These roles need not be different persons, depending on the DMV Staff's expertise and availability, but many of these roles will require significant effort and time:

1) **Project Manager** – A single project or program manager for the entirety of the project scope will provide continuity and enable a single person for contact and management of the various project tasks.

2) **Business Requirements** – capable of gathering and discussing business requirements from each prospective DMV team involved with this solution. This can be a single person but is usually more, due to the breadth of the DMV team's roles, and it is important to discuss each team's needs clearly and in enough detail the VALID's project team will need.

3) **Technical Leads** in each of the following areas will be needed to ensure success:
   a. *Existing Solution Administrator* – this person will be required to assist in coordination of migration activities for transition away from the existing DL/ID solution.
   b. *Existing System Administrators* – for each system needing access to, or providing data to the new DL/ID enrollment solution

c. Existing Infrastructure, Networking and Security Administrators– needed for planning, migration, installation and maintenance of the proposed solution.
d. *DMV internal development managers*– for any existing DMV systems wishing to consume or access the VALID solution via API
e. *DMV QA manager* – will work with the VALID QA manager and project team to create and maintain test plans, and assist in implementing SIT and UAT testing as well as ongoing QA needs
f. *Facility Managers* – for each location VALID will be deploying its enrollment hardware into.
g. *Technical Support Staff* – for implementation of the enrollment hardware on the existing DMV workstations

4) **Training Lead** – this role is helpful in providing information needed for building the training plan, specifically working with the VALID project team to identify what types of training is needed, who will be receiving the training, and scheduling with those staff when the training will occur.

5) **Support or Internal Help Desk Manager** – while VALID will support and manage solution related calls, it is important that the transition from the existing system to the VALID proposed solution include the existing internal support team lead, so there is a clear path for issues during the transition and beyond.

4. Describe your typical conversion plan to convert data from existing systems to your proposed solution (if applicable).

VALID will convert and enroll all existing customer image records, including legacy images and signature data, into our facial recognition (FR) system. Additionally, we will capture and enroll all new image records on an ongoing basis, and will meet the industry standards for formatting and compression. We will provide full documentation when this is accomplished; and we will precede it with a customized VT Data Conversion and Migration (DCM) Plan to be approved by the DMV.

Information, images, documents, and signatures needed to populate the previous application history for credential holders will be imported into the WebLink ID database. This will enable applicants to request renewals of existing credentials, and enables the staff to view previous applications without having to use the legacy application. Information needed for the inclusion in the BioLink ID application for facial recognition system population, which contains all previous photos and specific, agreed upon demographic information for each photo, will similarly be processed into the BioLink ID database.

VALID will conduct an analysis of the data prior to the migration into QA environment. The analysis will highlight any possible concerns with the existing data, incomplete records, partial data sets, or records that are not complete enough to migrate. The purpose of this analysis is to an adjustment or correction of the problematic data prior to migration.

The migration itself will occur on the QA and Production systems in a scheduled and organized fashion, with migration reports being available at any time. Following the completion of the migration, the data will be available within WebLink ID for validation.

At a high-level, there are three processes used for large-scale 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.

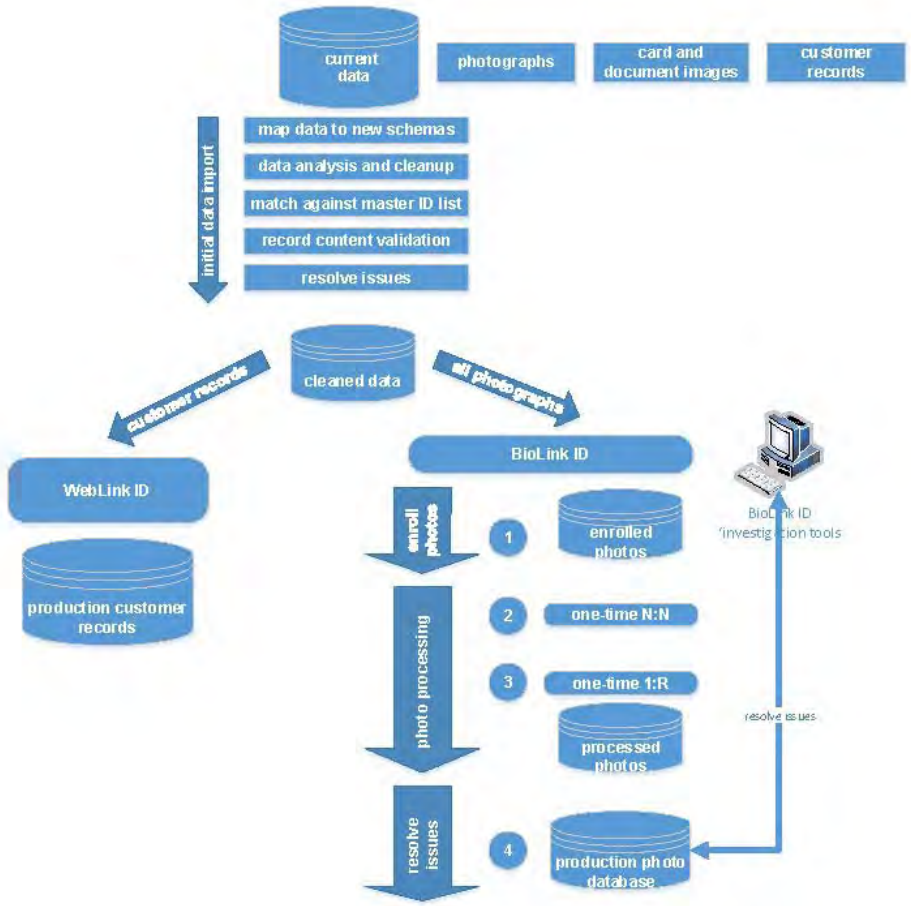


Figure 65: Overview of VALID's Data Migration Process

VALID will enroll all existing customer image records into our facial recognition (FR) system, BioLink ID, and our enrollment and management software, WebLink ID, well before production cutover. VALID uses its proven data conversion and migration (DCM) process outlined below. While the specifics of converting and migrating the DMV database may differ slightly, VALID generally follows a six-stage process for DCM, as follows:

1. **Initial Card Image File (CIF) processing** – This step is composed of testing and validation
   - Running SSIS (SQL Server Integration Services) Package to import CIF data.
   - Each job runs a month of data; and we have discovered that running 24 jobs in parallel is the most efficient way to import the CIF data.
   - After jobs complete, another job runs to truncate log files.
2. **Initial historical card image processing** – This is the full processing after testing and validation is completed. VALID runs stored procedures to import card images; and depending on the quality of the database, VALID can generally run an average of 100+ images per second.
3. **Initial database processing** – VALID will transfer the appropriate data, decrypting and re-encrypting as needed.
   - Use SQL replication to keep our database in sync with the DMV database.
   - Transfer data as needed from the replicated database to staging tables.
   - Decrypt and re-encrypt any data currently encrypted on the DMV database.
4. **Initial customer number processing**. VALID will work with the DMV to obtain a table of its records, so that it can cross-check the customer identifiers.
   - The DMV will supply a table for DEV and QA.
   - VALID will store the Customer ID and /or other customer identifier.
   - For non-matches, VALID will supply a list to the DMV to create customer numbers.
5. **Validation** – VALID will validate with DMV sample CIF data, images and historical card images.
   - Use a web-based viewer to display CIF data, images, and historical card images.
   - Use the current vendor CIF viewer to open existing CIFs.
   - Use VALID viewer to open imported CIFs and card images.

- Once the data is consumed by WebLink ID and BioLink ID, perform Validation using those tools and the current vendors' applications.
- Provide extracts of any migrated records to the DMV for comparison to original data sources.
- Validate imported data via a comparison of the DMV database and CIF data via the customer ID or other identifier.
- If overlapping data fields match identically for a given customer ID, then data integrity is considered verified.
- Compare CIF data to the DMV database data to determine any discrepancies.
- For data that exists in both, the DMV will determine which is the true source.

6. **Synchronization** – This step ensures that the DMV data and the imported files on VALID are all in full alignment, and remain so going forward.
   - Keep the DMV database in sync with SQL replication.
   - Import CIF images via a scheduled SSIS job.
   - Import historical card images via a stored procedure job.
   - Update customer ID via a service call to the DMV database.
   - State data for WebLink ID and BioLink ID consumption.

During the appropriate phase of the project, the DMV data will be migrated first to the QA environment, then to the production environment. Data need to be migrated into two different application databases, WebLink ID, and BioLink ID.

VALID's organization includes a dedicated team specialized in migrating, transforming, and managing data. VALID's solution offering for the DMV includes services of a VALID Data Migration team that has extensive experience managing data migration, cleansing and consolidation for commercial and government clients.

One of the challenges in migrating large amount of data and records from a legacy system is directly related to systems resources required and available. Our team will work with the DMV IT team to ensure the most efficient use of the resources available with least impact on ongoing operations. VALID will conduct an analysis of the data prior to the migration into QA environment. The analysis will highlight any concerns with the existing data, incomplete records, partial data sets, corrupt images, or records that are not complete enough to migrate. The purpose of this analysis is to enable the teams to adjust or correct the problematic data prior to migration. Additionally, VALID's BioLink ID solution can enhance some images that are not clear.

Migration itself will occur on the QA and production systems in a scheduled and organized fashion, with migration status reports available at any time during the process. Following the completion of the migration, the data will be available within WebLink ID for validation.

5. **Describe and attach your typical Implementation Plan (label it Attachment 6), which will include planning for the transition to maintenance and operations.**

Our Implementation Plan is in **Attachment #6.** It includes planning for (1) transition, (2) deployment, and (3) ongoing operations and maintenance.

6. **Describe the experience and qualifications of the technical resources proposed for this engagement. Provide their resumes and label them Attachment 7.**

The resumes of our technical resources proposed for this engagement are in **Attachment #7**.

7. **Describe the training that is included in your proposal.**

VALID's approach to successful training are as follows:

- Group individuals to be trained into common functions (e.g., operational staff, administrative staff, front-line staff, technical staff, etc.).
- Tailor the training to each group.
- Ensure that the training occurs just in time (JIT) for associates to start using the new system, but so much in advance that the training is forgotten.
- Evaluate the effectiveness of the training.
- Provide refresher training as needed to ensure that associates remain current with system features and functions.

VALID, in conjunction with the DMV project team staff, will develop the strategies to ensure effective and efficient training. VALID's experience at other customer sites, including templates and content, will be leveraged to maximize successful adoption of the new system. The training typically includes a combination of training methods and materials to meet all audience needs. All classes must contain scenario-based process flows, and clearly state the audience and purpose up front. Realistic mock-up data will be used whenever possible. Once all classes and materials have been created, VALID will provide a walk-through to ensure that audience needs are being met. The following is a list of the methods that may be used for training:

- Hands-on training (sandbox training)

- Instructor-led training (classroom training)
- Web-based training (demonstrations and interactive learning)
- Video instruction (including recorded video training and workflow sessions)
- Webinar training

VALID's Training Manager will design the various training modules. The VALID Project Manager will have responsibility for evaluating the training status, efficiency, and reporting that information to the DMV staff. It is expected that the DMV will assign a similar responsible party for evaluating and coordinating the training, as needed.

VALID understands that the training of DMV's staff must focus on the various roles that staff members have – what VALID refers to as role-based constituencies. By segmenting the types/levels of training, VALID can develop curricula and training materials tailored in accordance with the roles of each group. VALID focuses on five overall training levels, but we can alter this approach to accommodate less or additional groups. The five groups are:

- Operational (front-office) staff.
- Administrative (back-office) personnel (a varied and diverse group).
- IT/technical staff.
- Special Training groups such as UAT training and DMV Help Desk training.
- External partners – such as law enforcement and retailers.

Operational Training

The Operations side focuses on the end users in the branch locations who are customer-facing with the citizens of Vermont. VALID will focus on the functionality of the credentialing system, WebLink ID, and on the use of the installed equipment. VALID will provide user manuals, quick reference guides, web-based training, and other training documentation, after consulting with the DMV. For the instant issuance station at the DMV headquarters, VALID will provide operational, procedural and equipment training

DMV's responsibilities include having the operational staff available for training, and providing the venue for the training.

In all jurisdictions, a common theme of end-users is their lack of time for extensive training. What we have found works is a series of presentations to the end users explaining what is coming (e.g., using Webinars/conference calls for pre-training and Q&A), web-based training to support primary training, (which doubles as supplemental training for new hires and for remedial training support), and a focused training session during and immediately following installation of the new equipment. We generally use our installers to act as trainers for ½ day immediately following a DMV office install, both providing training of the end users and acting as on-site consultants the first day. Additionally, we have found it advisable to have a user from each branch office visit the Pilot offices soon after conversion and work with the Pilot office staff for 1-2 days.

DMV may want to consider the use of "super users"— key end users designated to learn the new system and train other DMV staff. Also, during formal training sessions, they can align with the VALID trainers in order to explain the differences between new capabilities and the existing legacy processes. Those jurisdictions that use super users have found them to be a significant help, as they can bridge the gap between the 'old system' and the 'new system'. For some states, the super users function as trainers on their own right, and in that role, VALID is prepared to provide them with instructor course materials to be used when they deliver end-user training for solutions.

Administrative Training

While the overview of the new DL/ID System will be the same for all the administrative groups, most of the content of the training will differ by user subgroup. Since the DMV administrative staff are so diverse and specialized, training modules will be created to address each functional area in separate training sessions, in accordance with a published schedule, agreed upon by the DMV and VALID, respectively. VALID will focus on its two products, BioLink ID and WebLink ID, and on the security processes, hands-on processing, reporting, and audit functions.

IT/Technical Training

Training topics will include the system architecture and connectivity, security processes, troubleshooting and monitoring, preventative maintenance, issue management, and an array of routine technology tasks. In addition, VALID will train the technical staff regarding the administrative functions of its two primary, integrated products – WebLink ID and BioLink ID. Some of VALID's technical training will occur via on-job training efforts in concert with VALID technical staff visits to Vermont, whereby the technical teams from VALID and DMV will work closely, and learn from each other.

VALID will support the technical team with a procedures manual which it will prepare for the designated DMV technical team, including a series of walkthroughs of the document to ensure its comprehensiveness and usefulness. This procedures manual will be updated throughout the life of the project, as needed.

Special Training Groups

This refers to special training for UAT or perhaps training for the DMV Help Desk. UAT participant training usually occurs a short time prior to UAT. VALID will prepare test the test scripts, but must train the UAT testers on how to navigate the new system as well as follow the test scripts and document the results. It is often helpful to have some super users participate in UAT to gain additional insights into the system solution.

Partners

Law Enforcement personnel have special needs, as they need to determine the legitimacy of a driver's license. Retailers need to know about any changes in credential design (to determine credential legitimacy) and the ability to rapidly determine age. For law enforcement, we recommend explaining the DMV Level 1 and Level 2 security features on the DL/ID credentials. VALID recommends brochures (separate designs for LEOs and retailers) which it would design and which the DMV can print and distribute. VALID will help the DMV with the design of other brochures or PowerPoints that the DMV can make available to law enforcement and retailers.

For additional information, please see **Attachment 10, Knowledge Transfer and Training Plan**

8. Describe the system, administrator, and/or user documentation that is included in your proposal.

VALID understands the importance of high-quality training materials to support DMV's staff during and after formal training. For all segments of the credential issuance process, VALID will develop a comprehensive set of training materials and leave-behind materials to include electronic (fully editable) and printed copy format of all training documents, including but not limited to, the following:

- Training plan and schedule
- Training curriculum and syllabus
- Training handouts.
- Online help materials
- User guides (PDF and Microsoft Word versions).
- Web-based training modules (demos, videos, etc.)
- Quick reference guides (including troubleshooting)
- Presentation materials
- Training evaluation surveys

- Special role-based materials for super users and others

VALID will develop and deliver comprehensive training materials, specifically designed and tailored to meet the business requirements of the DMV as configured in the central issuance solution, covering all important business and technical functions as determined by the DMV. VALID recommends a F2F walkthrough of all draft training materials with the DMV prior to their final revision. This includes user guides, maintenance manuals, training aids, brochures, and quick reference guides, etc. VALID will produce the final training materials at least 60 days prior to deployment and finalization of the training schedule. All training materials are provided in in electronic formats to accommodate future changes and for reproduction and distribution.

VALID will update and redistribute training materials at no additional cost to the DMV. VALID will correct, update, and redistribute at no additional cost to the DMV, any training materials on which a discrepancy is discovered. Further, if additional documentation is warranted due to a VALID change or a discrepancy in its other training materials, VALID will produce the additional documentation at no additional cost.

Part 7: Maintenance and Support Services

1. **Provide answers to the questions below regarding your company's Maintenance and Support Services:**

Q	Bidder Response
Service: Customer Phone &/or Email Support	
What is the method for contacting technical support?	VALID can receive Help Desk calls via web tracking, telephone, or email. VALID will provide a toll-free, support telephone line, an email address, as well as a web-based portal to the DMV to notify VALID of any issues. The VALID Help Desk will review the issue and respond to the appropriate DMV site within 15 minutes. If the Help Desk can resolve the issue, then the trouble ticket will be closed. If it cannot do so within 15 minutes, then the HD customer service representative (CSR) will dispatch a call to the nearest Field Services technician who will travel to the site to resolve the concern. If the call is regarding malfunctioning equipment, then the HD operator will request the following: • Location of the office (full physical address) • Contact point (name, phone and email) • A concise summary of the issue With the above information, the Help Desk dispatches one of our field support technicians to the site. The field support technician will resolve the issue by fixing or replacing the equipment within the stated SLA. Upon completion of the repair / replacement, the open ticket will be close. Per response to Question 13 from the RFP Q&: The DMV can choose to have its own DMV Help Desk call the VALID Help Desk, or it can have each individual DMV location call the VALID Help Desk. VALID can support <u>either</u> option, and there is no difference in cost. VALID would recommend that the Vermont Help Desk act as the first level support, logging in a trouble ticket and then calling the VALID Help Desk as the second level of support. We make this recommendation for two reasons: First, it has been our experience that the licensing offices do not always know what vendors to call for what services. They know they need help, and so often they call the first available phone number. If the offices call VALID to fix an issue that is not something we support, or they call another vendor that cannot support the equipment VALID has deployed, that often slows down the process of getting the right vendor out to remedy the concern. And the delays created could be significant. The DMV Help Desk would be better positioned to quickly ascertain the issue and who

	to contact to get an issue resolved, and open trouble ticket through resolution. Second, the primary function of the DMV front offices is to support their customers. They may not remember when they called, or immediately write it down, or recall the data and time when an issue was remedied. But if the VT Help Desk is managing the process for opening a ticket and getting resolution, then it will maintain a documentation on when it called the VALID Help Desk and when the call was closed. Having these statistics is very important to the DMV when evaluating reports from VALID and determining if SLAs for response times were met.
What are the hours of operation for support?	VALID will align its Help Desk and Field Support Team coverage with the DMV location schedules. VALID will provide during business hours whenever the DMV locations are open. Today, such support would cover 7:30 AM thru 4:30 PM eastern time, for Mondays, Tuesdays, Thursdays and Fridays. On Wednesday our Help Desk will remain open until 6 PM eastern time.
What is the turnaround time for responses?	The SLA for these calls has yet to be determined. VALID has suggested in its sample SLAs in **Attachment 8** the following: • Help Desk calls will be answered and responded to within a 15 min window • Dispatched calls where a field services technician needs to travel to a DMV location and make a repair or replacement should incur a 4-hour window.
What is the escalation process for support issues?	Generally, the Project Manager will be the first point of contact for escalation during the Vermont DL/ID System Project. At the completion of the implementation, as the project ends and the Operations and Maintenance (O&M) phase begins, the first point of contact will shift to the VALID Operations Manager.

The senior functional manager will diligently work to resolve all issues, while keeping the DMV's Project Manager fully informed. When a situation arises that requires escalation, the Project Manager/Operations Manager (First Point of Contact ("FPOC")) will escalate. The FPOC will coordinate the proper resources to respond to the situation and resolve the issue. If the situation warrants further intervention by Executive Management, then the FPOC will inform the Project Sponsor to garner his assistance. In normal, non-urgent cases, VALID recommends that the FPOC would have two business days to resolve the issue or provide a plan on resolution. In the event that the State provides formal notification by email or voice mail, the FPOC will respond to the State within four hours from the receipt of the request.

Figure 66: Routine Escalation Process

For urgent matters, the State can expect an immediate acknowledgement (within one hour) from the FPOC that the issue is being worked and a high level resolution plan will be presented within four hours. If at any point in this process, if the State wishes to escalate the process to the Executive Management, they are welcome to do.

If any of the primary individuals named in the escalation process – the FPOC, Project Sponsor, or Executive Sponsor – are unavailable, e.g., illness or vacation, for a period greater than two business days, an alternative with the same decision-making authority will be formally named. The FPOC will have this information available to him/her at all times throughout the CPS Project. If the FPOC is himself unavailable due to illness, vacation, or other reason, then a replacement will be identified for that period and this will be formally communicated to Vermont DMV.

Figure 67: Urgent Escalation Process

	VALID recognizes that there will be times when a critical technical or support issue must be resolved quickly. In those situations, we will have our Field Services Manager focused on the issue. He will have the authority to tap whatever resources he will need to resolve the matter. VALID will dedicate an appropriate number of technical resources to support Vermont DMV. These resources will be very knowledgeable about the Vermont system, and they will work with the VALID Field Services Manager and the Technical Lead to resolve any support or technical issue. If necessary, other VALID resources will be made immediately available. **Figure 68: Urgent Escalations** VALID will want the FPOC to be fully engaged in the issue resolution, but he/she would do so in conjunction with the Field Services Manager and Technical Lead and their respective staffs. As with other members of the escalation team, should the VALID Field Services Manager or Technical Lead go on vacation or become ill, their alternatives, with the same decision-making authority, will be named and that information provided to Vermont DMV. An escalation document with full contact information and alternative contacts and their information will be provided to Vermont DMV, after contract award.
Who comprises the support team and what are their qualifications?	The "support team" has two components: a Help Desk (HD) and a Field Support Team. The Help Desk is located at Ft. Wayne, Indiana; it documents all calls received from issue to resolution. The HD has 15 minutes or less to make a determination regarding how the issue might be resolved. In many case, such as malfunctioning equipment, it will need to dispatch a Field Services team member to the site to fix or replace the equipment. The Field Support Team resides in Vermont. Their disposition throughout the State is meant to facilitate the troubleshooting of issues as they occur throughout Vermont. The Field Support technicians are trained on all the equipment deployed to the DMV locations. In some cases, "repair" can be affected with a minor adjustment. However, in situations where the root cause of the issue is not obvious, it is usually better to just replace the

	equipment component and diagnose it later. In that way, we can maintain solution availability throughout the State. The Field Support team is composed of technical staff who are very familiar with the equipment in the DMV offices – Workstations, signature pads, scanners, printers, backdrop screens, and cameras. They are also familiar with the applications software – WebLink ID and BioLink ID – that resides on the hardware
Define your response resolution metrics and how you capture and report them.	VALID tracks all calls from the moment the call reaches our Help Desk until the technician resolves the issue. VALID uses a ShoreTel automated call distribution (ACD) system which will automatically track calls, provide call durations, etc. Additionally, the VALID HD Customer Service Representation (CSR) will log the open ticket into JIRA, VALID's issue management system, where the call will be recorded, tracked, and progresses through final resolution. VALID will report to DMV monthly all agreed-upon metrics as they relate to all calls to the Help Desk, response times, resolutions, etc.
Service: Incident/Security Breach Notification and Process	
Describe your identification and notification process for security breaches.	[redacted]

	[redacted]

	[redacted]
Service: Data Management	
Describe how data is stored, retained and backed-up (including frequency).	VALID will provide adequate storage for all existing legacy data as well as accounting for expected data growth throughout the life of the contract. VALID will assume certain growth percentages per year, based on the DMV's historical issuance volumes, and add that growth to the current data sizes required. VALID's proposed solution also scales the anticipated growth in transactional volume and application response times due to larger data sets. The proposed solution will account for acceptable response times not just at the beginning of the contract, but in the last year of the contract. Using the hosted solution's auto-scaling database, we can account for the growth of the environmental data. As we are proposing a geographically redundant, hot sync hosted solution, the need to bring the environment down for data backup or restore does not exist. Backups are conducted against a synced copy of the databases. VALID will define the backup schedule with the DMV. We propose a system backup at least weekly, with transactional backups occurring as the transactions themselves occur, not in a timed format, but real-time. These backups will be retained in accordance with the DMV's data retention policies, and archived upon completion of the retention cycle required by law.
Service: Hosting	
Describe the hosting service and associated service levels.	VALID's proposed solution is a cloud-based hosted solution. VALID has chosen Amazon Web Services as the hosting partner, as it provides solid, proven environment availability, security and redundancy. AWS similarly provides the most sophisticated sets of tools for managing and monitoring the environments, as well as administrative tools for reporting, intelligence, analytics and process management, while providing a lower operating cost and greater scalability.

Questions	Bidder
Service: Scheduled Maintenance/Downtime	
What is the frequency of scheduled maintenance and downtime?	VALID does not plan to utilize or require regularly scheduled maintenance. Maintenance for system updates, patches or bug fixes are not regularly scheduled and will be requested only as needed.
What is the notification process for scheduled maintenance and downtime?	VALID anticipates any scheduled downtime requests will be processed by the VALID Project or Account Manager and directed to the designated DMV contact or team who will authorize the request and its requested scheduled time. The actual process for maintenance and scheduled down time requests will be identified and formalized during the implementation project and bi-partisan certification of the defined process should be a requirement for project completion.
Describe how "maintenance" updates are tested with customers prior to installing them in their live environments.	***Patches/Fixes Management*** Internally, at VALID-hosted servers, patch management is monitored on a regular basis. Patches are tested on a dedicated machine for stability before they are deployed. VALID tests OS patches and updates monthly as part of its product maintenance. It tests updates in its internal Development Environment that replicates the configuration deployed to the cloud based environments. VALID develops software in a separate, internally-hosted environment. The software is then typically integrated and configured into the corresponding hosted environment, which may have several environments of its own: Development, Quality Assurance, and Production. All component/configuration changes are migrated through these environments through specific installation instructions and procedures – this is referred to a "step-up" strategy. This step-up strategy enables VALID and DMV to test technology stack (OS, web server, database server, etc.) updates and VALID's application software (runtime libraries, WebLink ID, BioLink ID, etc.) updates within the cloud based Dev or QA environment without affecting the Production environment.

	Sample Step-up Strategy to Testing Patches The software updates actually begin at VALID-hosted data centers within separate Development and QA environments. These environments are virtualized and will share a similar configuration to cloud-hosted Development environment. WebLink ID, BioLink ID, and Job Control System developers modify and build in the Development environment at VALID's Fort Wayne, IN Data Center. VALID then utilizes an Atlassian Bamboo continuous integration server to build the QA environment at VALID's Downers Grove, Illinois Data Center when a planned release is stable and ready for testing. Releases to the VALID-hosted QA environment will receive automated unit and functional tests during the continuous integration build. Additionally, VALID's QA team will use pre-defined test scenarios and cases to perform manual testing. These cases heavily target application areas that are not friendly to automated testing. After it passes the QA process, VALID's QA team will then promote the version or technology stack update. This promotion will be communicated to DMV staff who will schedule the installation for the update to the cloud-hosted Development environment. DMV and VALID QA teams perform additional testing in the cloud-hosted Development environment with a heavy focus on integration and functional test cases. The release or update is then promoted to the cloud-hosted QA environment after passing those tests. DMV and VALID QA teams perform more testing in the cloud-hosted QA environment. The QA environment is an exact replication of the Production environment. Here, the update receives heavy integration and performance test focus. Finally, with permission of DMV, a version or update is promoted to the Production environment after passing the testing process in all other environments. **Summary of the "step-up" QA strategy:** • VALID-hosted Development environment. • Promotion to VALID-hosted QA environment. • Promotion to cloud-hosted Development environment. • Promotion to cloud-hosted QA environment. • Promotion to cloud-hosted Production environment.

	VALID clears test data and accounts from the appropriate environments after testing, and VALID never intermingles test data and production data. VALID will provide to DMV a report with a quarterly or 'upon request' periodicity, which will cite any patches or software updates to the solution during the time period covered, as well as the type of patch/update (application, anti-virus, etc.) and the equipment affected. In keeping with its standard procedure, VALID will conduct testing, and then notify DMV of the test results and any pending updates/patches to the solution software prior to their execution. VALID will work with DMV to establish a procedure regarding the amount of notice needed and the appropriate contact points. VALID will never promote any solution software updates to Production without consent of DMV.

Service: System Upgrades	
Are software upgrades provided as part of the software support contract?	WebLink ID, BioLink ID, and the Job Control System are VALID products that have a lifecycle of updates, bug patches, and new features and functions within the products. Yes, VALID commits to supporting DMV with updates for all of its deployed applications throughout the life of the contract and potential extension years. Planned updates and application upgrades will come with additional documentation and training materials, as necessary, to support transition of new information. Most importantly, VALID is always working to provide the latest software technology, offering our clients' an obsolescence-proof solution. However, DMV can pick and choose which updates it wants, and the timing of those updates. ***Operating System, Web Server, and Database Server*** VALID aligns its product support with Microsoft updates for Windows Server, IIS, SQL Server, and internet browsers. Currently VALID supports Windows Server 2012 R2, Internet Explorer 11 (and latest versions of Chrome and Firefox), SQL Server 2014 and 2016, and IIS 8.x. VALID will support older versions of Microsoft products. VALID will add support for future versions of Microsoft products as part of its overall product strategy, and to support DMV Data Center updates to its infrastructure. ***Application Software*** Application Software products are updated as the implementation requires with special attention paid to avoid breaking changes. If a vendor releases a new version or update and that update may cause a loss of features or function, VALID will refrain from incorporating the updates until a time where the integration can be smooth, non-breaking, and provides added value. All updates are performed during scheduled

Describe your software upgrade process.	VALID will extend, at no cost for the update, for the duration of the contract, any system updates that are developed. Updates are specific to the version implemented, in this proposal WebLink ID 2.0. Should an update require changes to the DMV's customized business logic, gated issuance process, or other such customization, and is not within the scope of the initial project, VALID will discuss the impact of the updates with the DMV to identify any customization changes required. If, and when VALID has a version Upgrade for the DMV to assess, different from same-version updates, maintenance, change requests or hot-fixes, a new upgrade version server can be presented for the DMV to assess. This upgrade server will exist in the cloud, and will be accessible to the DMV staff reviewing the new features of the upgrade. In the event the DMV wishes to proceed with the upgrade, our project management team will engage the DMV staff to define and execute an upgrade project. As upgrades might impact the existing workflow design, business processes, system interconnectivity, and overall environment functionality, this process does require a proper project team to plan and execute. Similar to applying maintenance patches, updates and hot-fixes, VALID will deploy an upgrade version to a new Dev server in the cloud to verify the upgrade version passes all development tasks required. From the development environment it will pass to the QA environment for further testing. UAT might be needed to ensure operator acceptance. If it is, it will be defined during the upgrade project planning. Additionally, upgrades might require a new data migration, from the previous version to the new version, assessment of the migration need will occur during the upgrade project planning phase. Similar to the initial project, migration of existing data will occur such that it is available during testing in the dev and QA environments as needed or required. Once upgraded version testing is complete, a differential migration will occur to cover the data that has been modified or created since the initial migration into QA. Provided VALID is still under contract with the DMV, the upgrade version will have no licensing cost, and will be provided to the DMV at no additional price. The project to deliver the upgrade, any customizations, and implementation will be discussed with the DMV.

How often are new versions released?	[redacted]
Is documentation and training provided for system upgrades?	Yes. All system upgrades include documentation and training, as applicable.
Are there additional costs for upgrades and/or new releases?	[redacted]
Describe how and when the State will have an opportunity to test system upgrades/releases prior to live installation.	Similar to applying maintenance patches detailed above, the State can upgrade or new release deployed to their QA environment for testing and validation procedures. The same process defined above would apply. Internally, at VALID-hosted servers, update management is monitored on a regular basis. Updates and upgrades are tested on a dedicated machine for stability before they are deployed. VALID tests OS patches and updates monthly as part of its product maintenance. It tests updates in its internal Development Environment that replicates the configuration deployed to DMV's cloud-hosted solution. VALID develops software in a separate, internally-hosted environment. The software is then typically integrated and configured into the cloud-hosted environments, which may have several environments of its own: Development, Quality Assurance, and Production. All component/configuration changes are migrated through these environments through specific installation instructions and procedures – this is referred to a "step-up" strategy. This step-up strategy enables VALID and DMV to test technology stack (OS, web server, database server, etc.) updates and VALID's application software (runtime libraries, WebLink ID, BioLink ID, etc.) updates within the cloud hosted QA environment without affecting the Production environment. ***Sample Step-up Strategy to Updates and Upgrades***

	The software updates actually begin at VALID-hosted data centers within separate Development and QA environments. These environments are virtualized and will share a similar configuration to cloud hosted environments. WebLink ID, BioLink ID, and Job Control System developers modify and build in the Development environment at VALID's Fort Wayne, IN Data Center. VALID then utilizes an Atlassian Bamboo continuous integration server to build the QA environment at VALID's Downers Grove, Illinois Data Center when a planned release is stable and ready for testing. Updates and upgrades to the VALID-hosted QA environment will receive automated unit and functional tests during the continuous integration build. Additionally, VALID's QA team will use pre-defined test scenarios and cases to perform manual testing. These cases heavily target application areas that are not friendly to automated testing. After it passes the QA process, VALID's QA team will then promote the version or technology stack update. This promotion will be communicated to DMV staff who will confirm the schedule to the cloud hosted QA environment. DMV and VALID QA teams perform additional testing in the cloud-hosted QA environment with a heavy focus on integration and functional test cases. The release or update is then promoted to the cloud-hosted QA environment after passing those tests. The QA environment is an exact replication of the Production environment. Here, the update or upgrade receives heavy integration and performance test focus. Finally, with permission of DMV, a version or update is promoted to the Production environment after passing the testing process in all other environments.
Describe how the State will validate post installation and how changes will be backed out in the event that a problem is encountered.	VALID will work with the DMV to define post installation validation plans, ensuring the proper business logic, rules, messaging and data transports are functional post implementation and before production 'goes live'. Based on the validation plans, maintenance and validation might have to take place over a weekend, or a period of extended production down time to ensure proper promotion to production has been attained. In the event a rollback is required, VALID will work with the state staff to ensure it is achieved within a defined, and agreed upon rollback policy. Rollback of the implementation is relatively simple as VALID stored previous versions, and corresponding customizations, and can deploy those as needed. Data rollback can be accomplished, as VALID's solution stores previous app data, and those previous revisions can be set to current.

Question	Bidder
Service: Bug Fixes and Minor Enhancements	
Describe the frequency and process for providing, testing, and installing bug fixes and minor enhancements.	Similar to maintenance and updates, bug fixes follow the VALID "step-up" QA strategy defined earlier in this section. This "step-up" strategy will enable VALID and DMV to test technology stack (OS, web server, database server, etc.) updates and VALID's application software (runtime libraries, WebLink ID, BioLink ID, etc.) updates without affecting the Production environment. The process for providing and testing bug fixes actually begin at VALID-hosted data centers within separate Development and QA environments. These environments are virtualized and share a similar configuration to Cloud-hosted Development environment. WebLink ID, BioLink ID, and Job Control System developers modify and build in the Development environment at VALID's Fort Wayne, IN Data Center. VALID then uses an Atlassian Bamboo continuous integration server to build the QA environment at VALID's Downers Grove, IL Data Center when a planned release is stable and ready for testing. Releases to the VALID-hosted QA environment receive automated unit and functional tests during the continuous integration build. Additionally, VALID's QA team has pre-defined test scenarios and cases to perform manual testing. These cases heavily target application areas that are not friendly to automated testing. VALID's QA team then promotes the version or technology stack update after it passes the QA process. The promotion will be communicated to the DMV staff who schedule an installation for the update to the cloud-hosted Development environment. DMV and VALID QA teams perform additional testing in the cloud-hosted Development environment with a heavy focus on integration and functional test cases. The release or update is then promoted to the QA environment after passing those tests. The DMV and VALID teams perform more testing in the cloud-hosted QA environment. The QA environment is an exact replication of the Production environment. Here, the update receives heavy integration and performance test focus. Finally, a version or update is promoted to the Production environment after passing the testing process in all other environments **Summary of the "step-up" QA strategy:** • VALID-hosted Development environment. • Promotion to VALID-hosted QA environment. • Promotion to cloud-hosted QA environment.

	• Promotion to cloud-hosted Production environment. Bug Fixes might have a slightly smaller set of test plans to pass through each phase.
Service: Disaster Recovery	
Describe the disaster recovery services included in this proposal for any non-state hosted services.	At the onset of an emergency condition, VALID employees and resources will respond quickly to any condition which could impact VALID's ability to perform the critical functions. Our procedures have been designed to provide clear, concise, and essential directions to recover from varying degrees of interruption and disaster. VALID has fully-redundant facilities for all of its major business components and contracts. Due to the secure nature and requirements of our Payment, Commercial, and Identity customers, VALID has developed and maintains a fully-implemented and rigorously-tested disaster recovery and business continuity plan. Cognizant about concerns with disaster recovery, and the risks of potential downtime and delays in producing cards for mission-critical applications, VALID has implemented a unique solution for its customers who cannot readily absorb downtime or even the risk of downtime. At no additional charge, VALID offers a dual hot-site solution. VALID uses two geographically-separated personalization factories to produce IDs/DLs – each running well under 50% capacity, and each capable of receiving all of the ID/DL workload from one facility to the other – initiated within a moments' notice. This capability fully mitigates risks of major disasters and unforeseen events, but it also assuages concerns over malfunctioning printers and sorters needing repair, or waiting on parts. Further, disasters are not only about equipment and facilities, but they are also about re-staffing at the disaster site. With VALID's dual hot sites, both locations maintain a full complement of staff who know your application intimately, and who produce your ID/DLs daily.

	VALID will maintain complete duplication of data handling, card production, and card personalization facilities throughout the life of the contract between VALID and Vermont DMV. VALID easily has the capacity to support the full card production for the DMV, including growth, at either of its personalization factories. However, by providing two, fully-redundant personalization factories, VALID can provide the VT DMV with seamless, ongoing hot backups. That is why VALID splits the printing between two personalization factories – so that both printing crews are well-versed in producing the DMV's cards. Thus, VALID can meet the most stringent SLAs in producing DLs/IDs for the DMV, as it can move files from one personalization factory to another in minutes. The DMV disaster recovery scenarios will be simulated in collaboration with DMV to verify response systems and procedures function as required. All potential points-of-failure will be identified and will be mitigated. Disaster recovery scenarios are tested on an annual basis following the initial business continuity test prior to "Go Live" production. The annual test scenarios will be updated each year to best simulate the most current and plausible situations. Annual tests serve as a necessary training refresh on documented procedures. Evidence and results of the executed annual disaster recovery testing will be shared with the DMV. VALID anticipates a joint review of the results with the DMV to analyze and identify potential risks and opportunities for improvements. As the DMV and VALID contribute to successful operation of an overall system, procedural improvements may be applicable to VALID and the DMV alike. VALID's detailed Disaster Recovery and Business Continuity (DRBC) Plan will be made available to the DMV, on request, for complete review and approval.

	[redacted] With the use of two production operations active on a routine basis, actual transfer of operations to the unaffected production location is straight forward. Transfer of operations requires only that the allocation application be configured to send 100% of each incoming job to the other production facility. Since this situation utilizes data handling and production resources that are already in use, no additional testing is planned. These facilities follow the same level of security standards and are certified by credit card brands (Visa, MasterCard) in following Payment Card Industry (PCI) security standards. [redacted]

	[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

	[redacted]
What is your standard RPO and RTO?	[redacted]
Describe the plan your company has in place for its own disaster recovery of any sites that may be involved in support of this proposal.	VALID has set up its credential processing to fully mitigate the risks of unforeseen downtime or serious interruptions of its ability to produce credentials. Our factories are duplicated, as are our equipment and systems. Even our factory allocator, which sends card files received from the State to the factories, is backed up and duplicated in another geographic setting. Our power systems are backed up, and our telecommunications links among our factories are redundant. We produce the credentials in batches and track each batch. If a local disaster occurs during a batch run, we send the credentials in that batch to the other location, and we destroy the credentials already produced from the batch in the first location so that there can be no duplicated credentials. Our procedures are periodically tested. There is no loss of data, and our recovery time is generally under four hours. The following describes how VALID has planned for disasters at its personalization factories. In general terms, a disaster is defined as the total loss of a Card Personalization Facility for an extended period of time, as when a facility would be impacted by tornado or other natural disaster. In cases such as this, rebuilding the facility and/or installing new, unqualified equipment is typically required.

	Because VALID operates two production centers on a routine basis, actual transfer of operations to the unaffected production location is straightforward, the allocation application sends 100% of each incoming job to the unaffected production facility. • The next step is reconstruction. This may be as simple as restoration of services such as utilities or as complicated as rebuilding and reinstallation of new production equipment. The important distinction is that resuming production after a disaster may require the restoration of the production process using new personnel, equipment and/or facility. In which case: • Unit testing will be completed followed by end-to-end testing utilizing internally generated test jobs. The purpose of this testing is to simulate UAT and to verify that personnel and equipment are prepared for UAT. • An abbreviated UAT will be performed – similar to the UAT performed at initial contract acceptance, but limited in scope to this facility. • Upon acceptance, a new Production Card Approval Document will be created and upon approval, the facility will be deemed ready to receive jobs. Initial production will be overseen by engineering and top personnel.

2. Describe any other services not mentioned in the above list that are included in your standard Service Level Agreement (SLA) and include a copy of your SLA with your response to this RFP. Label the SLA Attachment #8.

VALID has no other specific services that have not been identified in this document. We have included a copy of standard SLA in Attachment #8.

3. Describe how adherence to your service levels is measured and what remedies you would provide the State when performance doesn't meet the standard?

VALID is cognizant that a service level agreement (SLA) helps to clarify the level of service expected by Vermont DMV by VALID, laying out the metrics by which each service is measured and the remedies or penalties that would occur if the agreed-upon service levels are not achieved. Upon contract award VALID expects to negotiate the SLA agreement with Vermont DMV to include a definition of the measurement standards, methods of measurement, reporting processes and frequency, and a dispute resolution process. We have enclosed in **Attachment 8** a suggested set of SLAs, how they are measured, and the remedies that we believe are appropriate should we fail to meet the suggested standards.

Part 8: Pricing

As instructed by the DMV, we are placing the financial pages for this proposal in a separate, sealed envelope; and have submitted that envelope with the proposal.

Part 9: Terms and Conditions

In deciding which Respondent/s to shortlist the State will take into consideration each Respondent's willingness to meet the State's terms and conditions. Indicate any objections or concerns to our stated terms and conditions in the RFP or any of the exhibits, addendums or attachments including **Attachment C** and **Attachment D**. Add lines to the table below as needed.

Important: Bidder will be bound to all terms and conditions stated in the State's RFP, exhibits, attachments, and/or addendums except and then only to the extent specifically set forth in the table below, and only if and to the extent expressly agreed and incorporated in writing in a resulting contract.

VALID can accept the standard terms and conditions, subject to contract negotiation period after selection, as stated in the RFP. VALID has no concerns regarding the State's RFP or its exhibits, addendums or attachments.

Clause Location	Concern	Proposed Verbiage
[indicate RFP, exhibit, attachment or addendum, section & page number]	[briefly describe your concern about this clause]	[describe your suggested alternative wording for the clause or your solution]

Part 10: Authorized Company Signature

I am authorized to submit a proposal to the State of Vermont in response to this RFP on behalf of my organization. The information provided as part of my organization's response is a true and accurate representation of my organization's ability to meet the State of Vermont's business needs as expressed in this RFP.

Signature:	
Full name:	Michael Fox
Title:	Vice President
Company:	Valid USA, Inc.
Date:	January 2, 2018

Attachments

Attachment #1 – Valid USA, Inc. Financial Statement

Attachment #2 – Valid USA, Inc. Road Map for Proposed Solution

Attachment #3 – PowerPoint Presentation providing Executive Summary of Proposal

Attachment #4 – Project Schedule

Attachment #5 – Project Manager Qualifications

Attachment #6 – Implementation Plan

Attachment #7 – Technical Resources Qualifications and Resumes

Attachment #8 – SLA with additional services

Attachment #9 – Card Feature Sheet

Attachment #10 – Knowledge Transfer and Training Plan

Attachment #1 – Valid USA, Inc. Financial Statement

Provide a Financial Statement* for your company and label it Attachment #1. A confidentiality statement may be included if this financial information is considered non-public information. This requirement can be filled by:

- A current Dun and Bradstreet Report that includes a financial analysis of the firm;
- An Annual Report if it contains (at a minimum) a Compiled Income Statement and Balance Sheet verified by a Certified Public Accounting firm; or
- Tax returns and financial statements including income statements and balance sheets for the most recent 3 years, and any available credit reports.

**Some types of procurements may require bidders to provide additional or specific financial information. Any such additional requirements will be clearly identified and explained within the RFP, and may include supplemental forms in addition to this Bidder Response Form.*

(see financial report on next 3 pages)

[redacted]

[redacted]

[redacted]

- Disclose any judgments, pending or expected litigation, or other real potential financial reversals, which might materially affect the viability or stability of your company or indicate below that no such condition is known to exist.

VALID does not have any outstanding or ongoing legal actions against it, in any state.

Attachment #2 – Valid USA, Inc. Road Map for Proposed Solution

Provide a Road Map that outlines the company' s short term and long term goals for the proposed solution/software and label it Attachment #2.

[redacted]

[redacted]

[redacted]

[redacted]

Attachment #3 – PowerPoint Presentation providing Executive Summary of Proposal

Provide a PowerPoint (minimum of 1 slide and maximum of 10 slides) that provides an Executive level summary of your proposal to the State. Label it Attachment #3

VALID IDENTITY SOLUTIONS

Prepared for State of Vermont Department of Motor Vehicle

VALID THE SECURE SIDE OF INNOVATION

VALID AT A GLANCE

READY FOR A FULLY **CONNECTED WORLD**

- Founded in 1957: **60 years** keeping up with an **ever-changing world**
- Listed company: **Bovespa since 2006**
- 2016 net revenues: **R$1.7 billion ($526USD)**
- **16 countries**: 6,000 employees
- **Global Top 10**: Identification of people, things and transactions
- **450 million microchips**: Deployed in 2017, smartcards and SIM cards
- **2+ million DL/ID cards:** deployed in state of WA and territory of Guam in 2017
- One size does not fit all: **Configurable solutions** and **long-term relationships**

COMPETENCY

CONVERGING MARKETS CREATE VALID PRODUCT SYNERGIES

VALID

DATA

PAYMENT

IDENTITY

MOBILE

- **Data:** aggregate, host, cleanse, deduplicate clients' data. Supplement w/ VALID data & services augmenting data accuracy and unlocking BI opportunities
- **Payment:** EMV/non-EMV cards, payment apps
- **Identity:** h/w & consumables, and s/w product suite to enroll, adjudicate identity, and manage credential lifecycle and PKI/security certificates
- **Mobile:** SIM, applets, eSIM, subscription management

U.S. IDENTITY SOLUTIONS

ID: Global Co. | Local Focus

- US HQ in Chicago area with ops in NJ, IN, MN, and CA
- Web-based software for identity & card management, biometric matching and investigation
- 200-employee and 600K sq. ft. space dedicated to card perso. & manufacturing
- ~25 dedicated US ID software and solution engineers and support staff resources
- Configurable product-based approach
- Trusted partner government and enterprise clients including WA DOL & Territory of Guam

ID Vertical Markets

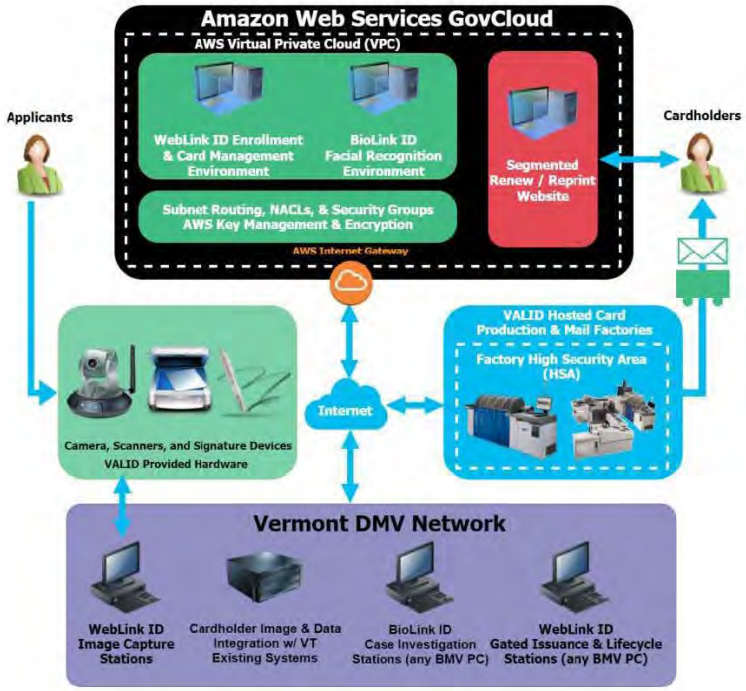
- State government identification: driver's license, state-wide employee ID applications
- Fed & state gov't benefits programs: WIC, EBT, SNAP
- Education: K12 & higher education
- Public transit: IL, AZ, CA

ID Trends

- Multi-technology apps/projects: ID card/identity mgmt. + payment + mobile ID + smart card (applets) + biometrics
- Bundled services: ID software & hardware solutions with integrated data BI
- Cloud-based services: Hosted SW solutions

Scalability Embedded: Cloud-Based Hosted

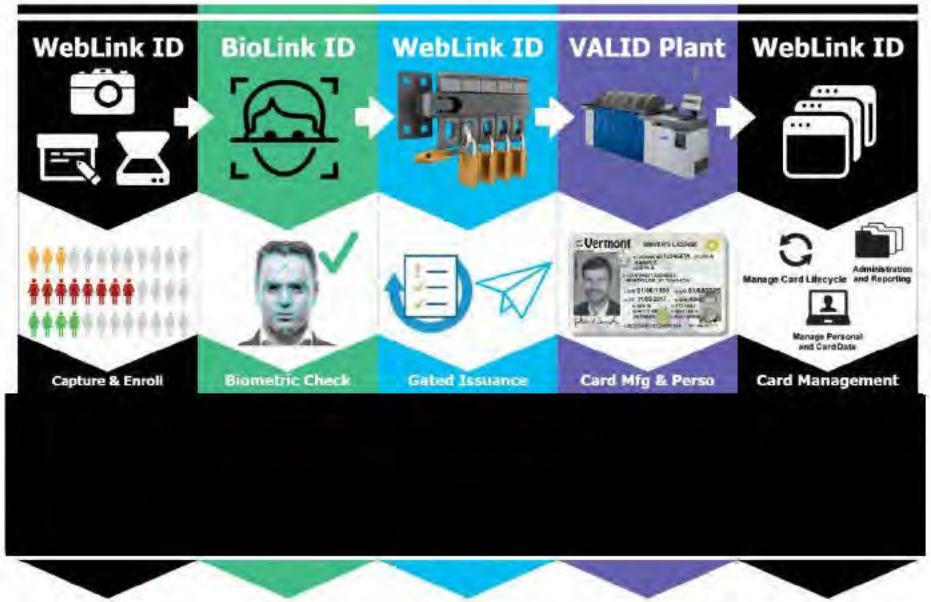
- Future Proof
- Auto scaling and fault tolerant
- Reliability in system availability & up-time
- Minimized IT capital investment & dedicated resources to support
- 365/24/7 Real time monitoring
- Compliance with the latest security measures & industry standards for life of the engagement



[redacted]

Integrated Suite of Products & Services

- Expandability: API-rich integration
- Flexibility: Micro services software architecture
- Visibility: Real-time status reporting for better insight
- Efficiency: Gated issuance to manage business processes
- Customization by Configuration: User configurable workflows

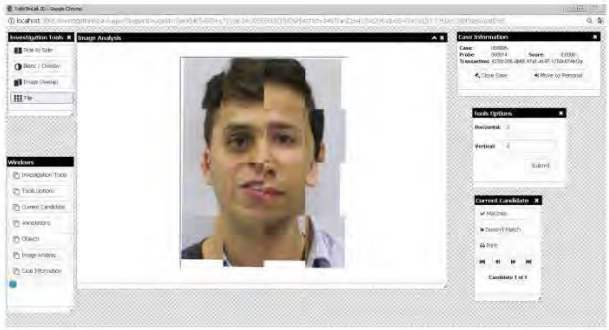


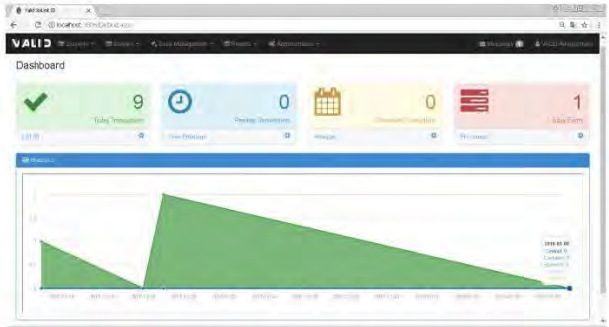
WebLink ID: Enrollment & Card Lifecycle

- Hosted or on-premise web app supporting latest browsers, card printers & hardware to capture photos, signatures, documents, and more
- Email photo request module (self upload)
- Card status & lifecycle management
- Optional gated issuance
- UI designer for cards, forms & workflows
- Tightly integrate w/ REST APIs

BioLink ID: Biometric Match & Investigation

- Web app investigation & case management
- Supports 1:1, 1:R, 1:N, & N:N matching: cluster controller w/ N match nodes
- Multi-modal architecture: face now w/ finger & iris coming soon
- FR algorithm agnostic: NEC, Toshiba, Cognitec & Innovatrics
- Integrates with WebLink ID and other 3rd party enrollment apps through robust REST & SOAP APIs





Card Services

[redacted]

[redacted]

[redacted]

www.valid.com

Thank you

MICHAEL FOX
Vice President, CCO

Michael.fox@valid.com
260-407-1177 Office
[redacted]

VALID THE SECURE SIDE OF INNOVATION

Attachment #4 – Project Schedule

Provide a proposed list of project phases, tasks, and an implementation time-line. Label this Attachment #4.

VT DMV Project Schedule_v1.0_TASK LIST

ID	Task Name	Duration	Start	Finish	Predece	Resource Names
1	**VT DMV CIS Project**	**320 days**	**Fri 5/11/18**	**Fri 8/2/19**		**DMV,Valid**
2	Vermont DMV awards Contract	1 day	Fri 5/11/18	Mon 5/14/18		DMV
3	Project Starts	1 day	Mon 5/14/18	Tue 5/15/18	2	Valid
4	**Project Initiation, Prioritization, Scheduling**	**13 days**	**Tue 5/15/18**	**Fri 6/1/18**		
5	Finalize the Project Schedule, and prepare the Communications Plan and Change Management Plan	2 days	Tue 5/15/18	Thu 5/17/18	3	Valid
6	Meet with DMV to collaborate on the project schedule, and other items in prepping for Project Kickoff	3 days	Thu 5/17/18	Tue 5/22/18	5	DMV,Valid
7	Create Deliverables by Phase document	4 days	Tue 5/22/18	Mon 5/28/18	6	Valid
8	Send to DMV for review	3 days	Mon 5/28/18	Thu 5/31/18	7	DMV
9	Prepare a draft Risk Register, Issue Log, Quality Management Plan, and procurement process document	4 days	Mon 5/28/18	Fri 6/1/18	7	Valid
10	**Project Management and Planning**	**292 days**	**Mon 5/21/18**	**Wed 7/3/19**		
11	**Project Management**	**292 days**	**Mon 5/21/18**	**Wed 7/3/19**		
12	**Monthly Project Status Report**	**281 days**	**Tue 6/5/18**	**Wed 7/3/19**		**Valid**
27	**DMV Review of Monthly Project Status Report**	**261 days**	**Tue 6/12/18**	**Wed 6/12/19**		**DMV**
41	**Weekly Project Progress Report**	**291 days**	**Mon 5/21/18**	**Tue 7/2/19**		**Valid**
101	**DMV Review of Weekly Project Progress Report**	**291 days**	**Tue 5/22/18**	**Wed 7/3/19**		**DMV**
161	**Project Plan Update**	**281 days**	**Fri 6/1/18**	**Mon 7/1/19**		**Valid**
219	**DMV Review of Project Plan Update**	**281 days**	**Mon 6/4/18**	**Tue 7/2/19**		**DMV**
277	**VALID Staffing Resource Plan Update**	**241 days**	**Tue 7/3/18**	**Wed 6/5/19**		**Valid**
290	**DMV Review of VALID's Staff Resource Plan Update**	**241 days**	**Thu 7/5/18**	**Fri 6/7/19**		**DMV**
303	**Risk Management Review**	**261 days**	**Thu 6/7/18**	**Fri 6/7/19**		**Valid,DMV**
357	**Project Governance Coordination Meetings**	**262 days**	**Tue 6/5/18**	**Thu 6/6/19**		**DMV,Valid**
371	**Project Kickoff**	**11 days**	**Wed 5/30/18**	**Thu 6/14/18**		
372	Prepare for Project Kickoff with Agenda and Materials	4 days	Wed 5/30/18	Tue 6/5/18		Valid,DMV
373	Project Kickoff Agenda and Materials Reviewed by DMV	4 days	Tue 6/5/18	Mon 6/11/18	9,372	DMV
374	Project Kickoff Event	2 days	Mon 6/11/18	Wed 6/13/18	372,37	DMV,Valid
375	Project Kickoff Event Reviewed by DMV	1 day	Wed 6/13/18	Thu 6/14/18	374	DMV
376	Project Kickoff Completed	0 days	Thu 6/14/18	Thu 6/14/18	374,37	DMV,Valid
377	**Requirements: Functional and Technical (Fit/Gap)**	**36 days**	**Thu 6/14/18**	**Fri 8/3/18**		
378	Refine the Project Plan	3 days	Thu 6/14/18	Tue 6/19/18	376	Valid,DMV
379	Establish Implementation Strategy	3 days	Thu 6/14/18	Tue 6/19/18	376	Valid,DMV
380	Assess Internal / External Project Dependencies	1 day	Tue 6/19/18	Wed 6/20/18	378	DMV,Valid
381	Establish Internal / External Project Risks	2 days	Tue 6/19/18	Thu 6/21/18	379	DMV,Valid
382	Finalize Communications Management Plan	3 days	Tue 6/19/18	Fri 6/22/18	379	DMV,Valid
383	Finalize Change Management Plan	1 day	Fri 6/22/18	Mon 6/25/18	382	DMV,Valid
384	Finalize Quality Management Plan	1 day	Mon 6/25/18	Tue 6/26/18	383	DMV,Valid
385	Finalize Risk Register and Issue Log	1 day	Mon 6/25/18	Tue 6/26/18	383	DMV,Valid
386	Develop Deliverables by Phase Document	2 days	Tue 6/26/18	Thu 6/28/18	385	DMV,Valid
387	Identify New/Enchanced Business Processes	2 days	Thu 6/28/18	Mon 7/2/18	383,38	Valid,DMV
388	Prep for Fit/Gap Sessions	3 days	Mon 7/2/18	Thu 7/5/18	387	DMV,Valid
389	Conduct Fit/Gap Assessment, including new and enhanced business processes, and review of data elements	13 days	Thu 7/5/18	Tue 7/24/18	388	DMV,Valid
390	Document Requirements	2 days	Tue 7/24/18	Thu 7/26/18	389	Valid,DMV
391	Create Updated Fit/Gap Document	3 days	Thu 7/26/18	Tue 7/31/18	390	Valid
392	BMV to review Updated Fit/Gap Document	3 days	Tue 7/31/18	Fri 8/3/18	391	DMV
393	Produce Initial draft of the Requirements Traceability Matrix (RTM)	3 days	Thu 7/26/18	Tue 7/31/18	390	Valid
394	BMV to review Initial Draft of RTM	3 days	Tue 7/31/18	Fri 8/3/18	393	DMV
395	Fit / GAP Complete	0 days	Fri 8/3/18	Fri 8/3/18	393,39	DMV,Valid
396	**Design**	**151 days**	**Thu 6/14/18**	**Fri 1/11/19**		
397	**System Design**	**37 days**	**Fri 8/3/18**	**Tue 9/25/18**		
398	**Iterative System Design Reviews**	**37 days**	**Fri 8/3/18**	**Tue 9/25/18**		
399	**Create Function Design Documents**	**12 days**	**Fri 8/3/18**	**Tue 8/21/18**		
400	Create SDD for Data Layout Design	2 days	Fri 8/3/18	Tue 8/7/18	395	Valid
401	Review and Approve SDD for Data Layout Design	2 days	Tue 8/7/18	Thu 8/9/18	400	DMV
402	Create SDD for Interfaces Design	3 days	Tue 8/7/18	Fri 8/10/18	400	Valid
403	Review and Approve SDD for Interfaces	2 days	Fri 8/10/18	Tue 8/14/18	402	DMV
404	Create SDD for Extensions Design	3 days	Fri 8/10/18	Wed 8/15/18	402	Valid
405	Review and Approve SDD for Extensions Design	2 days	Wed 8/15/18	Fri 8/17/18	404	DMV
406	Review Current Reports	2 days	Wed 8/15/18	Fri 8/17/18	404	DMV
407	Design Additional Reports	2 days	Wed 8/15/18	Fri 8/17/18	404	Valid
408	Review the additional Reports	2 days	Fri 8/17/18	Tue 8/21/18	407	DMV
409	**Create Technical Design Documents**	**14 days**	**Fri 8/17/18**	**Thu 9/6/18**		
410	Create SDD for Data Layout Design	2 days	Fri 8/17/18	Tue 8/21/18	405	Valid

Proprietary for internal use by VT DMV, do not distribute without written consent by VALID **Page XXX**

VT DMV Project Schedule_v1.0_TASK LIST

ID	Task Name	Duration	Start	Finish	Predece	Resource Names
411	Review and Approve SDD for Data Layout Design	2 days	Tue 8/21/18	Thu 8/23/18	410	DMV
412	Create SDD for Interfaces Design	3 days	Tue 8/21/18	Fri 8/24/18	410	Valid
413	Review and Approve SDD for Interfaces	2 days	Fri 8/24/18	Tue 8/28/18	412	DMV
414	Create SDD for Extensions Design	3 days	Fri 8/24/18	Wed 8/29/18	412	Valid
415	Review and Approve SDD for Extensions Design	2 days	Wed 8/29/18	Fri 8/31/18	414	DMV
416	Review Current Reports	2 days	Fri 8/31/18	Tue 9/4/18	415	DMV
417	Design Additional Reports	2 days	Fri 8/31/18	Tue 9/4/18	415	Valid
418	Review the additional Reports	2 days	Tue 9/4/18	Thu 9/6/18	417	DMV
419	**Performance, DCM and Solution Planning**	**25 days**	**Tue 8/21/18**	**Tue 9/25/18**		
420	Establish Performance Requirements	1 day	Wed 8/29/18	Thu 8/30/18	414	Valid
421	Create Process Flows with Key Inputs and Outputs	3 days	Thu 8/30/18	Tue 9/4/18	420	Valid
422	DMV to review Process Flows	2 days	Tue 9/4/18	Thu 9/6/18	421	DMV
423	Create Interface Control Documents	3 days	Tue 9/4/18	Fri 9/7/18	421	Valid
424	DMV to review Interface Control Docs	2 days	Fri 9/7/18	Tue 9/11/18	423	DMV
425	Create Data Conversion / Migration (DCM) Plan	4 days	Tue 8/21/18	Mon 8/27/18	410	Valid
426	DMV to review DCM Plan	2 days	Mon 8/27/18	Wed 8/29/18	425	DMV
427	Create Solution System Architecture Documents	5 days	Tue 9/11/18	Tue 9/18/18	424	Valid
428	DMV to review Solution System Architecture Documents	2 days	Tue 9/18/18	Thu 9/20/18	427	DMV
429	Update Enterprise Architecture Documents	2 days	Tue 9/18/18	Thu 9/20/18	427	Valid
430	Create System Sizing Requirements	3 days	Tue 9/18/18	Fri 9/21/18	427	Valid
431	Establish Test Environment Plan	3 days	Thu 9/20/18	Tue 9/25/18	429	Valid
432	Establish SDLC Environments	4 days	Tue 9/18/18	Mon 9/24/18	427	Valid
433	System Design Completed	0 days	Tue 9/25/18	Tue 9/25/18	431	DMV,Valid
434	**Card Design**	**162.13 days**	**Thu 6/14/18**	**Mon 1/28/19**		
435	**Card Design Specs and Prototype Layout**	**48.13 days**	**Thu 6/14/18**	**Tue 8/21/18**		
436	VALID's graphic designer will create basic card layouts for DMV review	8 days	Thu 6/14/18	Tue 6/26/18	376	Valid
437	DMV Reviews Card Layouts	5 days	Tue 6/26/18	Tue 7/3/18	436	DMV
438	Card Designer to discuss expectations with DMV and prepare concepts document	10 days	Tue 6/26/18	Tue 7/10/18	436	DMV,Valid
439	Review concepts document and iterate over changes.	4 days	Tue 7/3/18	Mon 7/9/18	437	DMV,Valid
440	DMV approves basic card layouts	5 days	Mon 7/9/18	Mon 7/16/18	439	DMV
441	Create Card Design Specification	5 days	Mon 7/9/18	Mon 7/16/18	439	Valid
442	DMV Approves Card Design Specification (CDS)	5 days	Mon 7/9/18	Mon 7/16/18	439	DMV
443	VALID provides prepress artwork and "soft copy" proofs	4 days	Mon 7/16/18	Fri 7/20/18	441	Valid
444	DMV Review and Approves prepress artwork and "soft copy" proofs	4 days	Fri 7/20/18	Tue 7/31/18	443	DMV
445	VALID provides Prototype Card Layout	5 days	Tue 7/31/18	Tue 8/7/18	444	Valid
446	DMV to review Prototype Card Layout	3 days	Tue 8/7/18	Fri 8/10/18	445	DMV
447	VALD provides Core Approval Document	4 days	Fri 8/10/18	Thu 8/16/18	446	Valid
448	DMV to review Core Approval Document	3 days	Thu 8/16/18	Tue 8/21/18	447	DMV
449	**Produce First Article of Card Blank**	**31 days**	**Tue 8/21/18**	**Wed 10/3/18**		
450	Pre-Press (inc. prepare PDF Proofs)	10 days	Tue 8/21/18	Tue 9/4/18	448	Valid
451	Obtain PDF Proof approval	2 days	Tue 9/4/18	Thu 9/6/18	450	Valid
452	Print Fronts	2 days	Tue 9/4/18	Thu 9/6/18	450	Valid
453	Print Backs	2 days	Tue 9/4/18	Thu 9/6/18	450	Valid
454	Collate	1 day	Thu 9/6/18	Fri 9/7/18	453	Valid
455	Laminate	1 day	Fri 9/7/18	Mon 9/10/18	454	Valid
456	Punch	1 day	Mon 9/10/18	Tue 9/11/18	455	Valid
457	Verification	2 days	Tue 9/11/18	Thu 9/13/18	456	Valid
458	VALID produces Card Blank Approval Document (CBAD) and FA Samples	4 days	Thu 9/13/18	Wed 9/19/18	457	Valid
459	DMV approves CBAD and FA Samples	10 days	Wed 9/19/18	Wed 10/3/18	458	DMV
460	**Card Prototypes**	**20 days**	**Wed 10/3/18**	**Wed 10/31/18**		
461	Review design results	5 days	Wed 10/3/18	Wed 10/10/18	459	DMV
462	VALID produces Card Protypes	10 days	Wed 10/10/18	Wed 10/24/18	461	Valid
463	DMV approves Card Prototypes	5 days	Wed 10/24/18	Wed 10/31/18	462	DMV
464	**Submission of Cards for AAMVA and Durability Testing**	**63 days**	**Wed 10/31/18**	**Mon 1/28/19**		
465	Provide sample set of cards for submission to AAMVA for testing	45 days	Wed 10/31/18	Wed 1/2/19	463	Valid
466	VALID provides a sample set of cards for submission for independent testing	30 days	Wed 10/31/18	Wed 12/12/18	463	Valid
467	Sample Cards are approved by AAMVA and DMV	2 days	Wed 1/2/19	Fri 1/4/19	465	DMV
468	VALID prepares multiple copies of a Production Card Approval Document (PCAD)	15 days	Fri 1/4/19	Fri 1/25/19	467	Valid
469	DMV reviews and approves	1 day	Fri 1/25/19	Mon 1/28/19	468	DMV
470	Card Design Phase Completed	0 days	Fri 1/25/19	Fri 1/25/19	468	DMV,Valid
471	**Development & Configuration**	**170 days**	**Thu 6/14/18**	**Thu 2/7/19**		
472	**Test Planning**	**7 days**	**Wed 8/15/18**	**Fri 8/24/18**		

Proprietary for internal use by VT DMV, do not distribute without written consent by VALID

VT DMV Project Schedule_v1.0_TASK LIST

ID	Task Name	Duration	Start	Finish	Predece	Resource Names
473	Develop/Compile Overall Test Plans	3 days	Wed 8/15/18	Mon 8/20/18	404	Valid
474	Develop Test Analysis Report	2 days	Mon 8/20/18	Wed 8/22/18	473	Valid
475	Establish QA Metrics	2 days	Wed 8/22/18	Fri 8/24/18	474	Valid
476	Refine Development Plan	2 days	Wed 8/22/18	Fri 8/24/18	474	Valid
477	**Develop Code / Solution**	**15 days**	**Tue 8/28/18**	**Tue 9/18/18**		
478	**Interfaces, Extensions & Reports**	**15 days**	**Tue 8/28/18**	**Tue 9/18/18**		
479	Develop Interfaces	8 days	Tue 8/28/18	Fri 9/7/18	413	Valid
480	Develop Extensions	8 days	Fri 8/31/18	Wed 9/12/18	415	Valid
481	Develop Reports	8 days	Thu 9/6/18	Tue 9/18/18	418	Valid
482	**Set QA Metrics and UATPlanning**	**19 days**	**Fri 8/24/18**	**Thu 9/20/18**		
483	Gather and Report QA Metrics	2 days	Tue 9/18/18	Thu 9/20/18	481	DMV,Valid
484	Develop UAT Plan with test scripts and test cases	7 days	Fri 8/24/18	Tue 9/4/18	476	DMV,Valid
485	DMV to review UAT Plan, Scripts and Cases	2 days	Tue 9/4/18	Thu 9/6/18	484	DMV
486	Develop Training Plan	10 days	Thu 8/23/18	Thu 9/6/18	411	DMV
487	**Data Conversion and Migration**	**50 days**	**Mon 8/27/18**	**Mon 11/5/18**		
488	Create Data Mapping Document for Legacy Systems	20 days	Mon 8/27/18	Mon 9/24/18	425	Valid
489	DMV to review Data Mapping Document	10 days	Mon 9/24/18	Mon 10/8/18	488	DMV
490	Perform Data Extraction	20 days	Mon 10/8/18	Mon 11/5/18	489	DMV
491	**Disaster Recovery and Business Continuity Testing**	**30 days**	**Thu 12/27/18**	**Thu 2/7/19**		
492	Valid to Provide Updated DR / BC Plan with DR Test Plan	5 days	Thu 12/27/18	Thu 1/3/19	516	Valid
493	DMV to review Updated DR / BC Plan & DR Test plans	10 days	Thu 1/3/19	Thu 1/17/19	492	DMV
494	Testing of Disaster Recovery Failover from one site to another	5 days	Thu 1/17/19	Thu 1/24/19	493	Valid
495	DMV to review Failover Testing	10 days	Thu 1/24/19	Thu 2/7/19	494	DMV
496	Remediate any issues determined in Failover Test	2 days	Thu 1/24/19	Mon 1/28/19	494	Valid
497	DMV to review any needed Remediation of Failover Tests	5 days	Mon 1/28/19	Mon 2/4/19	496	DMV
498	**Valid Procurement and Factory Preparation**	**150 days**	**Thu 6/14/18**	**Thu 1/10/19**		**Valid**
499	Create and update the BOM	5 days	Thu 6/14/18	Thu 6/21/18	376	Valid
500	Procurement & Install - Factory	5 days	Thu 6/21/18	Thu 6/28/18	499	Valid
501	Vendor Manufacturing	60 days	Thu 6/28/18	Thu 9/20/18	500	Valid
502	Perform SAT	2 days	Thu 9/20/18	Mon 9/24/18	501	Valid
503	Unit test equipment	15 days	Mon 9/24/18	Mon 10/15/18	502	Valid
504	Decommission, move to Katrine, reinstall	5 days	Mon 10/15/18	Mon 10/22/18	503	Valid
505	Install Oz and integrate to JCS	5 days	Mon 10/22/18	Mon 10/29/18	504	Valid
506	Unit test control software	5 days	Mon 10/29/18	Mon 11/5/18	505	Valid
507	Complete end-to-end testing inc. MXD/Mxi	10 days	Mon 11/5/18	Mon 11/19/18	506	Valid
508	Complete load testing	5 days	Mon 11/19/18	Mon 11/26/18	507	Valid
509	Prepare "Variations" job for testing	5 days	Mon 11/26/18	Mon 12/3/18	508	Valid
510	Produce "Variations" job	1 day	Mon 12/3/18	Tue 12/4/18	509	Valid
511	Installation at Montrose	5 days	Tue 12/4/18	Tue 12/11/18	510	Valid
512	Perform Montrose SAT	2 days	Tue 12/11/18	Thu 12/13/18	511	Valid
513	Unit test Montrose equipment	3 days	Thu 12/13/18	Tue 12/18/18	512	Valid
514	Install Oz and integrate to Montrose JCS	1 day	Tue 12/18/18	Wed 12/19/18	513	Valid
515	Unit test control software	5 days	Wed 12/19/18	Wed 12/26/18	514	Valid
516	Complete end-to-end testing inc. Montrose MXD/Mxi	1 day	Wed 12/26/18	Thu 12/27/18	515	Valid
517	Complete load testing	3 days	Thu 12/27/18	Tue 1/1/19	516	Valid
518	Produce "Variations" job	1 day	Tue 1/1/19	Wed 1/2/19	517	Valid
519	Test Factory Allocation data flow and handling	4 days	Wed 1/2/19	Tue 1/8/19	518	Valid
520	End to end test using DMV data	2 days	Tue 1/8/19	Thu 1/10/19	519	Valid
521	**Verification (Testing)**	**165 days**	**Tue 9/4/18**	**Tue 4/23/19**		
522	**Functional Test Stage**	**33 days**	**Tue 9/18/18**	**Fri 11/2/18**		
523	Establish Functional Test Plan with Expected Results	3 days	Tue 9/18/18	Fri 9/21/18	481	Valid
524	DMV to review Functional Test Expected Results	2 days	Fri 9/21/18	Tue 9/25/18	523	DMV
525	Create Equipment Test Plan	4 days	Tue 9/25/18	Mon 10/1/18	524	Valid
526	DMV to review Equipment Test Plan	4 days	Mon 10/1/18	Fri 10/5/18	525	DMV
527	Execute Functional Testing	10 days	Mon 10/1/18	Mon 10/15/18	525	Valid
528	Defects and Issues Log for Functional Testing	3 days	Mon 10/15/18	Thu 10/18/18	527	Valid
529	Execute Equipment Testing	2 days	Thu 10/18/18	Mon 10/22/18	528	Valid
530	Collect Performance Metrics	1 day	Thu 10/18/18	Fri 10/19/18	528	Valid
531	Produce Functional Testing and Equipment Testing Reports	5 days	Fri 10/19/18	Fri 10/26/18	530	DMV
532	DMV to review Testing Reports	5 days	Fri 10/26/18	Fri 11/2/18	531	DMV
533	**System and Integration Test Stage**	**55 days**	**Fri 11/2/18**	**Fri 1/18/19**		
534	Establish System Test Expected Results	3 days	Fri 11/2/18	Wed 11/7/18	532	Valid,DMV
535	Establish UAT Expected Results	3 days	Wed 11/7/18	Mon 11/12/18	534	DMV,Valid
536	Establish SIT Test Plan and Procedures	8 days	Mon 11/12/18	Thu 11/22/18	535	Valid
537	DMV to review SIT Test Plan	3 days	Thu 11/22/18	Tue 11/27/18	536	DMV
538	Perform SIT Test (Alpha Test)	15 days	Thu 11/22/18	Thu 12/13/18	536	Valid

Proprietary for internal use by VT DMV, do not distribute without written consent by VALID **Page XXX**

VT DMV Project Schedule_v1.0_TASK LIST

ID	Task Name	Duration	Start	Finish	Predece	Resource Names
539	Defects and Issues Log for SIT Test	3 days	Thu 12/13/18	Tue 12/18/18	538	Valid
540	DMVL to review Defects and Issues Log	3 days	Tue 12/18/18	Fri 12/21/18	539	DMV
541	Collect Performance Metrics	1 day	Tue 12/18/18	Wed 12/19/18	539	Valid
542	Produce System Test Report	3 days	Wed 12/19/18	Mon 12/24/18	541	Valid
543	Create System Technical Documentation	10 days	Mon 12/24/18	Mon 1/7/19	542	Valid
544	DMV to review System Technical Documenation	5 days	Mon 1/7/19	Mon 1/14/19	543	DMV
545	Publish Version Release Document	5 days	Mon 1/7/19	Mon 1/14/19	543	Valid
546	DMV to review Release Document	4 days	Mon 1/14/19	Fri 1/18/19	545	DMV
547	**Security Testing**	**30 days**	**Fri 1/18/19**	**Fri 3/1/19**		
548	Create Security Test Plan	10 days	Fri 1/18/19	Fri 2/1/19	546	Valid
549	DMV to Review Security Plan	10 days	Fri 2/1/19	Fri 2/15/19	548	DMV
550	Perform Security Testing	5 days	Fri 2/15/19	Fri 2/22/19	549	DMV,Valid
551	Provide result to DMV	5 days	Fri 2/22/19	Fri 3/1/19	550	Valid
552	**DCM Implementation**	**73 days**	**Fri 11/2/18**	**Wed 2/13/19**		
553	Prepare DCM Plan	10 days	Fri 11/2/18	Fri 11/16/18	532	
554	DMV to review the DCM Plan	6 days	Fri 11/16/18	Mon 11/26/18	553	
555	Prepare Data Extract Templates	2 days	Mon 11/26/18	Wed 11/28/18	532,554	Valid
556	DMV to review Data Extract Templates	3 days	Wed 11/28/18	Mon 12/3/18	555	DMV
557	Data Conversion Test Plan with Scripts	8 days	Mon 12/3/18	Thu 12/13/18	556	Valid
558	DMV to review Data Conversion Test Plan with Scripts	5 days	Thu 12/13/18	Thu 12/20/18	557	DMV
559	Data Extraction	15 days	Thu 12/20/18	Thu 1/10/19	558	DMV,Valid
560	Data Integrity Testing	5 days	Thu 1/10/19	Thu 1/17/19	559	DMV,Valid
561	BioLink enrolls CIF data	10 days	Thu 1/17/19	Thu 1/31/19	560	Valid
562	WebLink ID consume the CIF data from BioLink	5 days	Thu 1/31/19	Thu 2/7/19	561	Valid
563	Prepare for Data Refreshes	2 days	Thu 2/7/19	Mon 2/11/19	562	DMV,Valid
564	Data Refreshes	2 days	Mon 2/11/19	Wed 2/13/19	563	DMV,Valid
565	**Data Synchronization**	**49 days**	**Wed 2/13/19**	**Tue 4/23/19**		
566	Convert images to standard format	2 days	Wed 2/13/19	Fri 2/15/19	564	Valid
567	Complete conversion of all data and stage it in production	7 days	Fri 2/15/19	Tue 2/26/19	566	Valid
568	Enroll data into the facial recognition (FR) BioLink solution environment	10 days	Tue 2/26/19	Tue 3/12/19	567	DMV,Valid
569	Load all incremental folio data from current vendor into WebLink environment	6 days	Tue 3/12/19	Wed 3/20/19	568	Valid
570	Validation of existing production data extractions	3 days	Wed 3/20/19	Mon 3/25/19	569	DMV,Valid
571	Ongoing synchronization and testing for Compet CIFs and DMV db	21 days	Mon 3/25/19	Tue 4/23/19	570	Valid,DMV
572	Data Synchronization Complete	0 days	Tue 4/23/19	Tue 4/23/19	571	DMV,Valid
573	**Training Planning**	**97 days**	**Tue 9/4/18**	**Thu 1/17/19**		
574	Develop Training Scripts	5 days	Tue 9/4/18	Tue 9/11/18	484	Valid
575	Develop Training Plan	15 days	Tue 9/11/18	Tue 10/2/18	574	Valid
576	Create a Training Curriculum	5 days	Tue 10/2/18	Tue 10/9/18	575	Valid
577	DMV to review Curriculum Plan	10 days	Tue 10/9/18	Tue 10/23/18	576	DMV
578	Create End-User Training Materials	7 days	Tue 10/23/18	Thu 11/1/18	577	Valid
579	DMV to review End-User Training Materials	15 days	Thu 11/1/18	Thu 11/22/18	578	DMV
580	Create On-Line Help Materials	10 days	Thu 11/22/18	Thu 12/6/18	579	Valid
581	DMV to review On-Line Help Materials	10 days	Thu 12/6/18	Thu 12/20/18	580	DMV
582	Create Quick Reference Guides (QRG) / User Job Aids	10 days	Thu 12/20/18	Thu 1/3/19	581	Valid
583	DMV to review QRGs and User Job Aids	5 days	Thu 1/3/19	Thu 1/10/19	582	DMV
584	Produce a Training Schedule	5 days	Thu 1/3/19	Thu 1/10/19	582	Valid
585	DMV to review Training Schedule	5 days	Thu 1/10/19	Thu 1/17/19	584	DMV
586	**Site Surveys**	**80 days**	**Tue 9/25/18**	**Tue 1/15/19**		
587	Create Site Survey Plan	10 days	Tue 9/25/18	Tue 10/9/18	433	Valid
588	DMV approves the Site Survey Plan	5 days	Tue 10/9/18	Tue 10/16/18	587	DMV
589	Perform Site Surveys	45 days	Tue 10/16/18	Tue 12/18/18	588	Valid
590	Summary Report of Site Surveys	15 days	Tue 12/18/18	Tue 1/8/19	589	Valid
591	DMV approves the Site Survey Summary Report	5 days	Tue 1/8/19	Tue 1/15/19	590	DMV
592	**Performance Test Stage**	**30 days**	**Wed 12/19/18**	**Wed 1/30/19**		
593	Performance Test Plan	5 days	Wed 12/19/18	Wed 12/26/18	541	Valid
594	DMV to review Performance Test Plan	13 days	Wed 12/26/18	Mon 1/14/19	593	DMV
595	Execute Performance Testing	5 days	Mon 1/14/19	Mon 1/21/19	593,594	Valid
596	Remediate any issues or bugs	5 days	Mon 1/21/19	Mon 1/28/19	595	Valid
597	DMV to review Remediation	2 days	Mon 1/28/19	Wed 1/30/19	596	DMV
598	Completion of Performance Testing	0 days	Wed 1/30/19	Wed 1/30/19	597	Valid,DMV
599	**User Acceptance Test Stage**	**36 days**	**Fri 3/1/19**	**Mon 4/22/19**		
600	Prepare for UAT	7 days	Fri 3/1/19	Tue 3/12/19	551	
601	Perform User Acceptance Testing (Final System Acceptance)	10 days	Tue 3/12/19	Tue 3/26/19	600	DMV
602	List and Prioritize Defects and Issues	2 days	Tue 3/26/19	Thu 3/28/19	601	Valid

Proprietary for internal use by VT DMV, do not distribute without written consent by VALID

VT DMV Project Schedule_v1.0_TASK LIST

ID	Task Name	Duration	Start	Finish	Predece	Resource Names
603	DMV to review Defects and Issues Log for UAT	2 days	Thu 3/28/19	Mon 4/1/19	602	DMV
604	Create Remediation Plan for Outstanding Issues and Bugs	3 days	Thu 3/28/19	Tue 4/2/19	602	Valid,DMV
605	Execute Remediation Plan	5 days	Tue 4/2/19	Tue 4/9/19	604	Valid
606	Perform Regression Testing	5 days	Tue 4/9/19	Tue 4/16/19	605	Valid
607	DMV reviews Regression Testing Results	2 days	Tue 4/16/19	Thu 4/18/19	606	DMV
608	Update Operational Documents	2 days	Thu 4/18/19	Mon 4/22/19	607	Valid
609	User Acceptance Testing and Regression Testing Completed	0 days	Mon 4/22/19	Mon 4/22/19	608	Valid,DMV
610	**Transition and Deployment**	**63 days**	**Mon 4/1/19**	**Thu 6/27/19**		
611	**Transition**	**20 days**	**Mon 4/1/19**	**Mon 4/29/19**		
612	Finalize Implementation Plan to include Transition, Deployment and Maintenance	2 days	Mon 4/1/19	Wed 4/3/19	603	Valid
613	DMV to review Transition Plan & Release Checklists	2 days	Wed 4/3/19	Fri 4/5/19	612	DMV
614	Transition Operational Procedures	3 days	Fri 4/5/19	Wed 4/10/19	613	Valid
615	Publish Job Control Schedule	2 days	Wed 4/10/19	Fri 4/12/19	614	Valid
616	Establish SLA Parameters	2 days	Fri 4/12/19	Tue 4/16/19	615	Valid
617	Assemble Audit Impact Statement (integrity, security & privacy)	2 days	Fri 4/12/19	Tue 4/16/19	615	Valid
618	Execute an FR Scrub	7 days	Tue 4/16/19	Thu 4/25/19	606	
619	Execute Operations Training	5 days	Tue 4/16/19	Tue 4/23/19	617	Valid
620	Perform Release Verification	2 days	Tue 4/23/19	Thu 4/25/19	619	Valid
621	Update Enterprise Architecture and Data Model	2 days	Thu 4/25/19	Mon 4/29/19	620	Valid
622	Update Data Center Environments	2 days	Thu 4/25/19	Mon 4/29/19	620	DMV,Valid
623	**Deployment**	**43 days**	**Mon 4/29/19**	**Thu 6/27/19**		
624	Perform Practice Cutover	1 day	Mon 4/29/19	Tue 4/30/19	622	Valid
625	DMV to review Practice Cutover	1 day	Tue 4/30/19	Wed 5/1/19	624	DMV
626	**Initialization**	**1 day**	**Wed 5/1/19**	**Thu 5/2/19**		
627	All systems' components installed, tested, and verified	1 day	Wed 5/1/19	Thu 5/2/19	625,52(	Valid
628	**Rollout -- Stages 1 thru 4**	**40 days**	**Thu 5/2/19**	**Thu 6/27/19**		
629	Stage 1 - External Services (CIS data / photo service / EDS service)	2 days	Thu 5/2/19	Mon 5/6/19	627	Valid
630	Stabilization of External Services	2 days	Mon 5/6/19	Wed 5/8/19	629	Valid
631	Stage 2 - BackOffice Capture /Issuance	3 days	Wed 5/8/19	Mon 5/13/19	630	Valid
632	Stage 3 -- Cutover Front Office(s) for Pilot	10 days	Mon 5/13/19	Mon 5/27/19	631	Valid
633	Pilot Complete	0 days	Mon 5/27/19	Mon 5/27/19	632	DMV,Valid
634	DMV reviews Pilot -- Decision to go Statewide	1 day	Mon 5/27/19	Tue 5/28/19	632	Valid
635	Statewide Deployment Planned	2 days	Tue 5/28/19	Thu 5/30/19	634	DMV,Valid
636	**Stage 4 - Statewide Deployment**	**18 days**	**Thu 5/30/19**	**Tue 6/25/19**		**Valid**
637	Install and Train 2 sites	3 days	Thu 5/30/19	Tue 6/4/19	635	Valid
638	Install and Train 3 sites	5 days	Tue 6/4/19	Tue 6/11/19	637	Valid
639	Install and Train 3 sites	5 days	Tue 6/11/19	Tue 6/18/19	638	
640	Install and Train remaining sites	4 days	Tue 6/18/19	Mon 6/24/19	638,63!	Valid
641	Review Installations	1 day	Mon 6/24/19	Tue 6/25/19	640	
642	Complete Statewide Deployment	0 days	Tue 6/25/19	Tue 6/25/19	640,641	DMV,Valid
643	Final System Acceptance by DMV	2 days	Tue 6/25/19	Thu 6/27/19	641	DMV
644	**Post-Production Activities**	**28 days**	**Tue 6/25/19**	**Fri 8/2/19**		
645	Post-Implementation and Evaluation Report	15 days	Tue 6/25/19	Tue 7/16/19	641	Valid
646	DMV to review Cutover Assessment Report	10 days	Tue 7/16/19	Tue 7/30/19	645	DMV
647	**Project Close Activities**	**26 days**	**Thu 6/27/19**	**Fri 8/2/19**		
648	All project documents completed, organized and provided to DMV for Storage	8 days	Thu 6/27/19	Tue 7/9/19	643	Valid
649	All project activities closed	5 days	Tue 7/16/19	Tue 7/23/19	645	Valid
650	Plans completed for Transition to Maintenance and Ongoing Support	3 days	Tue 7/23/19	Fri 7/26/19	649	Valid
651	DMV to Certify Project Completion	5 days	Fri 7/26/19	Fri 8/2/19	650	DMV
652	Project Completion	0 days	Fri 8/2/19	Fri 8/2/19	651	DMV,Valid

Attachment #5 – Project Manager Qualifications

[redacted] is a global project management professional with 25 years of experience in applying PMO processes to SDLC. [redacted] began his career as an information engineer at the esteemed IT consultancy, James Martin & Co. At James Martin & Co., [redacted] assisted organizations using techniques pioneered by Dr. Martin, including Computer-Aided Software Engineering (CASE) tools, Rapid Application Design (RAD), and Joint Application Design (JAD). [redacted] has delivered dozens of successful projects for large organizations.

[redacted] has worked in two continents with cultural sensitivity and success leading onsite and remote matrix teams with leading processes and local execution. He brings broad experience in planning and executing multi-million-dollar high visibility and mission-critical application development and enterprise application delivery projects in the insurance, medical device, pharmaceutical, health care, utilities, education and general manufacturing industries. He has also worked for or alongside well-known software companies such as IBM, Oracle, Tivoli, Compuware, SAP, McKesson and SAS. [redacted] is detail-oriented, customer-focused and excels in applying his diverse skill set to developing sustainable solutions. He is experienced in project managing state government projects, including the DL/ID systems.

Project experience includes:

- Successful management of $10K-$4M dollar projects, leading up to 250 business and IT professionals.
- Developed high reputations and competence in directing projects of varying size and complexity, regardless of platform.
- Leading cross-functional teams to complete results-generating tasks and projects on time.

[redacted] resume is located in **Attachment** #7, per the response to Question 26 regarding the RFP.

Attachment #6 – Implementation Plan

Describe and attach your typical Implementation Plan (label it Attachment #6), which shall include planning for the transition to maintenance and operations.

Our typical Implementation Plan is actually three plans – a Transition Plan, a Deployment Plan and an Operations and Maintenance Plan – as that is what most government agencies request. However, whether three plans or one, these plans must be fully developed and ready to go prior to "Go Live". We have combined them in the plan below, as requested by the DMV.

VALID Implementation Plan

1. Introduction

For a successful project, we need effective planning of the transition, the deployment and the ongoing maintenance as soon as practical. Lack of effective planning and execution may lead to severe reconciliation problems and schedule attenuation. Such issues can be prevented if appropriate thought is given to plan this phase in a way that is least intrusive and in sync with the DMV's resources.

Implementation will start just before the Project goes live (transition) and will continue through deployment, (which includes installation and training), and through ongoing operations and maintenance activities. This planning represents a set of detailed, sequenced tasks and activities which are performed to deploy the pre-production components to the production environment and activate them; to onboard supported systems, data, interfaces, system components, documentation and related operational support; to outline the handling, delivery and installation roles from the Pilot to the statewide deployment; and to detail how VALID will ensure all maintenance activities will be performed, and how all VT requirements will be met with minimal disruption to the DMV locations.

2. Purpose

To plan the execution of activities required to successfully migrate the business operations from the current solution to the new DL/ID System Production system, install the equipment and train the users, and then maintain the systems.

3. Scope

This plan focuses on all requirements which must be met, and all tasks and activities to be performed to transition the Vermont DMV from its existing DL/ID environment to its new central issuance solution, as well as the management of processes to support that effort. It includes preparation for the Pilot, execution of the Pilot and the statewide deployment, and all ongoing support for that deployment.

4. Transition

4.1 Objectives

- Execute "Go-Live" cutover with minimum negative impact to daily business objectives.
- Coordinate with the DMV to connect service delivery between DMV and VALID's personalization factories.
- Coordinate with multiple sets of stakeholders to ensure a successful transition.
- Implement processes and controls that will not interfere with DMV's ongoing business operations.
- Ensure that the administrative and technical staff are trained and ready, and they have appropriate user documentation.
- Quickly reach a stability level where the project can be handed over to the respective Operations and Maintenance teams.
- Execute cutover within established timeframe, deploy the new solution statewide, and maintain the system throughout.

4.2 Assessment

VALID will assess the resource requirements (e.g., hardware, software, and staffing), time requirements, known impact or dependencies on other projects, and other information mutually agreed upon. VALID will inventory and describe the operations being migrated; and it will identify, track, and report all DMV operational software on supported servers. Finally, VALID will list the baseline performance attributes of the current legacy environment. As a result of these efforts, VALID can fully assess the current environment vis-a-vis the new DL/ID System environment, can identify gaps, and can assess what needs to occur to transition DMV from its current solution to a centralized issuance solution.

Additionally, this assessment will provide a baseline for performance levels of supported servers, processes (both online and batch), and other measurable elements of system performance for the current environment. Later, this will be used for comparison to the new DL/ID System environment to validate performance improvements. VALID will provide to the DMV proposed strategies and standards to coordinate information and solution architecture across DMV locations.

4.3 Prepare

During the Test phase, the QA teams will have developed test scenarios and test scripts etc., and will have executed all the necessary testing to make sure the system fully worked. However, it is intuitively appealing to insert a prepatory stage between testing and production cutover.

Most of the activities in preparing for cutover will be finalized over the weeks leading up to the actual cutover point. During this preparation period, data can be migrated and locked down in the live system, equipment is received and prepped, back-office training is completed, and the installation schedule is continually validated. By thoroughly preparing for the cutover, we can reduce the cutover workload and risks.

Once we get to the stage where we are ready to Go-Live, we enter a final but critical juncture where we review the likelihood of showstoppers and gauge our likelihood of success. First, we must ensure the training meets the needs of the users. The end users will be learning the system in a thorough way, and should be able to iron out small mishaps early on.

When we get to the actual cutover point, it is pivotal to have a detailed checklist, which must include everything that needs to happen, and it must be comprehensive and accurate. The project managers will act as the central control points, so activities must be reported back to them, and they will update the cutover plans. To sum up the above, the key to a successful cutover and deployment lies with detailed transition planning.

4.4 Implementation Sequence

1 – Deployment of External Services – These are the third-party interfaces that must be maintained – Law enforcement, Department of Homeland Security (DHS), etc. These connections must be tested again just prior to Cutover.

2 – Deployment of all Back Office units – Prior to the implementation of a single pilot, the administrative and technical support teams must be fully trained and prepared to support the issuance of driver licensees.

3 – Deployment of the Pilot sites – This is where we will first issue the new identification cards and driver licenses.

4 – Deployment of the operational locations (schedule to be determined)– during this implementation, our mutual goal will be to efficiently transition the remainder of the DMV's locations in accordance with the prescribed schedule.

4.5 Stabilize

Projects should never go live without a full understanding of how they will be measured, how success will be determined, and how to define the point-of-stability. The main project objective must always be to reach a stability level where the project can be handed over to operations and maintenance (O&M) teams. We must clearly validate the key performance indicators (KPIs) that need to be met to proclaim the system stable.

4.6 Key Performance Indicators with Success Criteria

- Complete all documentation: training documentation, user manuals and a technical procedures manual
  Success Criteria: Positive feedback from the DMV administrative staff, operational staff, and from the technical support staff

- Ensure that the administrative and operational teams receive transitional support to keep workflow and process disruptions to a minimum
  Success Criteria: Positive survey results

- Render the Pilot locations successful
  Success Criteria: No critical or high severity open issues

- Install the DMV sites (in accordance with installation schedule) – once rollout begins, or meet the schedule by adjusting the rollout quantity
  Success Criteria: No critical or high severity open issues

- Ensure each DMV location has equipment pre-positioned the night prior; and installed the morning of – for each specific location
  Success Criteria: Minimal intrusion in operations of DMV locations (no complaints); and all equipment installed and working to specs

- Ensure each operational and administrative location receives adequate training and support prior to, during, and after each cutover
  Success Criteria: Administrative and operational staff are able to support the new DL/ID System solution with minimal re-training

- Ensure that all items in the Show Stopper Report are addressed and solutions are approved by sponsors
  Success Criteria: No open show stopper entries are in the report

4.7 Transition Components

a. Card Design Complete	This includes card approvals by DHS and AAMVA, and a signed Production Card Approval Document
b. Testing Complete	Ensure that all testing–interface, system integration, performance, Disaster Recovery, and UAT/regression – are completed.
c. Card Factory Preparation	The card production equipment components are Tested. The factory allocator works flawlessly and VALID Internal Acceptance Testing was completed.
d. Production to Build	Activities to Build technical environment – infrastructure, configuration, security – are complete
e. Data Conversion & Migration	The historical data in existing system -- production (DCM) system, and card images – are all tested, consumed, and synchronized
f. Training & Documentation	Must be completed for all teams (e.g., admin, Operations, DMV Help Desk, etc.); as well as all Documentation (User Guides, QRGs, etc.) completed, approved and distributed.

g. Site readiness checklist activities	Those steps performed to ensure project success – equipment prep, site preparation, showstopper report submitted, practice cutover completed, and entrance criteria met.
h. Production Metrics	Activities to monitor/track performance across key baseline metric readings and target measures
i. Go/No Go	Process performed via periodic checkpoints to ensure completion of critical tasks

4.8 Transition Organization, Responsibilities and Approach

4.8.1 Transition Composition

Members will include the Readiness Rollout Manager, Project Managers, Technical/Architecture Lead, Developer Lead, QA Lead, and Training Lead.

4.8.2 Responsibilities

- Direct the overall planning and coordination of the Transition and related deliverables
- Secure resources needed to plan, execute, and evaluate the Practice Cutover and Cutover
- Manage and control the execution of all Practice Cutover and Cutover tasks
- Coordinate issue resolution using predefined processes and coordinating across other resources (administrative, technical and operational) to drive analysis and resolution
- Work with respective project sponsors to ensure critical issues and barriers are resolved in a timely manner using predefined communications and escalation processes
- Coordinate and oversee activities to ensure alignment with entrance and exit criteria
- Assess potential impacts to timeline based on any issues that arise
- Ensure timely resolution of assigned issues and provide a timely status update of all issues using agreed-upon processes during rollout
- Review and identify any possible changes required to the Transition tasks and dependencies

4.8.3 Transition Approach

- Define and prioritize the effort transition effort
- Define stakeholder goals and expectations

- Ensure consistent timelines, dependencies, entrance and exit criteria
- Refine high-level requirements
- Verify data conversion and migration (DCM) processes and procedures
- Validate reports and forms for operational use
- Conduct quality and progress reviews between VALID and DMV staff
- Complete all readiness steps and criteria in the Transition Readiness Assessment checklist
- The Rollout Readiness Manager and Project Managers will oversee the execution of every step in the Transition efforts.
- Provide tools and processes to synchronize master data (deltas) as necessary
- Conduct a practice cutover run (dress rehearsal) prior to 'Go Live' Cutover to validate the Transition assumptions. Test the backup and restore of the production environment during dress rehearsal

4.9 Transition Activities

4.9.1 Progress and Issues

- Log issues/bugs in JIRA (VALID's issue management solution)
- Review all issues in daily meetings

4.9.2 Transition Tasks

1	**Inventory and describe the operations being migrated**	VALID will work with DMV to determine all the operations and processes that occur during the issuance process, and site which ones will migrate or be replaced by the new DL/ID System processes
2	**Inventory, track, and report all DMV operational software on supported servers**	Prior to transitioning DMV operational software on a supported server, VALID will inventory and provide a report to DMV. VALID will not disable any functionality of the current operations until it has validated with DMV that its solution materially conforms to the SOW requirements, and only then, after DMV has authorized the disablement.
3	**List the baseline performance attributes of the current legacy environment**	Using the comprehensive list of baseline performance attributes, VALID and DMV can validate system performance of the DL/ID System environment post-migration, and determine what adjustments, if any, need to occur.

4	**Production Card Approval Documents**	VALID will produce Production Card Approval Documents of each card type.
5	**Describe the documentation, methods and procedures, personnel and organization to be used in the Transition.**	VALID will coordinate with DMV to describe in detail the documentation needed (user guides, quick reference guides, etc.), methods and procedures associated with a central issuance solution, as well as a thorough description of the personnel and organization that will implement the Transition.
6	**Provide a schedule of migration activities**	The project schedule will address all migration activities; and will update those activities weekly. VALID uses MS Project and its Gantt charts for this task. It will include a detailed list of all deliverables and milestones, depict the task durations, dependencies among tasks, and show task ownership (VALID, DMV, or another party). See Project Schedule.
7	**Roles and Responsibilities**	VALID will work with DMV to delineate the roles and responsibilities of DMV, the current contractor, and of VALID. It will coordinate with the DMV and its current vendor to prepare a Responsibility Matrix for discrete activity tasks, as part of the transition activities.
8	**Transition Readiness Assessment Checklist**	Cutover readiness assessment – is a critical planning artifact that provides a checklist of items which need to be complete prior to cutover. Items will be prioritized and integrated into the Transition.
9	**Show-Stopper Report**	This is another planning artifact that provides a risk assessment of issues with severities and impacts. This report will assess the current risks and provide ways to mitigate or deflect the risks so that the Transition takes place on schedule without disruption to DMV operations.
10	**Completion Criteria**	For each stage of the Transition, VALID will provide a definition of the completion criteria to enable an objective assessment when each stage has been successfully completed.
11	**Remediation Process**	VALID will establish a process to reschedule and re-execute any part of the Transition that the DMV deems to pose a risk or hazard to DMV's business interests.
12	**Production Readiness Confirmation**	Production Readiness Confirmation - Confirmation from VALID that (1) the DL/ID System has met all of the business and technical requirements; (2) it has no outstanding Level 1 Defects or Level 2 Defects; (3) all tasks and activities necessary to take the DL/ID System into Production, including applicable education and training, have been completed; (4) all Transition preparation has been completed; and (5) the new system is otherwise ready for Production.
13	**Training**	VALID will perform all training in accordance with its Training Plan for the operational, administrative, and technical staff. The training for the administrative and technical staff must be performed prior to

		production cutover; the training for the operational staff will occur at the time of installation as deployments occur. See Training Plan.
14	**Practice Cutover**	This is a practice and dry run for activating the Cutover to Production.
15	**Cutover**	Place DL/ID System and its components into Production upon written approval by DMV.
16	**Validation of Successful Transition**	This task is inclusive of user acceptance and assessment of acceptable performance with respect to comparison of baseline operational and performance attributes collected during preceding phases (i.e., design, build, and test).

4.9.3 Objectives of Practice Cutover

A practice cutover is utilized to practice and validate the Transition prior to Go Live! It is a way of fine-tuning the process and of minimizing risks prior to full production cutover.

- To exercise Go-Live cutover in the production environment
- To involve everyone in cutover to practice and confirm steps to execute cutover
- To discover and resolve logistical issues (e.g., deploying and setup of the equipment)
- To better understand timings

4.9.4 Cutover Entrance Criteria

- All key performance indicators (KPIs) and their success criteria are defined and pre-rollout metrics satisfied
- No outstanding Level 1 or Level 2 defects
- All tasks and activities to take DL/ID System into Production
- All training has been completed, or on schedule to be completed (with dates, user audiences defined, and training content prepared)
- All documentation and training support materials (quick reference guides, user guides, computer-based training, etc.) is approved, and ready for distribution
- An approved Deployment Plan is ready
- An approved Support Plan for the Operations and Maintenance effort is ready
- All identified critical or high priority risks are mitigated, transferred or accepted
- Practice cutover was successful
- Cutover Readiness Assessment checklist comprehensively addresses the readiness criteria, and it is approved

5. Deployment

This section describes how VALID will prepare for, setup, test, and verify equipment functionality, then deliver to each DMV location the evening before the scheduled cutover date, fully train the DMV location staff the following morning, and provide status reporting.

5.1 Deployment Schedule

The Schedule for the DMV's statewide rollout will be determined by the DMV. VALID Field Services will review the schedule on a week by week basis, throughout the rollout schedule, making any adjustments as directed by the DMV. VALID Field Services will strive to maximize our efficiency with the rollout and the training effort.

5.2 Deployment Preparation

In preparation for DMV deployments, the following will occur:

- The VALID Field Services will establish a central equipment depot in Vermont.
- VALID Field Services will receive, tag, and enter into its inventory system, all equipment procured for DMV sites. All equipment will receive an asset tag.
- VALID Field Services will prepare a set of site logs to be completed at DMV locations and DR offices. These site logs will be set up electronically, and able to print an individual sheet for each deployment location.
- VALID will create a set of checklists and scripted processes for the VALID Field Services team. These scripted processes will be used to help ensure that each technician follows his training to install software and drivers, in what order, and covers all aspects of the installation.
- VALID Field Services will deliver all image capture workstation (ICW) components to DMV office location the early evening prior to installation, and right after close of business, so as not to disturb normal business operations.
- During the Cutover Practice, the VALID Field Services teams will review the processes employed and the sequence of these activities, and make any needed adjustments. If additional cutover practices are warranted, they will be initiated. Similar timings will be used to review

the SLA requirements during the Maintenance and Support phase. During the Pilots, they will re-test this process at actual sites, and continue to make appropriate adjustments.

- In collaboration with DMV, the VALID Field Services teams will update their schedules of installation dates for all DMV locations at the beginning of the deployment, and maintain subsequent adjustment schedules for the remaining of the deployment. DMV will identify the quantity and type of equipment to be installed at each DMV location.

- VALID Field Services will provide the names of the individuals in each team in accordance with the current schedule.

- DMV will be asked to obtain contact information for each DMV location and provide that to the installation teams, at least two weeks prior to the selected installation date for each DMV site and DR office.

5.3 Rollout – This stage encompasses seven key phases, as follows:

- **Stage 1– External Services (DL/ID System data and photo service and EDL service).** This will ensure that external entities who inquire into DMV's system for data and image retrieval can access this information within the appropriate response times (e.g., DHS and state law enforcement).

- **Stage 2 – Back-Office / DMV Headquarters locations.** A small volume of folios that are processed in DMV headquarters and requires special handling. This will run for a two-day period.

- **Stage 3 – Front Office Capture/Issuance Pilot.** The Pilot would consist of a select number of business offices, representing multiple sizes of DL offices as well as differing geographic locations. What will be accomplished during the Pilot is validation of the front-end processes (including data communications), as well as a determination of any issues in the business end of this offices (such as remedial training needs).

- **Stage 4 – Statewide Deployment.** This consists of the deployment of the remaining location offices across Vermont as quickly as possible.

- **Rollback** – This stage is optional, and would only occur if a significant issue surfaces after Stage 1 has started, but before Stage 3 has begun.

Note: For field offices, once the process begins, any issues will be dealt with and corrected; there will be no rollback once the front office deployment is underway.

5.4 Installation

VALID Field Services technicians will install and test the equipment and application functionality the early evening (immediately after end of normal business activity) prior to the scheduled "Go Live" date at a given DMV location. The morning after installation, a VALID Field Services technician will be onsite at the applicable DMV locations to assist the DMV staff in using the equipment and the WebLink ID product.

The VALID Field Services technicians will perform the following tasks, in accordance with a scripted process that it will prepare and review with DMV.

- Install new camera towers with IC workstations
- Ensure that any needed chains to hold the camera backdrop screens are positioned
- Install the backdrop screens
- Check out the installation and perform functional testing on each piece of equipment
- Measure the distance from the camera to the drop down screen, and make any adjustments needed
- Install and or configure the most current image to the ICW systems which will include print drivers and additional software as necessary. We plan to use an ICW-specific Windows image that will be pre-configured for the printer drivers, WebLink ID shortcut(s), Capture Manager software, and Windows service.

The VALID Field Services team will ensure asset ownership tags have been applied to all installed equipment. Additionally, the team will remove and dispose from DMV locations and DR offices all packing materials and other debris from the installation. Any cabling will be neatly labeled and orderly.

The VALID Field Services team will maintain a site log that details the hardware and software configurations for each site. The site log will be the property of the DMV, and one copy will be left on-site with the DMV location the site designee and another copy will be sent to DMV point of contact.

5.5 Post Installation

The VALID Field Services technicians will arrive the morning after the installation of equipment at each DMV location and will do the following:

- The Field Services technician team will help them with any questions or training needs, and that will continue throughout the morning.

- Provide any needed equipment support
- Field Services technicians will not leave a DMV location without checking out with DMV manager / supervisor.

If at a later date, DMV requires the DL/ID System solution equipment to be uninstalled and then reinstalled and tested at a different location, VALID will perform that task in coordination with DMV, closely along the same installation processes as the original deployment.

5.6 Reporting

The VALID Field Services installation teams will report back through their established communications channels and established periodicity (daily calls and weekly reports) through a single point of contact regarding the deployment and installation of the equipment at each DMV location. The concept is to have the most current information regarding the installations in the hands of DMV.

During the installation the VALID Field Services team will complete a site log of the hardware and software configuration for each site. The site log will include all of the following:

- Date of Equipment Installation
- Site Location
- Equipment Installed
    - Asset Name/Model
    - Asset Tag Identifier #
    - Serial Number
    - Asset Descriptor
- Any Issues Encountered
- Special Concerns

A copy of the site log will be given to the site / location supervisor. At the end of the week, the site logs for all sites installed during that week will be sent to DMV for its review.

6 Operations and Maintenance

The VALID Field Service team will be responsible for troubleshooting, replacing equipment, reporting, and other assigned tasks, supporting the equipment and services deployed at the DMV locations. During the Operations and Maintenance (O&M) period which follows the Deployments,

the staffing level maintained by VALID will be more than adequate to meet DMV's SLAs in supporting the equipment and responding to all service calls. These Field Service technicians will be recruited from Vermont, and trained up prior to training and deployment.

6.1 Staffing and Coverage

VALID will position its field technicians throughout the state, as well as a manager/supervisor, to provide the needed coverage for maintenance and support. It will establish a central equipment depot VALID will maintain its staffing levels to support trouble calls throughout the state. VALID Field Services will maintain and distribute to DMV all the technicians' contact information including their names, physical location, mobile telephone numbers, and email addresses. VALID will also update DMV monthly on the equipment inventory, by product/model, maintained to support the DMV locations.

Our Field Services technicians will be fully trained on and capable of diagnosing, replacing and servicing the deployed equipment, both hardware and software, as well as their operation. They will have detailed maintenance documentation at their fingertips. VALID Field Support is responsible for service during business hours of all DMV office locations.

6.2 VALID Call Procedures

6.2.1 Initiating a service call

VALID will deploy a full set of equipment to each DMV location, and provide a toll-free number for DMV sites to contact it for any issues. When the DMV location contacts the VALID Help Desk, the latter will open a ticket and follow all issues to resolution. VALID will require the following information:

- Location of the office (full physical address)
- Contact person, phone number, and email
- A concise summary of the issue

6.2.2 Recording the call at VALID

VALID can receive Help Desk calls via web tracking, phone, or email. VALID will align its Help Desk coverage with DMV location schedules (generally, Monday thru Friday, 7:30 AM thru 4:30 PM (eastern time), except on Wednesdays, when the Help Desk will be available until 6 PM eastern time). Upon receipt of the call ticket from the DMV, the VALID Help Desk Service Representative (SR) will review the issue, and will either dispatch a VALID Field Technician to the site (Level 3), or will call the DMV site supervisor to get a clarification of the issue. Once dispatched, the VALID Field Technician will call the DMV contact person to apprise him or her of the ETA. If the VALID Help Desk can resolve the call over the phone, then the trouble ticket will be documented and closed. If a technician is dispatched, then the Help Desk will track the trouble ticket until the technician resolves the issue, and will document the timelines associated with that effort. In agencies with redundant Contractor provided equipment, if VALID-owned equipment needs repair or replacement, the service must be completed within 6 business hours of the initial report.

Upon arrival at the DMV site, the VALID field technician will notify the VALID Help Desk that he or she has arrived.

While the VALID Help Desk maintains a ShoreTel automated call distribution (ACD) system which will automatically track the calls, call duration, etc., the VALID HD SR will log the call into JIRA, VALID's issue management system, where the call will be recorded, tracked, and progressed through final resolution.

6.2.3 Closing the Call

When the VALID Field Technician completes the service call, either resolving the issue or replacing the malfunctioning equipment, then he will check out with the DMV site contact person, and then call the VALID Help Desk. The VALID HD SR will place a return message/call to the DMV Help Desk, and will resolve the call in JIRA. If malfunctioning equipment was replaced, then later, when the VALID Field Technician checks out the equipment at the VALID equipment depot, the actual cause of the malfunction will be sent to the VALID HD, which will update the issue within JIRA.

6.3 Reporting

By the 3rd working day of each month the VALID Help Desk will prepare a monthly report detailing the calls for the month, the issue resolution, time to resolution, and any other pertinent data. In the report, the Help Desk will provide DMV with any trends revealed by the monthly data or data over a past set of months (e.g., some issues with cameras might have been resolvable at the site by DMV staff). The report will be sent to the VALID Operations Manager for DMV who will review it and present it to DMV as part of her overall monthly reporting.

On an as-needed basis, using JIRA, the Help Desk can provide special reports on certain types of equipment or on specific DMV sites.

VALID Field Technicians will submit a daily report to their supervisor consisting of a list of all service calls closed, updated or otherwise worked on as well as any equipment replaced, brought back to the warehouse and any other tasks completed during their shift.

Each week the in-state VALID Field Services Manager will submit a report to VALID management for continued monitoring of events. VALID will provide a set of reports to the DMV as described below.

6.3.1 Daily Reports

- The "*Open Request Status Report*" will list all open service requests with performance and response times
- The "*Requests Closed Since Last Report*" will list all closed resolved requests with pertinent problems, resolutions, root causes, and performance information

Note: Should a systemic or repeating issue affecting a significant number of sites or devices occur, VALID Field Services may be required to update DMV with frequent (e.g., daily) progress conference calls until DMV regains its confidence that service requirements are being met.

6.3.2 Monthly Reports

- The "*Volume Summary Report*" contains all service requests that quantifies calls opened, closed, problem types, resolution, etc., by equipment type. This information will include a review of the previous 12 months to help identify trends.
- The "*Inventory Report*" shows the location and status of all VALID Field Services' equipment deployed throughout the state. It tracks installed equipment, spare hardware, equipment out-for-repair, and any "retired" (inactive and removed) equipment.
- The "*Performance Report*" lists all the performance data against SLA requirements including: (1) Response Time, (2) Arrival Time. (3) Time To Repair, and (4) Close Time

Note: This data is generated monthly, but published with a 12-month history for trend analysis

- The "*Ad Hoc Reports*" are on-demand reports to address a specific need such as call volume analysis, site history reporting, operator history reporting, etc.

6.4 Troubleshooting & Repair

VALID Field Technicians will try to reproduce the issue when they arrive on location so that they can either confirm the problem and repair it, or swap out any equipment needed. The VALID field technician will follow a basics-first troubleshooting procedure after arriving on location – making sure that all cables, connections and power are present and plugged in correctly. He will then try to power on, reproduce the error or reset the system.

In support of each service call to a DMV location, the VALID technicians will provide a summary of what the call entailed, the issues found, the actions taken and the status and closure of the issue. That information will be used to update the call ticker, and together with the call data from the VALID Help Desk (time call was received at VALID, time of dispatch, time call ended, etc.) an incident report will be prepared. VALID will send DMV a weekly summary of incident reports, and will provide detailed incident reporting monthly, distributed via email and/or uploaded into SharePoint or other DMV-preferred repository.

When the problem has been identified, reproduced, repaired or replaced, the VALID Field Technician will conduct a series of tests (TBD) to make sure that the system is fully operational, and ensure that the DMV office is able to complete a transaction. The Field Technician will ensure that the office completes a live transaction or if no customers are waiting, they will complete another test to ensure all is operational before departing site.

6.5 Equipment

It has been VALID's experience that it needs to maintain approximately 5% to 7% of its deployed equipment in inventory to replace malfunctioning equipment. The specific amount is dependent on the type and model of equipment. All equipment required by VALID will be newly manufactured, and will be inspected to ensure excellent working order.

VALID Field Services will replace malfunctioning equipment with identical equipment, and malfunctioning parts with identical parts. VALID will ensure that it acquires enough equipment and parts to handle the anticipated needs of DMV through the contract term, to ensure that equipment doesn't become obsolescent. VALID will track all its equipment, and will provide DMV visibility into the status of each serialized equipment from inventory to installation, to repair and back into inventory. The equipment deployed to each DMV location includes:

- Camera towers
- Backdrop screens for photos
- Signature pads
- Printers
- Scanners

6.7 Preventive Maintenance

VALID Field Services plans for its technicians to visit each DMV location once per year for the purpose of checking on the deployed equipment, and to assist the location staff, as needed. This includes inspection, testing, and calibration, as necessary to ensure that all components are in good working order and that the equipment will continue in good working order throughout the duration of the contract. In order to minimize

the impact to the normal business operations of DMV locations, the preventive maintenance will be scheduled at a time mutually agreed upon by DMV and VALID Field Services. The preventive maintenance call will include all deployed equipment (e.g., image capture workstations, cameras, etc.).

All maintenance activity performed at each DMV location will be approved by the DMV site supervisor. The VALID technician will record the name of the site supervisor and the date/time of the preventive maintenance visit, and any comments provided by the site supervisor. This data will become part of the preventive maintenance incident report. The call information for these preventive maintenance visits will be made available to DMV via email or SharePoint.

Appendices

1 – Project Schedule, with detailed level of activity

2 – Transition Readiness Assessment Checklist (To Be Published)

3 – Showstopper Report – A Risk Assessment (TBP)

4 – Repair Checklist (TBP)

Attachment #7 – Technical Resources Qualifications and Resumes

VALID has provided resumes on its technical resources, and has grouped them in according with their roles. We have an incredibly talented technical team earmarked to support Vermont DMV, and we appreciate the opportunity to present to Vermont DMV their experiences, proficiencies, and accomplishments.

Project Manager – [redacted]. While not a "technical resource" per se, the RFP directed us to put all resumes in one attachment. [redacted] has 25 years of project manager and engineering experience. His focus is full life cycle solution implementations. He is looking forward to applying his extensive experience and project focus on this vitally important project.

Development Team – Led by [redacted], this is an exceptional team of software architecting, design and programming talent. They use the Agile software development method with SCRUM as its framework for Agile development. [redacted] is a SCRUM Master with 30+ years of experience. The core developers that will be focused on the DMV implementation include [redacted], [redacted]. Justin Hale has access to additional development resources, as needed. This highly proficient team delivered a DL/ID central issuance system (CIS) for the State of Washington Department of Licensing (DOL) on time for their spring 2017 rollout as well as to the Territory of Guam. Each person on this team had specific roles in support of Wisconsin DNR and RTA.

- [redacted], *Software Development Manager.* With over 12 years of experience, Justin Hale has a stellar record of implementation successes, including extensive work with RTA, Wisconsin DNR, Guam and Washington DOL. [redacted] spent extensive time in Olympia, WA in a customer-facing, senior role to ensure successful resolution of that DL/ID project.

- [redacted], *SCRUM Master*. She has approximately30 years' experience in development, project lead positions, and software lifecycle support. [redacted] was instrumental in achieving our success at the RTA and Wisconsin DNR. She has been with VALID and its predecessor, ScreenCheck, for over ten years.

- [redacted], *Application Developer*. With over ten years' experience in the design and creation of application software, [redacted] has become VALID's lead developer for web-based AAMVA integration, a skill he acquired when working with Guam and Washington DOL. [redacted] was also heavily involved in support for RTA and Wisconsin DNR.

- [redacted], *Software Developer*. [redacted] has focused on providing VALID's customers, such as Washington DOL and Guam, with an excellent user experience.

- [redacted], *Software Developer.* [redacted] had a key role in the development of user interfaces for Washington DOL and Guam. He is talented, focused, and has excellent customer-facing skills.

Quality Management Team – Our quality management team is led by [redacted], who has extensive experience as a developer and tester. [redacted] and [redacted] will be the focal point for all quality and configuration management activities, questions and issues. They will implement and ensure adherence to quality initiatives and be responsible for overseeing the project's quality processes, for facilitating ongoing quality and process improvement activities, and for maintaining the overall quality approach for the project's processes and deliverables. focused on transforming the requirements into solutions with test scripts. They will be backed by an array of Quality specialists. Both [redacted] and [redacted] will be spending time in Montpelier working with the DMV Quality team.

- [redacted], *QA Development Manager.* With 30 years' experience as a software programmer and quality testing, [redacted] creates the testing plans for each type of testing, in collaboration with the DMV test team, and he directs the execution of the test cases, test scenarios.

- [redacted], *QA Lead*. Sam will be our QA Lead for the DL/ID System for the DMV. [redacted] has over 30 years' experience in software development and testing. He was also the quality lead for Washington DOL's CIS project, and was the primary driver for troubleshooting as well as both informal and formal testing in Washington. [redacted] will also help to train up the DMV QA team to prepare for SIT and UAT testing.

Data Conversion and Migration (DCM) Team – DCM is a critical process that requires extensive data mapping and usually changes in data formatting. Led by Allen Maskell, our DCM team specializes in migrating, transforming and managing data from legacy systems to VALID's proposed DL/ID system solution. This includes the data migration strategies, conversion sequencing, data integrity testing and data synchronization efforts.

- [redacted], *DCM Manager.* With over 20 years' IT experience in software development and data management, [redacted] directs the efforts of our DCM team, as he did with Washington DOL. [redacted] in integral to the development of the DCM plans, and he will direct the analysis and design of the data migration solution, as well as the implementation and testing of the DCM efforts.

- [redacted], *Senior Database Administrator*. [redacted] brings over 12 years' experience in development and database administration. He provides design and implementation of databases, and has become an expert with data conversion and data migration, as reinforced for the Washington DOL implementation. [redacted] is very accomplished as an ETL (Extract, Transform, Load) expert in converting data from one system to another.

Card Design Team – VALID has a particularly strong card design team of highly-skilled resources to support the design and manufacture of secure, durable credentials that exceed AAMVA's most current requirements. Our credential experts use card engineering resources and industry best practices to design and produce exceptional, high quality cards. The VALID card design team has placed over twenty of its designs into production throughout various US state agencies.

- [redacted], *Card Design Specialist.* [redacted] offers over 20 years' experience in designing permanent and temporary card credentials and ancillary documents such as outreach brochures and law enforcement pocket guides. She is qualified is the use of JURA's Security Design product, the worldwide standard for currency, certificates and credentials, and she is an expert on AAMVA card requirements. [redacted] designed the cards for WA DOL, Guam, RTA and Wisconsin DNR, as well as numerous other state jurisdictions.
- [redacted] *Director, Manufacturing Engineering.* Rick offers almost 40 years' experience in engineering, operations, and R&D [redacted] is an expert at all aspects of card manufacturing and card personalization, and he will direct our factory preparation for VT DMV cards. [redacted] and the DMV to ensure a quality design with a full array of card security features, and will guide the delivery of the card deliverables throughout the project, as [redacted] issuance programs in those and other facilities.

Solutions / Product Management – VALID has organized itself to enable an over-watch and feedback function by two executives who report to the Division Vice President and Project Sponsor. The Director of Solutions and Director of Product Management have key roles in this relationship whereby they will continually garner feedback from DMV regarding its needs, and they will guide the development of products and services and our solutions to meet those needs. In this way, as new opportunities emerge and new technologies gain traction, they will help ensure that VALID continue to provide DMV with an obsolescence-free solution that fully meets its needs.

- [redacted], *Director of Solutions.* With over 20 years of technology solutions implementations, 19 of those in identity management, credential issuance or biometric solutions [redacted] the teams responsible for client solution design, project planning, implementation, training and support. [redacted] primary role is to deliver the DL/ID system solution to DMV's satisfaction.
- [redacted] *Director of Product Management.* With extensive experience in product and business development, [redacted] is tasked with driving our product roadmap, a powerful tool to share with our customers regarding what is coming next. [redacted] maintains a coherent view of where VALID is headed, and as he garners input from our customers he will share with them our product goals.

[redacted]

Skills

- Full life cycle solution delivery
- Project and program management
- Portfolio management
- IT and software application development
- PMO creation and management

Experience

- Managed PMO for multinational manufacturing company.
- Managed SAP program for a multinational pharmaceutical company.
- Provided information engineering as a consultant for a multinational IT firm.
- Lead total quality management project for a national manufacturing company.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Arts**, Philosophy, Indiana University, Bloomington, IN
- **Candidate - Master of Science**, Information Systems, DePaul University, Chicago, IL

[redacted]

Skills

- DL / ID software systems
- Software development lifecycle (SDLC)
- Scrum / iterative development
- Solutions architecture
- Project management
- System integration specialist
- RESTful API's
- Database and software development

Experience

- Manage internal development and QA teams.
- Successful delivery of multiyear projects.
- Prioritize, plan, and track multiple projects.
- Extensive experience integrating software solutions.
- Architect high availability and fault tolerant systems.
- Deploy creative solutions to highly technical problems.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Science**, Computer Information Systems, DeVry University

[redacted]

Skills

- Software development
- Software design and troubleshooting
- Customer service
- Training and documentation

Experience

- Provide business, technical and software support.
- Define business, functional and technical requirements to improve processes.
- Effectively communicate solutions to technical and non-technical audiences.
- Train staff and prepare documentation for customers and the internal card production department.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Science**, Computer Technology, Purdue University, Fort Wayne, Indiana

[redacted]

Skills

- C#/.NET
- Javascript
- Java
- HTML/CSS
- Solutions architecture
- RESTful API design
- Database optimization and development

Experience

- Successful delivery of multiyear projects.
- Architect high availability and fault tolerant systems.
- Design and build complex systems of interoperability.
- Debug and implement solutions to resolve system issues.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Science**, Computer Science, Florida Atlantic University, Magna Cum Laude
- **Associate of Arts**, Palm Beach State College
- Oracle Certified SQL Expert

[redacted]

Skills

- Software development
- Database development
- RESTful API's
- DL/ID software systems
- System integration
- Software architecture
- Scrum/Agile development
- Software development lifecycle (SDLC)
- Written/verbal communication

Experience

- Deliver successful, multi-year projects on time.
- Develop software solutions that solve customer problems while adding value to the product as a whole.
- Maintain existing solutions to ensure reliability in the face of changing landscapes in technology and client needs.
- Work with additional teams in every facet of the organization to ensure a smooth process from conception to delivery.
- Research the latest proven technologies to improve the development and testing of current and future solutions.
- Serve as a trusted team resource for software development and application functionality knowledge, experience, and expertise.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Science**, Information Technology, Western Governors University
- **Associate of Science,** Summa Cum Laude, Computer Information Systems, Ivy Tech Community College

[redacted]

Skills

- DL / ID Software Development
- RESTful API's
- Sever Side / Client Side Software Development
- Database Development
- Software Integration
- Software Architecture
- Agile Paradigm / SCRUM Methodology of Development

Experience

- Delivered multiyear projects on time.
- Work with clients to build solutions for their needs moving forward.
- Integrate software on clients' systems.
- Protect PII of individuals managed in our software.
- Architect high availability and fault tolerant systems.
- Build tests to aid in detection of software malfunctions.

Related Employment

[redacted]

Education and Certifications

- **Associate of Applied Science**, Computer Information Systems, Ivy Tech Community College

[redacted]

Skills

- Software requirements analysis, design and testing
- Software coding/unit testing
- Test case and test scenario authoring
- System integration testing
- User Acceptance Testing support

Experience

- Transforms customer requirements into solution architectures, implementations and test code.
- Captures software requirements in UML models and readable, unambiguous English; generates requirements and testing documents.
- Provides clarification and direction to software implementers and testers.
- Performs troubleshooting, informal testing and formal testing.

Related Employment

[redacted]

Education and Certifications

- **Master of Science**, Computer Science, Ball State University, Muncie, IN
- **Bachelor of Science**, Mathematics/Computer Science, Purdue University, Fort Wayne, IN
- **Master of Arts**, English, University of Arizona, Tucson, AZ
- **Bachelor of Arts**, English, Ball State University, Muncie, IN

[redacted]

Skills

- Requirements development and management
- Software testing
- Customer support and training
- Hardware testing

Experience

- Design and construct test facilities.
- Develop test programs, methodologies, processes, plans and procedures.
- Develop system and software level requirements.
- Design and prototype mechanical components.
- Perform on-site systems integration and customer support.
- Maintained a Top Secret clearance for over 20 years.

Related Employment

[redacted]

Education and Certifications

- **BS**, EET, DeVRY Institute of Technology, Columbus OH
- Emergency Medical Technician, State of Indiana

[redacted]

Skills

- Access and SQL Server database and application development
- NCOA, merge/purge, and postal presort programming and marketing
- Installation and maintenance of MS Server 2003 with MS SQL Server
- Network installation, maintenance and troubleshooting of both hardware and software

Experience

- Manage team of 40+ developers and CSRs in meeting the needs of over 70 data clients.
- Extensive experience in data aggregation.
- Extensive experience in database migration from a data integrity point of view.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Science**, Electronics Engineering Technology, DeVry Institute of Technology, Lombard Illinois

[redacted]

Skills

- OLTP and OLAP database design
- Data conversion, migration, and administration
- Business Intelligence development – cubes, reporting
- .net application development
- Database server implementation planning.
- Data modeling tools: ER-Win, Toad, Visio
- Expert in Transact-SQL
- Microsoft Certified System Engineer (MCSE)

Experience

- Implement business logic and batch processing in backend using stored. procedures and functions.
- Extract, transform, and load (ETL) data between homogenous and heterogeneous systems using SQL tools.
- Create multidimensional cubes using the SQL server analysis.
- Provide SQL server reporting, database administration, and implementation of security on high availability in cluster environment.

Related Employment

[redacted]

Education and Certifications

- **Bachelor in Technology** (Computer Science and Engineering), BBS engineering college Fatehgarh Sahib, India
- **MBA**, Marketing, Apeejay Institute of Management, Jalandhar India

[redacted]

Skills

- Experienced with Excentro security design program, incorporating fine detail and non-counterfeit card designs and detailed feature sheets.
- Experienced with Jura banknote and currency security design program, incorporating fine detail and non-counterfeit designs.

Experience

- Awarded a certificate for Honorary State Trooper from the State of Alabama for an outstanding completion of the driver license, brochure, and web page delivery program.
- Lead person in developing a training procedure book for security design using AAMVA guidelines.
- Expert in brochures, logos, catalogs, packaging design and print production.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Science,** Certificate in Web Design, (Magna Cum Laude), Fitchburg State College
- Web Design Certificate
- Jura Security Design Program incorporating banknote quality.
- MacAcademy, Cambridge, MA

[redacted]

Skills

- Technical writing focused primarily on test methods, standard operating procedures, and product and process specifications
- Quality management including structured problem solving and continuous improvement
- Project management utilizing Microsoft Project
- Adobe Photoshop, Minitab statistical analysis, Microsoft Office product suite including Visio and Project

Experience

- Assist all VALID locations in their continuous improvement and waste reduction efforts. This work includes use of the six sigma and lean manufacturing toolsets.
- Create preliminary designs for equipment and materials in support of new contracts or bid responses.
- Evaluate new card manufacturing and material technologies, particularly as they apply to secure identity documents. Recommend adoption of suitable technologies.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Science (ACS certified),** Purdue University, Fort Wayne, Indiana
- Six Sigma Black Belt, General Electric trained, Rea Magnet Wire Company certified

[redacted]

Skills

- Manage and facilitate needs analysis and requirement gathering activities for custom solutions to be deployed globally
- Deploy solutions using industry standard project management methodologies
- Managed design, development, deployment and lifecycle of multiple hardware products, supporting SDKs and middleware layers generating over 50 million USD per year

Experience

- Managed the design and deployment of the ScreenCheck's WebLink ID 1.0 driver's license platform to the US Territory of Guam, while adjusting RealID standards and AAMVA compliance changes.
- Deployed the Chicago U-PASS program allowing students form over 60 universities access to Chicago's public transportation.
- Co-authored the WebLink ID 1.0 web based enrollment and card production software specification in 2012.

Related Employment

[redacted]

Education and Certifications

- **Associate in Arts,** Information Systems, Florida State University
- Checkpoint Scrum Master (PSM I) and Professional Scrum Product Owner (PSPO I) Certified

[redacted]

Skills

- Technical product management
- Multi-year and multi-application roadmap, requirements, and market analysis
- Expertise in web and mobile platforms and high-level application architecture design
- Large-scale requirements gathering and solution configuration for multi-year, multi-million dollar integrated identity system projects

Experience

- Leading the Valid delivery of its driver's license and ID card solution for the State of Washington Department of Licensing (DOL).
- Managed user requirements and software delivery for the State of New Jersey employee ID application.
- Managed user requirements and software delivery for Cubic Transportation Systems, Inc.
- Co-authored the initial software specification for the first generation web-based ID platform in 2009, and second in 2012.

Related Employment

[redacted]

Education and Certifications

- **Bachelor of Science**, Business Administration, Indiana University
- Pragmatic Marketing Certified, Level Six (PMC-VI)
- Scrum Master (PSM I) and Professional Scrum Product Owner (PSPO I) Certified

Attachment #8 – SLA with additional services

Describe any other services not mentioned in the above list that are included in your standard Service Level Agreement (SLA) and include a copy of your SLA with your response to this RFP. Label it he SLA Attachment #8.

As service level agreements (SLAs) reflect specific, measured aspects of the service offering, they tend to differ by jurisdiction in accordance to what is considered important or what needs specific clarification. SLAs tend to benefit both the State and VALID by providing clarity in setting expectations about the services provided. VALID has provided below two charts for SLA review. The first is a suggested set of SLAs specific to this project. These SLAs reflect some of the service levels VALID is current performing or has performed with other jurisdictions. VALID has provided a description of each SLA, a suggested measurement and its suggested credit back to DMV for failure to meet a given SLA. VALID's expectation is that it will meet and negotiate a final set of SLAs with Vermont DMV, prior to contract signing.

[redacted]

[redacted]

Below is a sample of a monthly SLA report on some selected SLAs. VALID would craft together a monthly report format, for the approval of the DMV, that would reflect the status of the SLAs. This could be submitted with each invoice to the DMV.

[redacted]

Figure 70: Sample Monthly SLA Achievement Report

Attachment #9 – Card Feature Sheet

THE SECURE SIDE OF INNOVATION

STATE OF VERMONT
Department of Motor Vehicles

State of Vermont

Security Features

Preprinted Design Detail (Composite)

[redacted]

Not indicative of actual print color. For reference of card features only. 1

VALID THE SECURE SIDE OF INNOVATION

STATE OF VERMONT
Department of Motor Vehicles

State of Vermont

Security Features

Preprinted Design (5 PMS Colors) Composite

[redacted]

Not indicative of actual print color. For reference of card features only. 2

VALID THE SECURE SIDE OF INNOVATION

STATE OF VERMONT
Department of Motor Vehicles

State of Vermont

Security Features

[redacted]

Not indicative of actual print color. For reference of card features only. 3

VALID THE SECURE SIDE OF INNOVATION

STATE OF VERMONT
Department of Motor Vehicles

State of Vermont

Security Features

Preprinted Design Detail (Polycarbonate)

[redacted]

Not indicative of actual print color. For reference of card features only. 4

VALID THE SECURE SIDE OF INNOVATION

STATE OF VERMONT
Department of Motor Vehicles

State of Vermont

Security Features

Preprinted Design (4 PMS Colors) Polycarbonate

[redacted]

Not indicative of actual print color. For reference of card features only.

5

VALID THE SECURE SIDE OF INNOVATION

STATE OF VERMONT
Department of Motor Vehicles

State of Vermont

Security Features

Permanent Driver License Polycarbonate Laser Engraved

[redacted]

Not indicative of actual print color. For reference of card features only. 6

VALID THE SECURE SIDE OF INNOVATION

STATE OF VERMONT
Department of Motor Vehicles

State of Vermont

Security Features

Back of Card

[redacted]

Not indicative of actual print color. For reference of card features only. 7

VALID

THE SECURE SIDE OF INNOVATION

STATE OF VERMONT
Department of Motor Vehicles

State of Vermont

Glossary

CARD BODY DESIGN FEATURES

CARD SERIAL NUMBER
Identifier printed on card and/or on main components of the card before transfer to the personalization center(s).

COMPOSITE CARDS
Composite cards combine layers of PVC and PET. They combine the low cost and printability of PVC with the superior flexibility, durability and impact strength of PET. This combination accepts a wide variety of security features and has an excellent track record having been used for some time in programs throughout the USA.

POLYCARBONATE CARDS
Cards are fully fused and cannot be peeled apart like Teslin, PVC and composite cards. Polycarbonate cards are a single, monolithic piece.

UV-A DULL SUBSTRATE MATERIAL
Substrate material exhibiting no visibly detectable fluorescence when illuminated with UV light or with a controlled response to UV at 365 nm.

SECURITY DESIGN, RESISTANT TO REPRODUCTION FEATURES

DUPLEX SECURITY PATTERN
A design made up of an interlocking pattern of small irregular shapes, printed in two or more colors and requiring very close register printing in order to preserve the integrity of the pattern.

GUILLOCHE SECURITY DESIGN
A pattern of continuous fine lines, usually computer generated, and forming a unique pattern that can only be accurately re-originated by access to the software and parameters used in creating the original design.

LATENT IMAGE/DATA (IMAGE RELIEF)
A hidden image formed within a relief image which is composed of line structures which vary in direction and profile resulting in the hidden image appearing at predetermined viewing angles. A latent image/data is subject to the condition of the correct viewing angle-visible to the human eye without further equipment.

MICROPRINTING TEXT WITH DELIBERATE ERROR INTO THE DESIGN OR MICROPRINT
Very small text printed in positive and/or negative form, that may be used in conjunction with rainbow printing and which can only be read with the aid of a magnifying glass and not exceeding 0.3mm in height.

The proposed card design show "**VERMONT**" repeated in multiple areas. The deliberate error reads "**MERMONT**".

NO CMYK COLORS AND AT LEAST 2 SPECIAL COLORS
Colors that are not easily reproduced using CMYK colors.

SECURITY INK/PIGMENT FEATURES

INFRA-RED FLUORESCENT INK (IR)
In daylight invisible ink, which can only be seen when applying light in the infrared spectrum (630nm).

OPTICAL EFFECT PIGMENT
Visible or invisible pigments incorporated in an ink which is designed to be controlled by eye such as; optically variable ink also called color shifting inks, or iridescent inks.

UV FLUORESCENT INK IN SECURITY BACKGROUND PRINTING
UV fluorescent ink can be either transparent or integrated to an ink visible to the naked eye; in addition, some UV fluorescent inks can respond to standard wavelength UV light with one color and with another color to a shorter wavelength UV light, called Bi-UV.

PROTECTING PERSONALIZED DATA FEATURES

ENHANCED READABILITY
Data element contrasts optimized for ideal readability day or night.

GHOST PORTRAIT
A lighter reproduction of the original image that appears in the same area as the personal data such that the image appears to be in the background and the personal data can still be read without interference.

LAMINATE, OVERLAY OR COATING FOR SURFACE PRINTED DATA AND PORTRAIT
A transparent material, which may have security features such as optically variable devices contained within it and which is designed to be securely bonded to the DL/ID to protect the dynamic data elements and the security features within the card structure.

LASER ENGRAVING
A process whereby a laser is used to alter the card-body material to display information. The information may consist of text, images, pictographs and security features. (up to 1200 DPI). A fully Laser engraved card is embedded in the card body and cannot be easily altered, it is also highly abrasion resistant. The overlay is fully fused to the core material during the lamination process.

LEVEL 3 FEATURE
At least one Level 3 security feature is required. Specifics are not considered in this standard because level 3 security features are generally disclosed and only discussed between experts on a need-to-know basis. Issuing authorities may add additional security features to bolster security against any specific threats, provided such features do not have an adverse impact on other security features or personalized information.

Per RFP requirements and best practices, Valid USA's proposed level 3 feature(s) disclosure shall be in accordance with RFP proposal delivery specifications.

USE OF NON-STANDARD TYPE FONTS
Type fonts that are of restricted availability. The proposed card design shown in "**EXP**"=**EXP**. Also, shown in microprint.

PDF 417 BARCODE (1D AND 2D BARCODE)
The 2D barcode size is determined by how much demographic data (encrypted or unencrypted), it must contain error detection and correction level.

PRINTING DYNAMIC DATA ELEMENTS USING DIGITAL IMAGING TECHNOLOGIES
Information specific to the document and the holder.

REDUNDANT PERSONALIZED DATA
Dynamic text and/or image to be printed more than once for redundancy checking by whatever means.

The proposed card design show date of birth repeated on card back.

SECURITY BACKGROUND OVERLAPPING THE PORTRAIT IMAGE AREA
A pattern of continuously fine lines constructed by using two or more lines overlapping bands that repeat a lacy, web-like curve. (Shown in portrait and ghost portrait).

Not indicative of actual print color. For reference of card features only

8

Attachment #10: Knowledge Transfer and Training Plan

Vermont DL/ID System - Knowledge Transfer and Training Plan

Plan Overview

The DL/ID system is an intricate, business-critical application. Given its complexity, the process whereby VALID will provide knowledge transfer (KT) and training to the DMV staff regarding new processes, workflows, and the use of the DL.ID system is vitally important.

VALID will provide extensive training to the four critical groups associated with the DMV:

(1) Operational (front office) staff
(2) Administrative (back office) staff
(3) IT/Technical Staff
(4) External partners – (including law enforcement and retailers)

This document addresses the training needs of all these groups.

VALID's Knowledge Transfer (KT) program is a very specialized form of training, encompassing a transfer of acquired experiences from mentors who are proficient at using and maintaining the new solution to a set of identified mentees. VALID's mentors will teach all mentees how to use and support the new system.

In this plan, we will address how we will match responsibilities in the new DL/ID system solution to current DMV staff, determine how to establish their proficiencies in using and supporting the new system, develop individualized action plans, assign mentors, and review and report on the progress of the KT initiatives.

Goal

The overall goal of the training program for Vermont is to enable your DMV team to become self-sufficient in a given activity or task and to understand the core functionality of the system in such a manner as to enable modification processes and flows to support the DMV's ever-evolving business. In addition, the DMV external partners will be given the documentation they need to perform their missions in relation to the new DMV IDs/DLs.

Objectives

VALID's training objectives for Vermont are as follows:

- Provide and implement a comprehensive and complete training program to enable your DMV staff to quickly grasp and effectively utilize the DL/ID System Solution.
- Assure that the DL/ID System Solution training program is integrated within a role-based training model.

- Address and incorporate business process changes being undertaken by the DMV.
- Address and incorporate technical changes being undertaken by the DMV.
- Coordinate with the DMV's DL/ID System project manager and team.
- Address the unique challenges and opportunities of the DMV operations and assist the DMV to prepare for Production.
- Provide training to the DMV-designated personnel to enable them to train all appropriate end users on the DL/ID System Solution functionalities.
- Support a comprehensive training effort for end users.
- Provide the documentation (e.g., brochures / PowerPoints, etc.) needed by the external partners to perform their roles relative to IDs and DLs.
- Prepare the DMV staff in assuming ongoing operations and maintenance in the post-Production phase.
- Identify an overview of skills and positions that need to be properly staffed for a smooth transition and continuation of support and maintenance by the DMV staff.
- Prepare the DMV personnel who will provide support to end-users.
- Ensure knowledge is transferred to the DMV staff so the DMV has sufficient proficiency in supporting the solution.

Training

Roles and Responsibilities

The VALID trainers will focus on the functions of WebLink ID and BioLink ID–VALID's two key products.

Operational Personnel Training

VALID will focus on the image capture workstation (ICW), and similar functions of WebLink ID. VALID will provide user manuals, quick reference guides (job aids), web-based training, and other training documentation, after conferring with the DMV. VALID will conduct the in-field pilot office deployments, as well as answer any VALID-specific questions about WebLink ID and BioLink ID.

The DMV's responsibilities include having the operational staff available for training, providing the venue for the training, and supporting the training with super users who will help explain the changes from the legacy solution to the new DL/ID System solution.

Administrative Personnel Training

Similar to the front office training, VALID will directly train the administrative staff training; however, due to the diverse nature of the administrative teams, the content of the training will differ by Back Office user group, the administrative staff available for training, and selection of the venue for the training.

IT / Technical Personnel Training

Much of VALID's technical training will occur via on-the-job training (OJT) efforts in concert with VALID technical staff visits to Montpelier whereby the technical teams from VALID and the DMV will work closely, and learn from each other. In addition, VALID will train the technical staff regarding the administrative functions of its two primary, integrated products – WebLink ID and BioLink ID. Moreover, VALID will formally train up the DMV QA staff regarding WebLink ID and BioLink ID so that the DMV QA team can better conduct QA testing at UAT. Finally, VALID will support the technical team with a Procedures Manual which it will prepare, including a series of "walkthroughs" of the document to ensure its comprehensiveness and usefulness to the DMV technical team.

External Partners

VALID will do its part to help educate and train law enforcement and retailers regarding the new IDs/DLs. VALID will make itself available to support Law Enforcement seminars or other venues in which the security features of the DMV's Driver's License and Identification cards will be presented. What is primarily needed is hand-out materials that will assist law enforcement and retailers to better understand the changes being introduced into the DMV's ID/DL. VALID will help the DMV with the design of brochures or PowerPoints that the DMV can make available to Law Enforcement and Retailers.

Training Approach

The Training Plan tailors the curriculum and delivery across the four main target audiences. VALID, in conjunction with the DMV project team staff, will develop the strategies to ensure effective and efficient training of the DMV staff on all components of the DL/ID System Solution and is integrated into the DMV staff training program. VALID's experience at other customer sites, including templates and content, is leveraged to maximize successful adoption of the DL/ID System Solution. The following elements are incorporated into the approach used to execute the Training Plan:

- 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

  Materials will be created for each of the following role-based constituencies:
    - The DMV operational staff
    - The DMV administrative staff
    - External partners
    - IT / technical staff
    - Other roles to be specified by the DMV to support its business operations

- Develop and deliver comprehensive training materials, specifically designed and tailored to meet the business requirements of the DMV as configured in the DL/ID System Solution, covering all important business functions as determined by the DMV.
- Perform a document walkthrough (review) of all draft training materials and other documentation with the DMV prior to the documents' final revisions. This includes user guides, training aids, brochures, and quick reference guides, etc.
- Perform a "dry run" training presentation to the DMV staff for approval, including all training materials. The training materials will be provided in electronic formats, which can be readily edited and reproduced.

Operational Personnel

The Front Office Personnel Training Plan Requirements Table outlines and describes the requirements to be addressed for the DMV staff.

Operational Training Plan Requirements Table

Requirement Title	Requirement Statement
VALID and Education Manager	VALID to provide a training manager (lead) to manage the overall training plan.
Operational Staff Training Plan	VALID will refine the training plan for the DMV's operational staff, reviewing the plan's objectives, schedule, strategies for designing and developing curricula, and supporting training materials, training environment data, and methods for implementation. The Operational Staff Training Plan will include the following: • Method of training. • Length of training (estimate number of hours for each type of employee). • Facility requirements for training. • Detailed outline and description of each training session • List of training materials, user manuals and samples.
Training Curriculum	Addresses all components required, including curricula tailored specifically to operations staff and provides the content of the training courses including target audience, goals, objectives, instructional materials, time frame, and training evaluation.
Customized Web-based Training	VALID will provide customized web-based training to meet the DL/ID System Solution's training needs.
Customized Training Materials	VALID will develop customized and comprehensive training materials for the operational staff. Complete, comprehensive end-user training materials consisting of custom web-based training modules, the materials for instructor-led training, and practice scenarios.
Quick Reference Guides	The quick reference guides have been completed and are fit for purpose.

Final Revisions	Final revisions and edits are made to end user, instructor, on-line help, custom web-based trainings and printable course materials based on input from VALID and the DMV.

VALID understands that the DMV operations staff must receive sufficient system management and operations training to provide daily operational proficiency. The training at each site will include the following:

- Equipment/software driver information and operation.
- Trouble shooting and monitoring.
- Preventive maintenance tasks (i.e. cleaning, refills, replenishment).
- DL/ID solution operation.

Operational Personnel Training Curriculum

The operations personnel training curriculum may include the following:

- Introduction
- Software and equipment
- Overview of the DL/ID card production process
- Administrative functions
- Photo and signature best practices
- Preventive maintenance and troubleshooting
- Hands-on training
- Security processes and procedures
- Help desk procedures
- Question and answer session
- Training evaluation form
- Production support

Administrative Personnel

VALID will deliver to the DMV's administrative personnel training in the DL/ID System Solution. The Administrative Personnel Training Plan Requirements Table, shown below, outlines and describes the requirements to be addressed for each of the role-based constituencies.

Because the needs of the administrative DMV staff are so diverse and specialized, training modules will be created to address each functional area in separate training sessions, in accordance with a published schedule, agreed upon by the Training Directors from the DMV and VALID, respectively. VALID will focus on its two products, BioLink ID and WebLink ID.

Administrative Personnel Training Plan Requirements Table

Requirement Title	Requirement Statement
Administrative Training Plan	Refine the administrative training plan to train the DMV administrative personnel. The component must include and provide

	information on how the DL/ID System Solution interacts with other systems operated by administrative to enable such personnel, within their area of responsibility, to maintain and support their business functions on an ongoing basis. The Training Plan will include the following: • Method of training. • Length of training (estimate number of hours for each type of employee). • Facility requirements for training. • Detailed outline and description of each training session. • List of training materials, user manuals and samples.
Conduct training to Back Office personnel	Conduct training for the DMV administrative personnel.
Training Curricula	Address all components required, including curricula tailored specifically to business personnel and provides the content of the training courses including target audience, goals, objectives, instructional materials, time frame, and evaluation.
Customized Web-based Training	For roles-based constituencies selected by the DMV, VALID will provide customized web-based trainings to meet the DL/ID System Solution training needs.
Customized Training Materials	VALID will develop customized and comprehensive training materials for the operational staff. Complete, comprehensive end-user training materials consisting of custom web based trainings, a set of materials for classroom based instruction, and for each, practice scenarios.
Quick Reference Guides	The quick reference guides have been completed and are fit for purpose.
Final Revisions	Final revisions and edits are made to end user, instructor, on-line help, custom web based trainings and printed course materials based on input from VALID and the DMV.

The DMV Staff must receive sufficient system management and operations training to provide daily operational proficiency. Training will be conducted by VALID at the DMV facilities and must include, but not be limited to, the following:

1. Equipment/software driver information and operation.
2. DL/ID solution operation.
3. DL/ID solution maintenance.
4. Troubleshooting and monitoring.
5. Preventive maintenance tasks (e.g., cleaning).
6. Reporting.

Administrative Personnel Training Curriculum

The Administrative Training will include the following topics/subjects:

- Introduction
- Software and equipment
- DL/ID solution operation
- Administrative and supervisory functions
- Photo and signature best practices
- Reports and audit functions
- Preventive maintenance and troubleshooting
- Hands-on processing
- Security processes and procedures
- Help Desk procedures and escalation
- Questions and answer session

IT / Technical Personnel

This section addresses the DMV technical team who will work with VALID to integrate the DL/ID System solution for testing and support the application software at their data center, and the Maintenance and Operations (M&O) staff who will support the DL/ID System solution after the project has deployed.

Technical Team – VALID will educate and train the DMV's technical team on the administration, architecture, troubleshooting, and issue management and other technical aspects of the DL/ID System Solution, as requested by the DMV, in order to enable the DMV's technical ownership of the DL/ID System solution following completion of the DL/ID System project. VALID will provide the DMV technical team with a Procedures Manual that it will walk-through to explain the VALID environment, how to configure and install new software updates, and how to provide ongoing support for the application.

Maintenance and Operations – After the DMV identifies the staff who will support ongoing maintenance and operations, VALID will provide tailored training to each to ensure that they can perform their duties.

The IT / Technical Personnel Training Plan Requirements Table outlines and describes the requirements to be addressed for each of the role-based constituencies.

IT / Technical Personnel Training Plan Requirements Table

Requirement Title	Requirement Statement
IT / Technical Training Plan	Refine the IT / Technical Training Plan to educate and train the DMV technical personnel. The IT/Technical Training Plan will include: • Method of training. • Length of training (estimate number of hours for each type of employee). • Facility requirements for training. • Detailed outline and description of each training session. • List of training materials and samples including all maintenance user manuals and product specifications.
Conduct training of IT / Technical personnel	Conduct training for the DMV technical personnel.

Technical training should include, but not be limited to:

1) Routine information technology management tasks.

DL/ID solution operation, as well as an overview of the system hardware and software driver products architecture and connectivity, hardware component and system installation, hardware and software driver products problem diagnosis and resolution, software driver products distribution, etc.

DL/ID solution maintenance.

System integration and development.

Troubleshooting and monitoring.

IT/Staff Training Curriculum

The IT / Staff Training curriculum is as follows:

- Introduction
- Software and equipment
- DL/ID solution operation
- Administrative and supervisory functions
- Routine information technology management tasks
- Architecture and connectivity
- Hardware component and system installation
- Problem diagnosis and resolution
- Software driver products distribution
- Security processes and procedures
- Help Desk procedures and escalation
- Hands-on processing

- Questions and answer session
- Evaluation forms

Law Enforcement and Retailer Training

VALID will support law enforcement and retailers by providing training tools to better understand the new IDs and DLs that will be issued.

- Law enforcement needs to fully understand the endorsements and restrictions on licenses. Thus, VALID will help design a brochure, flier, or wallet-sized crosswalk card explaining endorsements and restrictions, which the DMV can print as its needs require.
- To address the security features on IDs and DLs so that law enforcement officers can quickly discern potential fraud, VALID will support the DMV's efforts to provide training information (e.g., PowerPoints) and to provide security training to Law enforcement groups, on an as-needed basis.
- Some retailers (restaurants, bars, and stores selling cigarettes) are concerned about quickly reviewing the new IDs and DLs to determine a person's age. Therefore, VALID will design and produce a set of single-page brochures which will graphically explain how to find the birth date of a given individual. This brochure will be given to the DMV in a format that can be readily printed by the DMV, as needed.

Other Specified Training

There are some additional training activities that must take place to ensure a cohesive, efficient operation of the DL/ID System Solution:

1. User acceptance testing (UAT) training
2. End user support training
3. Technical training

User Acceptance Training (UAT) Training

In support of UAT VALID will provide 'just-in-time' (JIT) training of the DMV staff that will support UAT. This will include UAT testers and "super users" from the operational staff who will help train up others in their offices. This training will occur approximately 1-2 weeks prior to the start of UAT. The training will include how to review and use the test scenarios / test scripts and how to log any errors found. VALID will provide enough training on the WebLink ID and BioLink ID products that testers will be comfortable navigating the system in compliance with the test scripts. The DMV will provide overarching leadership regarding the UAT Training; and VALID will provide training documentation and JIT Training of its WebLink ID and BioLink ID products. Testers will be trained to work from test scripts and follow written test scenarios. All training materials will go through a dry run for critique and to ensure consistency he DMV end-user.

Support Training

The following groups will be trained as part of the DMV's end-user training:

Front Office (Operations) Personnel – Upon VALID's initial installation and training of the Front Office staff at each installation, a VALID service team will remain to assist each office for approximately ½ day.

Technical Training

Some of the technical training for the DL/ID System project will occur during the testing phase where VALID Technical staff will walk-through the processes and procedures with the DMV Technical team. In addition, we will train-up the DMV QA staff to help them plan for and run UAT.

Methods and Materials

Training typically includes a combination of training methods and materials to meet all audience needs. All classes must contain scenario-based process flows, and clearly state the audience and purpose up front. Realistic mock-up data will be used whenever possible. Once all classes and materials have been created, VALID will provide a walk-through for the DMV to ensure that audience needs are being met.

The following is a list of the methods that may be used for training:

- Hands-on training (sandbox training)
- Instructor-led training (classroom training)
- Webinar training
- User Manual updates
- Fully responsive eLearning (web-based) courses created using Adobe Captivate that include:
  - Narrated presentations
  - Interactive process flow tutorials
  - Demonstrations

VALID understands operational time constraints at the DMV locations, and recommends the use of demonstration videos as a key training method. In addition, VALID recommends holding a one-time Webcast (approximately 45 minutes in length) that can be posted for future viewing.

Following is a list of the materials that may be used for training:

- Training plan and syllabus
- Handouts
- User Guides (PDF and Microsoft Word versions)
- Web-based training materials (demos, videos, etc.)
- Quick reference guides (including troubleshooting) (laminated)
- Presentation materials
- Training evaluation surveys

Deliverables

Following are the specific deliverables for each audience type:

- Develop a training strategy for each class, and formalize that strategy into a plan. Plans will include:
  - A description of the training tasks, including its duration
  - The number of participants per session
  - A detailed list of the tasks a participant must perform
- Develop curriculum plans and training materials in electronic (printable) and web-based training formats.
- Deliver training programs in an electronic format to operational staff and to technicians.
- Create end-user surveys to determine the adequacy of the training courses and materials.
- Update project documents and training materials to enhance and improve them.
- Project Manager to certify that all deliverables were completed.

NOTE: If significant changes are made in any new version of the DL/ID System, "refresher" training will be provided within 30 days prior to the release of the new version.

Topics

VALID will provide training on the following topics as determined by the DMV in addition to other topics as determined by the DMV and VALID:

(a) The central issuance solution and all Interfaces among the DL/ID System and Third Party Software.

- WebLink ID and BioLink ID
- Workflows
- WebLink ID Designers

(b) Enhancements to the DL/ID System Solution and interfaces.

(c) All available maintenance and support tools, utilities, diagnostic programs and supporting programs utilized by VALID in the support and maintenance of the DL/ID System Solution, interfaces and other deliverables.

(d) Security requirements and methodologies implemented under the terms of the Agreement to prevent or detect unauthorized access, and any networking security tools.

(e) The installation/maintenance of tools to support network performance analysis.

(f) Management and troubleshooting, including how to install and utilize management and remote troubleshooting tools.

(g) Maximizing the use of the DL/ID System Solution, Interfaces and other deliverables to perform key operational functions, including data backups, program downloads, and security checks and how to automate such functions to minimize manual intervention.

(h) Any and all updated, changed, or revised policies, practices, procedures, processes, and/or techniques with respect to the information previously transferred to the DMV.

Knowledge Transfer (KT)

Knowledge Transfer (KT) is a key training component to achieving a smooth transition to using the DL/ID System solution. The Knowledge Transfer Plan describes the training activities specific to ensuring that the DOL staffs gain a full understanding how to operate the new DL/ID System solution without outside intervention. KT focuses on each role of the DMV staff. It enables the use of individual action plans through the intervention of assigned mentors to assist in the learning process.

KT Roles and Responsibilities

The following table depicts the roles and responsibilities of all participants in the knowledge transfer process.

DMV	VALID	DMV / VALID
• Identify DMV Staff to undergo knowledge transfer. • Establish the DMV staff's roles for the new DL/ID Solution; and describe what the DMV Staff members individually want to get from the knowledge transfer. • Enable the availability of staff for KT.	• Assign mentors for each DMV staff who will undergo KT. • Provide mentoring throughout project. • Assess the proficiency of their assigned DMV staff to support the DL/ID System solution at project termination.	• Work through the individual action plans. • Involve the DMV staff in the design, development, and testing activities to the extent that DMV staff are available. • Provide staff with substantial roles in the pilot and rollout.

KT Process/Approach

VALID will work with the designated DMV personnel to learn all aspects of the new solution in order to significantly improve the proficiencies of the DMV's staff to use and support the DL/ID System solution. VALID's Knowledge Transfer effort will include the following tasks:

- Establish knowledge transfer needs by individual role
- Identify Knowledge Transfer participants within the DMV (note: there is often a preponderance of technical staff who require KT, but the value of KT is not limited to technical roles)
- Determine from the DMV the proficiency levels of identified staff to undergo KT
- Set individual baselines for each position – the baseline skill estimates would be customized to the individual enabling future comparison and progress evaluation.

- Assign by role the VALID mentors to each person in the DMV knowledge transfer program; each VALID mentor will endeavor to meet with each person assigned to him.
- Establish an action plan for each knowledge transfer participant with concrete objectives and success criteria
- On an ongoing basis, VALID mentors will meet telephonically with their assigned the DMV technicians to discuss critical topics in the project. They will share with the DMV technicians the how and why behind the designs, builds, testing and ongoing support.

Potential KT Topics

VALID will focus its knowledge transfer efforts on the topics identified by the DMV as crucial to their success. Some example topics might be:

- The DL/ID System Solution and all interfaces between and among the solution and third-party software.
- Enhancements to the DL/ID System Solution and interfaces.
- Understanding the data files and data definitions and relationships, data models, program and logic, interfaces, program architecture, design concepts, system designs, program structure, sequence and organization, screen displays and report layouts relating to the DL/ID System solution.
- All available maintenance and support tools, utilities, diagnostic programs, and supporting programs utilized by VALID in the support and maintenance of the DL/ID System solution, interfaces and other deliverables.
- Security requirements and methodologies to prevent or detect unauthorized access, and any networking security tools.
- Management and troubleshooting, including how to install and utilize management and remote troubleshooting tools.
- Maximizing the use of the DL/ID System solution, interfaces, and other deliverables to perform key operational functions, including data backups, program downloads, and security checks and how to automate such functions to minimize manual intervention.

KT Requirements

The following Table outlines and describes the requirements to be addressed:

KT Requirement Title	KT Requirement Statement
Knowledge Transfer Plan	Develop the Knowledge Transfer Plan to develop the needed proficiencies by the DMV staff to fully use and support the DL/ID System solution on a going forward basis.
Conduct Knowledge transfer activities and provide	Provide knowledge transfer support to the designated DMV staff personnel. This specific training will differ by DMV staff role.

KT Requirement Title	KT Requirement Statement
Knowledge transfer to technical personnel	
Knowledge Transfer Assessment	The DMV will assess the effectiveness of the knowledge transfer efforts to the DMV technical personnel.
Deficiencies Addressed	If there are deficiencies identified, the DMV and VALID will supplement the knowledge transfer program with additional training to remedy the deficiencies.