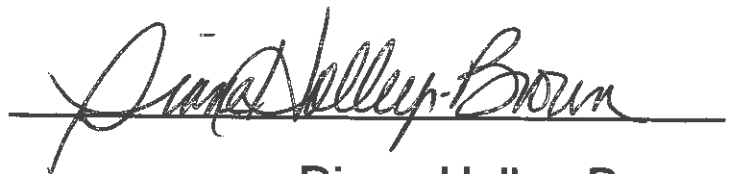


# NOTICE

Please note that this bid from Veridos Identify Solutions for solicitation CRFP DMV18\*1 was received at the Purchasing Division office prior to the established bid opening date and time (July 2, 2018 at 1:30pm) as noted on the time stamp. However, the bid was not publicly opened and read aloud.

A handwritten signature in black ink, reading "Diane Holley-Brown", is written over a horizontal line.

Diane Holley-Brown  
Assistant Purchasing Director



State of West Virginia

## RFP to Provide Driver's License and ID Cards

RFP DMV1800000001

### Technical Proposal - ORIGINAL

Submitted To:

Melissa Pettrey, Senior Buyer  
Department of Administration, Purchasing Division  
2019 Washington Street East  
Charleston, West Virginia 25305-0130

Submitted By:

Veridos America, Inc.  
45925 Horseshoe Dr.  
Dulles, Virginia 20166

06/29/18 09:58:49

WV Purchasing Division

Sales Manager: Kathleen Synstegaard

Proposal Manager: Nick Larter

Date: July 2, 2018

## Requests for Additional Information

All inquiries or requests for additional information should be made to the responsible party below:

Kathleen Synstegaard

Director, Sales USA

45925 Horseshoe Dr. Dulles, Virginia, USA

612.618.5124

[Kathleen.synstegaard@veridos.com](mailto:Kathleen.synstegaard@veridos.com)

## Table of Contents

<b>Requests for Additional Information .....</b>	<b>2</b>
<b>Letter of Transmittal.....</b>	<b>5</b>
<b>Attachment A: Vendor Response Sheet .....</b>	<b>6</b>
<b>Full End-to-end Solution .....</b>	<b>7</b>
<b>Security of Central Issuance.....</b>	<b>7</b>
High Level Overview of Veridos' Solution .....	9
Veridos as a Partner .....	9
Secure Manufacturing in the United States .....	10
Veridos' Experience .....	10
Partnerships for West Virginia DMV .....	14
References .....	15
Staffing Plan .....	22
<b>Proposed Security Features.....</b>	<b>40</b>
<b>Attachment B: Mandatory Specification Checklist.....</b>	<b>178</b>
Data Migration Process .....	202
Data Migration Plan .....	203
Development 1 .....	203
System Integration Testing (SIT) .....	203
User Acceptance Testing (UAT) .....	203
Production Records prior to installation .....	203
Data Migration During Transition.....	204
Data Migration Process .....	240
Data Migration Plan .....	241
System Integration Testing (SIT) .....	241
User Acceptance Testing (UAT) .....	241
Production Records prior to installation .....	242
Data Migration During Transition.....	242

<b>Attachment F: WV DMV Contract Privacy Policy .....</b>	<b>260</b>
<b>Attachment H: PII Acknowledgement .....</b>	<b>265</b>
<b>Addendum Acknowledgement Form .....</b>	<b>267</b>
<b>Exhibit A: Sample Training Plan .....</b>	<b>268</b>
<b>Exhibit B: Sample Test Documentation .....</b>	<b>302</b>
<b>Exhibit C: Sample Project Work Plan .....</b>	<b>337</b>

## Letter of Transmittal

July 2, 2018

Melissa Pettrey, Senior Buyer  
Department of Administration, Purchasing Division  
2019 Washington Street East  
Charleston, WV 25305-0130

**RE: RFP DMV1800000001**

**Dear Ms. Pettrey,**

On behalf of Veridos America, Inc. we are pleased to present our response to the West Virginia Division of Motor Vehicles (WVDMV), to **RFP DMV1800000001** Driver's License and ID Card.

Veridos understands the need of jurisdictions across North America to provide their citizens with the most secure credentials possible. We believe that together, we can implement a solution that increases both the security and customer experience of West Virginia's citizens while simultaneously offering cost savings to the WVDMV.

Veridos is currently providing similar solutions to jurisdictions in both the United States and Canada and we have identified a number of solutions within our proposal that would bring West Virginia's Driver's License and ID Card program ahead of the national curve. As part of the Giesecke + Devrient Group, Veridos offers the WVDMV over 160 years of experience providing secure documents and credentials. Our full range of identification products and solutions offer West Virginia a complete solution to all the requirements of this RFP.

We are happy to provide references who can speak to the quality of our solution, many of whom we have served for over a decade. It is this dedication to long-term quality, combined with innovation and customer focus that makes Veridos the ideal partner for the WVDMV.

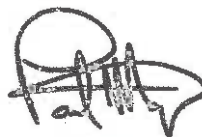
Upon contract award, Veridos requests an opportunity to discuss the Indemnification requirements on page 37 of the RFP. Veridos understands this provision but seeks an update on the potential cures offered by WV in Addendum 3 of the RFP.

We are confident that the Driver's License and Identity Card Solution contained within this proposal provides West Virginia with the most secure, cost effective central issuance solution.

Sincerely,



Kathleen Synstegaard  
Director, Sales USA

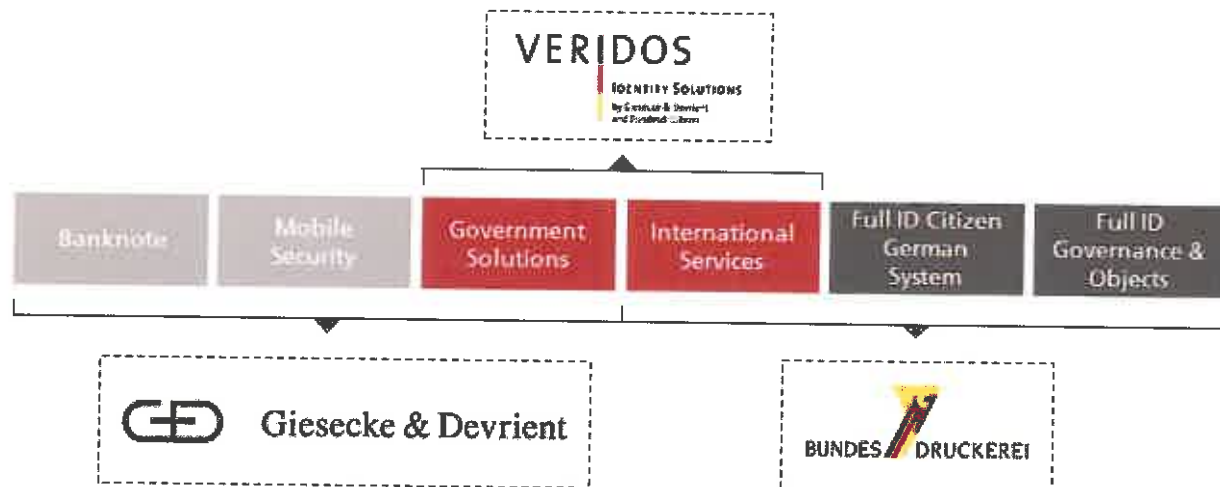


Paul Mazzeo  
President Veridos America, Inc.

## Attachment A: Vendor Response Sheet

Veridos America, Inc. is pleased to present our response to the West Virginia Division of Motor Vehicles (WVDMV), for RFP DMV1800000001 Driver's License and ID Card.

For many years the Government Solutions team of Giesecke & Devrient (G+D) has partnered with Bundesdruckerei to deliver class leading identity solutions. Veridos provides Government ID Solutions as a subsidiary of these two firms. Our unique history allows Veridos to be the only firm in the industry devoted exclusively to servicing the unique needs of Government clients. Together with our parent companies Veridos has successfully delivered more than 150 government ID projects encompassing hundreds of millions of Driver's Licenses ID cards and Passports.



Giesecke & Devrient (G+D) holds 60% ownership of Veridos and is an international supplier of banknotes, payment and smart cards, SIM cards and mobile / cloud solutions with a significant footprint in North America.

Bundesdruckerei holds 40% ownership of Veridos and is a class leader in secure identity systems including ePassports, Border Control Solutions and document verification services. Veridos is proud to build upon our parent firm's more than 25 years of success in the United States and more than 400 years combined experience in secure printing.

In the Americas Region, Veridos and our parent firm G+D have more than 1,300 employees in the United States, Canada and Mexico across eight (8) facilities including three (3) high volume production sites. Our Twinsburg, OH facility is our premier standards-compliant facility in the United States, producing secure government identification credentials for multiple jurisdictions.

We have read and understood the WVDMV's requirements contained within this RFP and are confident that our solution will facilitate West Virginia's transition to a full central issuance model securely, seamlessly, on-time and on-budget. If selected, Veridos offers the WVDMV our full commitment to providing the citizens of West Virginia with the most secure, durable and cost-effective documents. Through our continued investments into new and emerging technologies both in the United States and in our subsidiaries in 31 countries around the world, Veridos is an ideal partner for the State of West Virginia for the full term of this contract and beyond.

## Full End-to-end Solution

Veridos offers the West Virginia DMV a full end-to-end solution from image capture and enrollment, facial recognition and data management to central issuance card personalization and mailing. We will provide:

- A complete DL / ID card solution including highly-secure custom card designs
- Accurate manufacturing and printing the United States that includes secure tracking of all card stock
- Fully customizable, high-security, AAMVA-compliant card bodies created from extremely durable and secure substrate material. West Virginia's new cards are designed to be easily validated by law-enforcement and the private sector
- Secure temporary Driver's Licenses
- End-to-end system for driver's license / ID card issuance. In addition to providing fully installed image capture workstations in DMV offices, Veridos' software will assist operators to quickly enroll licensees and pass the request to our central issuance facility in Ohio for rapid card distribution
- Secure data transmission and reception in formats that will work with WVDMV's systems
- A proven operations and project management team that can meet your scheduling and planning needs
- Ultra-secure central issuance facility to ensure your information and product is always secure
- Exceptional, customized training to WVDMV's 'Train-the-Trainers'. Our customized training plan will include skills-based, hands-on modules created exclusively for the WVDMV by the OEM hardware manufacturers and Veridos' system architects.
- Best in class partnership and a total suite of professional services. Key to Veridos' success is our desire to be a long term partner to each of the jurisdictions we serve. Our comprehensive program management and extensive industry knowledge provide us the best ability to monitor, manage and track your solutions performance. From rapid service at DMV sites to regular meetings to demonstrate the latest trends and technology, Veridos will work tirelessly to ensure that our solutions provide West Virginia with the most secure programs available.

## Security of Central Issuance

Veridos' solution is designed to provide the WVDMV with both best in class security and world-class customer satisfaction. Veridos is the original manufacturer of the AAMVA and

Real-ID compliant cards proposed in this bid. These cards are constructed of a special blend of materials that have been extensively tested and qualified by Veridos and multiple independent laboratories. The card material cannot be obtained through any source other than Veridos. Each card will be marked with a Document Control Number at the time of manufacture and this number will be used to track the card through its entire life cycle including in the hands of the licensee.

From the moment of manufacture, through issuance and into the hands of the end-user, these card bodies will work with our Inventory Management System (IMS) to ensure total inventory control. As just one example of our unprecedented level of tracking options, the Datacard printers to be provided as part of our solution can be configured to scan the DCN from every card they print, automatically updating the systems to show when a specific card body has been issued. Combined with the custom security features unique to West Virginia, this level of inventory tracking and card material control will provide unrivalled resistance to fraud. With this level of security and control, WVDMV can provide a new level of security for federal Real-ID compliant cards issued from Veridos' high security facility.

## High Level Overview of Veridos' Solution



### Veridos' End-to-End Solution

- Fully installed workstations with all required hardware and software to produce and issue cards in minutes, or transmit request to Central Issuance facility
- Powerful Facial Recognition System with 1:1 and 1:N matching
- Online search and reporting capabilities
- Experienced Project Management and Delivery Team
- Proven Governance and Project Delivery Model.
- Local presence for rapid DMV maintenance
- Dedicated team for in field support and day-to-

### Secure Central Issuance for Federal ID Cards

- All card bodies for West Virginia will be printed at our high security facility in Twinsburg, Ohio
- Site certified by Visa, MasterCard, Discover and American Express
- Quality certification ISO 9001, 27001, 14001
- Total supply chain control and inventory management
- Fully customizable reporting allows for card tracking in real-time
- Secure fulfilment and mailing
- Encrypted and secure IT environments for file processing, testing and implementation.

### Card Design & Security

- Secure design from an expert Graphics team meeting all AAMVA standards
- State of the art, high quality card bodies designed to exceed West Virginia's longevity requirements
- Layered security features make cards extremely resistant to counterfeit and other attempts at fraud
- Ongoing redesign and card design security reviews
- Secure storage and shipping of card stock to DMV offices

## Veridos as a Partner

We recognize the challenge organizations face in balancing ways to reduce on-going costs and yet effectively process and deliver a highly secure Government identification card. Over the last several years, we have enabled our clients to overcome their challenges through our investments in technology, research and development, services, employees and strategic partnerships. We have extensive experience globally in helping government institutions reduce their total cost of ownership and provide a cutting edge secure solution. .

The Veridos vision is to provide superior business outsourcing services that enhance the long-term value and effectiveness of our clients. We realize this vision by employing a highly capable workforce and by providing our clients with superior quality services at a competitive cost. Our mission is to create, deliver and continuously improve our business services to help

transform and enhance our clients' business. Through our ongoing annual investments into research and development, Veridos is poised to offer exciting new products into the marketplace including advancements in Print on Demand offerings and I.D. verification services and new **mobile driver's license and identity card application** to allow WVDMV customers the chance to carry all of their secure credentials on their smartphone.

Our unique structure has enabled Veridos to grow substantially continue to deliver work for many high profile clients across North America. Our wider solutions portfolio includes the 80% of the Canadian secure payment card market, secure driver's licenses, AAA cards, national and local ID and health cards.

### **Secure Manufacturing in the United States**

We maintain PCI-CP certifications for manufacturing and personalizing Visa, MasterCard, Discover, and American Express cards, as well as ISO 9001, ISO 14001, ISO 18001, and ISO 27001. All cards manufactured by Veridos meet or exceed the International Standards Organization (ISO), International Card Manufacturers Association (ICMA), American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST), the ABA, and all major payment card manufacturing standards and specifications.

Veridos and our Parent firm G&D have more than 1,300 employees in the United States, Canada and Mexico across 8 facilities including 3 high volume production facilities. In North America, Veridos leverages all of G&D's facilities, to deliver class leading solutions.

Our North American footprint offers several advantages to the WVDMV, including:

- Cost savings from using Veridos' state of the art facility in Twinsburg, Ohio as the primary production and central issuance facility. The Twinsburg site is a key component of Veridos' North American footprint that is already established and fulfilling client orders.
- In the unlikely event of a natural disaster or disruption of service, Veridos has a secondary site located in Dulles Virginia to provide disaster recovery service.
- Both locations offer highly secure logical and physical environments. Having these sites in close geographical proximity to West Virginia means that the WVDMV is well positioned to rapidly implement any desired advances or updates as soon as they are available. This proximity also offers a reduction in lead-time for mailing and service.

### **Veridos' Experience**

Veridos (G+D) has implemented more than 150 government projects in the past 25 years.

Some of our larger implementations from the past decade include:

- Ontario Driver's License and Health Card, 2007 - Ongoing
- Manitoba Driver's License and ID Card, 2009 - Ongoing

- Saskatchewan Driver's License and ID Card, 2016 – Ongoing
- Oregon Driver's License and ID Card –  
Launching November 2018
- Ohio Driver's License and ID Card – Launching  
July 2018
- German EID, 2013 - Ongoing
- International Aero Transport Association, 2013 –  
Ongoing
- Austrian National Electronic Health Card,  
Residence Card, e-Passport chips, 2004 –  
Ongoing
- Brazilian Electronic ID Card, 2009 - 2012
- Bulgarian National ID & European Residence  
Card, 2009 - Ongoing
- Czech Republic European Residence Permit,  
2011 - Ongoing
- Dominican Republic Voter ID Card - 2007
- Macau Electronic ID Card, 2002 - 2008 and MWS upgrade, 2011 - 2012
- Macedonian New Identification Documents for Macedonia, 2005 - Ongoing
- Mexican Voters ID, July 2013 - Ongoing
- United Arab Emirates MIL ID, 2010 - Ongoing
- Austrian Passport - Supply of Chip Modules, 2006, 2010 - 2014
- Kosovo Travel Documents and Personalization System, 2000 - 2007, 2008 - 2011
- Botswana Passport, PP Production and Border Control System, 2008 - 2012
- Bhutanese Passports, 2005 - 2011
- Haiti Passport and Border Control System, 2002 - 2012
- Latvia Passports and Passport System, 2009 – 2012
- Turkmenistan National ID Documents, 2010 - 2012
- Madagascar Passports, 2005 - 2010
- Yemen Passports, 2004 - 2011
- Zambian Passports, 2006 – 2012



### **Ministry of Transportation of Ontario (MTO)**

Since 2007 Veridos has been the trusted partner of Canada's largest jurisdiction. When MTO first partnered with Veridos they required a complete end-to-end solution that started with photo-intake stations, full software for registration and photo investigation, data encryption and integration, manufacturing, printing and fulfillment of cards from a secure central issuance facility.



Within just 9 months Veridos was able to implement a full issuance solution for MTO with one of the most secure Driver's Licenses available anywhere in the world.

Today, the Veridos / MTO partnership continues to grow and includes the Ministry of Health (MoH). Veridos issues over 6.5 million cards per year on behalf of Ontario including over 300,000 Enhanced Driver's Licences and 3.5 million standard licenses.

#### **Highlights of the MTO program:**

- Design and security features for Ontario Driver License, Enhanced Driver License, Ontario Photo ID and Ontario Health Cards.
- Veridos provided all of the front-end capture systems and ongoing maintenance
- 1,100 sites were installed with new photo-capture equipment, scanners, and signature pads
- Manufacturing, personalization, fulfillment and mailing of all card types.
- Network connectivity and data hosting
- Delivery and Implementation, Project Management
- Delivered on time and to MTO's requirements

### **Manitoba Public Insurance (MPI)**

When Manitoba Public Insurance (MPI) first partnered with Veridos in 2008 they wanted to move to a more secure card body, with a range of security features and options that could be configured by industry experts to meet current and future regulatory and legislative requirements. Veridos provided the scope of services required by MPI, including card manufacturing, card personalization, card fulfillment, sourcing of card carriers, protective sleeves, activation labels, buckslips and envelopes for both the Province of Manitoba Driver License (regular and enhanced) and the Identification Card (regular and enhanced).



the Manitoba project involved full long-term account management, project management and delivery, design and manufacturing and fulfillment for Driver Licence and ID Cards. This large-scale project also included close partnership to ensure delivery of all standards, including AAMVA standards, and guarantee Enhanced DL's met border-control standards expected of identification at American/Canadian border checkpoints. This experience has proven the ability of Veridos' teams to provide:

- Secure card production services

- Design and Security Consultation for the Manitoba Driver License, Enhanced Driver License, Manitoba Identification and Enhanced Identification
- Enhanced DL design to be used for border crossing between Canada and the US (similar to a passport)
- Facial Recognition

#### **Saskatchewan Government Insurance (SGI)**

The latest Canadian jurisdiction to partner with Veridos was Saskatchewan Government Insurance (SGI) successfully launched their advanced Driver's Licence and ID card solution in April of 2016.

The solution included a Centralized Card Production and Mail Fulfillment Service, Image Capture Solution (camera, workstation, scanner and supporting software) and a full Facial Recognition System and data migration. The province's goal was to ensure that citizens of Saskatchewan could visit any of their nearly 400 geographically dispersed motor licensing issuing offices and have a seamless experience in the process while enhancing the technology used to reduce fraud and help safeguard the identities of its citizens.



Saskatchewan Government Insurance provides over 600,000 secure cards, a combination of DL and ID cards, annually or on average, 1,850 cards per day which are all manufactured and mailed from our central issuing facility in Markham, Ontario, Canada. The entire solution was implemented on-time and on-budget.

Veridos managed the installation, training, integration and support of all deliverables. Veridos also provides a depot maintenance program for all associated hardware and ongoing FRS system support. All periodic software updates are provided to the province as required on an ongoing basis subject to the agreed upon Software Maintenance for the length of the contract.

#### **Ohio Department of Public Safety / Bureau of Motor Vehicles (ODPS/BMV)**

The Ohio Department of Public Safety / Bureau of Motor Vehicles (ODPS/BMV) is transitioning from over-the-counter DL/ID card issuance to central issuance. Veridos is providing an image and signature capture solution, REAL-ID compliant polycarbonate card substrates and automated central issuance card personalization and mailing. Once launched in early 2018 Veridos will issue approximately 3.3 million cards annually for the State of Ohio.

#### **Relevant Process Improvements:**

- Capture solution for capturing ICAO/AAMVA-compliant images
- Signature capture solution for capturing signatures and applicant certifications
- Statewide installation and deployment services
  - 192 sites in one weekend
- Secure card production services
- Card quality assurance processes



- Automated mailing of credentials

## Partnerships for West Virginia DMV

For the West Virginia DL / ID solution, Veridos will engage in long-term partnerships to ensure that the WVDMV's new DL/ID program is a success. Both of our chosen subcontractors for this bid have proven themselves to be reliable and professional additions to the industry.

Entrust Datacard and Veridos have partnered for decades to deliver DL / ID solutions and Excel Management Systems has 28 years of experience providing IT and physical infrastructure support across the United States.

Veridos takes full responsibility for the performance of our subcontractors and has full confidence in their performance.

### Entrust Datacard

Veridos is working with Entrust Datacard to provide the front-end capture hardware, over-the-counter and central issuance card personalization and mailing systems for this bid. Veridos and Entrust Datacard have a proven track record of delivering solutions together. We have partnered to deliver projects across the globe including but not limited to the Ministry of Transportation of Ontario, Manitoba Driver License, Saskatchewan Government Insurance and we are working together to implement a successful driver license system for the State of Oregon. Over the past decade we have developed a tight partnership that will enable us to work together seamlessly to deliver the strongest possible solution for the WVDMV.

Entrust Datacard is a respected OEM solutions and hardware provider whose solutions are used in 6 Canadian Provinces and 15 U.S. States including West Virginia.

#### **EDC experience in Canada:**

- British Columbia
- Manitoba
- Ontario
- Quebec
- Saskatchewan
- Yukon

"Entrust Datacard is honored to be part of Veridos' team for this bid. Veridos is valued partner of Entrust Datacard's globally in both government identification and financial markets. Together, we have delivered several highly-successful and advanced government identification solutions around the world."

**Michael Berman,**

Entrust Datacard's General Manager and Vice President Americas Public Sector

#### **EDC experience in the United States:**

- |                 |                  |                 |
|-----------------|------------------|-----------------|
| • Alaska        | • Maryland       | • Washington    |
| • Colorado      | • New Hampshire  | • West Virginia |
| • Delaware      | • Ohio           | • Wyoming       |
| • Washington DC | • Oregon         |                 |
| • Hawaii        | • South Carolina |                 |
| • Idaho         | • South Dakota   |                 |

**Excel Management Systems Inc.**

EXCEL is a Veteran Owned, Minority Business Enterprise (MBE), incorporated in the State of Ohio by Mr. Curtis T. Jewell in 1989 with nearly Twenty (20) professionals on staff. The company has an excellent 27-year history, and outstanding past performance demonstrated in a variety of market sectors, including the Federal government, multiple state agencies, and commercial and non-profit organizations. EXCEL has established itself as a subject matter expert related to IT infrastructure and hardware maintenance as well as sound and proven processes that effectively enable the recruiting, vetting, training, and managing of subcontracted resources.

Excel has supported numerous national brands such as:

- Cash America
- Bob Evans Restaurants
- Donatos
- TBC Brands (Carroll Tire Company, Big O Tires, Tire Kingdom, Merchants Tire & Auto Centers, NTB, and Midas)

EXCEL will be responsible for the installation, maintenance and end-user training of project related hardware.

**References**

Below are our three (3) references that demonstrate our capabilities of implementing programs of a similar nature to WVDMV's. All three references have volumes of at least 400,000 cards per year and have been in production for at least three years. Our references clearly demonstrate our stability and capability of meeting WVMDV's card volumes.

<b>Jurisdiction Name:</b> Ministry of Transportation of Ontario (MTO)	<b>Reference Contact:</b> Ms. Heidi Francis Assistant Deputy Minister
<b>Project Name:</b> Ontario Driver's License and Health Card Program	1201 Wilson Ave. Downsview, Ontario, Canada +1 (416) 235-4453 Heidi.francis@ontario.ca
<b>Description of Project:</b>  The Ministry of Transportation of Ontario's (MTO) Driver Licence System had reached the end of its life as a secure solution and was no longer capable of meeting future security standards. They required a complete end-to-end solution that started with photo-intake stations, full software for registration and photo investigation, data encryption and integration, manufacturing, printing and fulfillment of cards from a secure central	

issuance facility.

MTO had been using a PVC card and most of their intake system equipment was out-of-date and in need of a full refresh from the ground up. They wanted to move to a more secure card body, with a range of security features and options that could be configured by industry experts to meet current and future regulatory and legislative requirements. The solution also needed to be scalable, to allow citizens and permanent residents to apply at a large and growing number of stations throughout the province.

The Ministry required a highly secure and durable driver licence card to protect the card data and ensure the validity of identification. Laser engraving technology was needed to personalize the photo, personal data and the bar codes on a polycarbonate based card to ensure compliance with security standards and allow for international ID standards to be met ongoing.

Finally, the Ministry had a very tight timeline. In less than 9 months from contract signing, they needed to implement a system that would enable everything mentioned above and start production for more than 3.5 million cards annually.

**Relevant Experience:**

- Design and security features for Ontario Driver License, Enhanced Driver License, Ontario Photo ID and Ontario Health Cards
- Together Veridos and EDC provided all of the front-end capture systems and ongoing maintenance
- 1,100 sites were installed with new photo-capture equipment, scanners, and signature pads
- Manufacturing, personalization and fulfillment of all card types.
- Network connectivity and data hosting
- Maintenance
- Delivery and Implementation, Project Management
- Delivered on time and to MTO's requirements

**Relevant Card Features:**

- Polycarbonate card body for Driver License and Enhanced Polycarbonate card body for Health Card
- Tactile laser engraved personalization data
- MLI/CLI lens / Ghost image
- Pre-printed serial numbers on card backs
- Microprint

- Black and White Laser Photo for Driver License, Color Photo for Health Card
- UV Print
- Data Encryption
- Chip Cards for Enhanced Driver License that prove Veridos' ability to provide EDL technology if WVDMV should ever wish to provide border crossing-enabled driver licenses.

**Relevant Experience From This Project:**

The Ontario DL and Health Card project involved full long-term account management, project management and delivery, design and manufacturing and fulfillment for both Driver Licenses and Health Cards. This large-scale North American project also included close partnership to ensure delivery of all standards, including AAMVA standards. Further, this project also involved setting up over 1,000 sites with photo-capture equipment. This experience has proven the ability of Veridos' Government Services teams to:

1. Provide manufacturing, personalization and fulfillment of high-grade governmental identification cards. Veridos' proposed plant for West Virginia has a capacity of 144 million cards annually and can well exceed the requirements of this RFP.
2. Provide Identification cards with advanced security features, designed to provide maximum counterfeit resistance to meet all governmental standards
3. Fulfillment and direct and indirect mailing of cards, working closely with postal services and couriers to ensure that the quality of cards remains intact through the shipping process
4. Provide ongoing consultation about relevant standards, including full AAMVA compliance, to ensure that all client's needs and security concerns are met
5. Security Infrastructure – Veridos planned and implemented the entire security infrastructure for this project, and the experience gained in this project will ensure the State of West Virginia's security is world class, provided by a team that has already proven its ability to deliver
6. Manage multiple internal and external stakeholders
7. Manage and deliver the installation of photo-capture equipment at widespread and geographically diverse locations.
8. Provide first-class project management for a large-scale project with a need for flexibility, to deliver different deliverables as government standards and systems change

**Project Dates:**

Project start: November 2007

Contract completion: November 2022

<b>Jurisdiction Name:</b>  Saskatchewan Government Insurance (SGI)	<b>Reference Contact:</b>  <b>Mr. Randy Stoneham</b>  Manager, Issuer and Customer Support Services  2260 11 <sup>th</sup> Avenue Regina, Saskatchewan, Canada  +1 (306) 751-3757  rstoneham@sgi.sk.ca
<b>Project Name:</b>  Saskatchewan Driver's License and I.D. Card Program / Facial Recognition Program	
<b>Description of Project:</b>  Veridos was chosen as the new vendor for SGI's (Saskatchewan Government Insurance) secure DL and ID card program. The solution included a Centralized Card Production and Mail Fulfillment Service, Image Capture Solution (camera, workstation, scanner and supporting software) and a full Facial Recognition System and data migration. The province's goal was to ensure that citizens of Saskatchewan could visit any of their nearly 400 geographically dispersed motor licensing issuing offices and have a seamless experience in the process while enhancing the technology used to reduce fraud and help safeguard the identities of its citizens.  Saskatchewan Government Insurance provides over 600,000 secure cards, a combination of DL and ID cards, annually or on average, 1,850 cards per day which are all manufactured and mailed from our central issuing facility in Markham, Ontario, Canada. The entire solution was implemented on-time and on-budget.  Veridos, together with our sub-contractor, Entrust DataCard managed the installation, training, integration and support of all deliverables. Entrust Datacard also provides a depot maintenance program for all associated hardware and ongoing FRS system support, 24 hours a day, 7 days per week. All periodic software updates are provided to the province as required on an ongoing basis subject to the agreed upon Software Maintenance for the length of the contract.	
<b>Relevant Experience:</b> <ul style="list-style-type: none"> <li>• Provide front-end capture systems and ongoing maintenance requirements to nearly 400 motor licensing offices throughout the province – many in rural areas.</li> <li>• Provide full F.R. solution to reduce fraudulent activity</li> <li>• Worked very closely with their design team to introduce a new, highly secure identification document while not altering the current design</li> </ul>	

- Manufacturing, personalization and fulfillment of all card types.
- Full network connectivity and support
- Maintenance
- Delivery and Implementation, Project Management
- Project delivered on-time and within the province's budget

**Relevant Card Features:**

- Polycarbonate card body for Driver License and I.D. Card
- Tactile laser engraved personalization data
- MLI/CLI lens / Ghost image
- Pre-printed serial numbers on card backs
- Microprint
- Black and White Laser Photo for Driver License, Color Photo for Health Card
- UV Print
- Data Encryption

**Relevant Experience From This Project:**

SGL's Driver's License and I.D. Card Project involved full long-term account management, project management and delivery, design, manufacturing and fulfillment for both Driver Licenses and Identification Cards.

Similar to the State of West Virginia, SGL's expectation from Veridos was that the transition from their incumbent would be as seamless as possible. As Veridos was responsible for a single procurement that included provisioning all necessary hardware, software, design, development, customization, installation, training, personnel, supplies and ongoing maintenance. Daily card production volume was estimated at approximately 1,850 cards per day being issued at almost 400 issuing locations across the province; many in rural locations. The implementation of card production, including front-end hardware transition/set up was to be completed as part of Phase 1 with the facial recognition portion being implemented within a 6 month period following successful operation of card production activities.

Our project management team developed and worked with SGL on a concise plan of action that outlined start and end dates for each portion of the project including a collaborative approach to card design portion, change control and any risk mitigation that might impact the extremely aggressive timeline. All issuing offices were outfitted with new equipment and a training plan was created and executed. Card production was transitioned – with superior security features on base card and significantly increased photo quality output on time and on budget.

Following successful implementation, Phase 2 of the project was initiated and included

the full rollout of a new Facial Recognition System which had a target launch date of 180 days. A complete system design including custom solution architecture, workflows and development was created. Customizable reporting was put into place and full system testing and integration was completed; over 375,000 legacy images were then migrated. The solution deployment to all environments was implemented once training was executed and the project was successfully deployed on time.

At project completion, a series of post-mortem calls were held with the key stakeholders at both SGI, Veridos and its sub-contractors to review project flow and continuing communication plan.

Today, SGI is successfully in production with one of the most secure DL and ID cards across Canada hosting a robust front-end capture solution that incorporates FR providing its citizens with technology that both reduces fraud and helps safeguard their identities.

**Project Dates:**

Project launch: May 2015 Contract completion: May 2025

<b>Jurisdiction Name:</b>	<b>Reference Contact:</b>
Manitoba Public Insurance (MPI)	<b>Mr. Brad Bunko</b>
<b>Project Name:</b>	Vice President – Information Technology
Manitoba Driver's License and I.D. Card Program	912-234 Donald Street
	Winnipeg, Manitoba, Canada
	+1 (204) 985-8770 ext. 7481
	bbunko@mpi.mb.ca
<b>Description of Project:</b>	
<p>The Manitoba Public Insurance's (MPI) Driver Licence System required a much needed refresh as the existing DL was not capable of meeting future security standards. They required a brand new DL and ID card incorporating laser engraving on a polycarbonate substrate. The contract would require manufacturing, printing and fulfillment of cards from a secure central issuance facility.</p> <p>MPI had been using a PVC card. They wanted to move to a more secure card body, with a range of security features and options that could be configured by industry experts to meet current and future regulatory and legislative requirements. Veridos provided the scope of services required by MPI, including card manufacturing, card personalization, card fulfillment, sourcing of card carriers, protective sleeves, activation labels, buckslips and envelopes for both the Province of Manitoba Driver License (regular and enhanced) and the Identification Card (regular and enhanced).</p>	



**Relevant Experience:**

- Secure card production services
- All steps, from manufacturing to mailing services
- Provide consultation and partnership to provide "ground up" design and development of a cutting-edge program
- Design and Security Consultation for the Manitoba Driver License, Enhanced Driver License, Manitoba Identification and Enhanced Identification cards for non-drivers
- Enhanced DL design to be used for border crossing between Canada and the US (similar to a passport)
- Facial Recognition
- Ongoing consultation and guidance on national and international standards and security
- Maintenance
- Delivery and Implementation, Project Management
- Delivered on time and on budget

**Relevant Card Features:**

- Polycarbonate card body for Driver License and I.D. Card
- Tactile laser engraved personalization data
- MLI/CLI lens / Ghost image
- Pre-printed serial numbers on card backs
- Microprint
- Black and White Laser Photo for Driver License, Color Photo for Health Card
- UV Print
- Data Encryption
- Chip cards for Enhanced Driver's License

**Relevant Experience From This Project:**

As with West Virginia's project, the Manitoba project involved full long-term account management, project management and delivery, design and manufacturing and fulfillment for Driver License and ID Cards. This large-scale North American project also included close partnership to ensure delivery of all standards, including AAMVA standards, and guarantee Enhanced DL's met border-control standards expected of identification at American/Canadian border checkpoints. This experience has proven the ability of Veridos' teams to:

- Manage multiple internal and external stakeholders
- Provide first-class project management for a large-scale project with a need for flexibility, to deliver different deliverables as government standards and systems change
- Provide ongoing consultation about relevant standards, from AAMVA to Real ID, to ensure that all client's needs and security concerns are met
- Work closely with postal services and couriers to ensure that the quality of cards remains intact through the shipping process
- Long-Term Account Management – in the words of the Manitoba Public Insurance, *"[Veridos] has become a valued and trusted business partner... We are very pleased with the working relationship we have developed with Veridos and look forward to continuing to work with the company well into the future."*
- Veridos will provide this same level of ongoing support and true partnership to the State of West Virginia, ensuring that its project is a success over the entire course of the contract.

**Project Dates:**

Project start: 2009

Contract completion: 2024

**Staffing Plan**

Our proposed Work / Project Manager for WVDMMV is **Anastasia Koulis**.

Anastasia has 25 years of experience in delivering highly secure solutions in both the financial and government solutions industries. Anastasia has been a regular, fulltime employee with Veridos and our parent firm G+D since 2014.

Anastasia will function as the Lead Project Manager and is responsible for the successful delivery of the project, coordination of WVDMMV activities, Veridos and third party resources as well as ongoing communication and strategy.

Anastasia has recently implemented several large projects of a similar scope and size to the requirements of this RFP.

Brief summaries of Anastasia's recent projects are highlighted below.

Project Reference #1	
Company Name:	Saskatchewan Government Insurance

Company Address:	2260 11 <sup>th</sup> Avenue, Regina, Saskatchewan, S4P 0J9
Contact Name:	Randy Stoneham, - Manager, Issuer and Customer Support Services.
Contact Telephone Number:	306-751-3757
Contact Email:	Rstoneham@sgi.sk.ca
Date Work Undertaken:	April 2016
Nature of Assignment:	<ul style="list-style-type: none"> <li>• Large scale project to introduce a brand new Driver's License and Identification card &amp; Capture Manager system by a specific set launch date, as well as a Facial Recognition System</li> <li>• High level of complexity involved to manage deliverables from numerous partners, and work streams, multi-phased approach, extensive documentation and testing</li> <li>• Duration of the project was 16 months – May 2015-Aug 2016</li> </ul>

Project Reference #2	
Company Name:	Manitoba Public Insurance
Company Address:	912-234 Donald Street, PO Box 6300, Winnipeg, Manitoba
Contact Name:	Brad Bunko - Vice President; Information Technology
Contact Telephone Number:	204-985-8770 EXT 7481
Contact Email:	bbunko@mpi.mb.ca
Date Work Undertaken:	Current – May 2017
Nature of Assignment:	<ul style="list-style-type: none"> <li>• Large scale project to in upgrade a Capture Management system and launch a Facial Recognition System</li> <li>• High level of complexity involved to manage deliverables from numerous partners, documentation and testing</li> <li>• Duration of project was 15 months – May 2015 – Aug 2016</li> </ul>

Veridos will utilize our established Staff Management process for this project. This process, described at high-level below, ensures that we have the best in class personnel available through the entire life of the project and that their work load is fully managed. The core of

When new staff joins the project, the Lead Project Manager provides an orientation to the project. The orientation discusses the following topics:

- Background of the Project
- Current Status of the Project
- Specific Job Duties and Expectations
- Introduction to the Staff and Consultants
- Overview of the Facility and Infrastructure
- Overview of the Project Processes, including time reporting, attendance, and status meetings
- Review of Confidentiality and Conflict of Interest
- The project manager then reviews with staff their current job skills and discusses mandatory or desired training with the staff. Typical types of training which may be required or of use to staff include:
  - Introduction to Project Management Principles
  - Introduction to the Project's own internal website (ex: company wiki, SharePoint)
  - Introduction to Project Business Tools

#### **Transition to Other Projects/Organizations**

In the event staff desire to transition to another project prior to the completion of the project, the staff functional manager will assume or re-assign the departing staff responsibilities.

The staff functional manager is responsible for ensuring any pending work is transferred to a remaining staff member to ensure timely transition and completion of the work. If appropriate, the receiving staff may request additional training to support the new responsibilities. At a minimum, job shadowing is performed for at least one week before staff transition off the project.

#### **Replacement of Staff**

Staff vacancies are addressed through the normal hiring process. The project office works with the Human Resources to advertise positions and perform interviews. Staff may also be replaced by redirecting resources from within or outside of the project, or their workload may be absorbed by other staff.

#### **Pre-employment Screening**

All prospective Veridos employees are subject to pre-employment screening including full time, part time, temporary employees, contractors, consultants, interns and summer students.

We conduct criminal background checks for all States where a potential employee has resided, i.e. for our Twinsburg, Ohio facility. We therefore conduct fingerprint checks from the FBI through the State of Ohio Law Enforcement Agency, Bureau of Criminal Identification (BCI).

In addition, we conduct anti-terrorist, driving and credit record checks, and conduct drug testing as part of the employee security screening process. We also conduct checks and verifications on all former employments and any claimed education attendance and/or graduations.

Security Screening is also performed annually on all current employees. Evidence of Screening is maintained on file during an employee's tenure and for two years after termination; it is available for onsite audits whenever required.

The key personnel on Veridos' proposed project team is provided below.

Key Person	Position	Responsibilities
<b>Anastasia Koulis</b>	Project Manager	Lead Project Manager, responsible for the successful delivery of the project, coordination of West Virginia and Veridos team resources, and ongoing communication and strategy
<b>Keith Liang</b>	Program Manager	Program Manager responsible for overall management and delivery of the proposed system and ensuring that all technical and administrative requirements are met in conformance with the project schedule and contract requirements
<b>Irina Lissok</b>	Senior Manager, Information Technology	Responsible for Production Programming Development, Secure Data Transmission and IT infrastructure
<b>Russell Walsh</b>	Director of Card Production  31 years at G+D	Operational responsibility for card design and production
<b>Cindy Peters</b>	Customer Relationship Manager	Responsible for day to day activities within the account
<b>Paul Mazzeo</b>	President, Veridos America  30 years at G+D/Veridos	Key point of escalation and ongoing consultation expertise, project sponsor responsible for governance and accountability
<b>Kathleen Synstegaard</b>	Sales Director  20+ years in	Overall responsibility of account

	industry	
<b>Tom Kelly</b>	Director, Business Development  30+ years in Industry	Key point of planning for ongoing security consultation and industry expertise
<b>Ian Astbury</b>	Director of Solutions Development, Americas	Manages the engineering team responsible for software development, configuration and server deployment
<b>Gary Keller</b>	Solution Architect	Architect of overall Capture Manager
<b>Jim Elder</b>	Training Program Manager	Leads and directs the development and execution of a full training plan, ensuring all front and back end users are fully trained
<b>Seth Stearns</b>	Chief Operations Officer, Excel Management	Responsible for statewide installation, training and ongoing on-call maintenance of capture solution
<b>Thomas Lynch</b>	Team Lead /Project Lead	Responsible for Site Surveys, Installation, Maintenance
<b>John Lawrence</b>	Team Lead	Responsible for Site Surveys, Installation, Maintenance
<b>Ryan Scholes</b>	Team Lead	Responsible for Site Surveys, Installation, Maintenance
<b>Alex Holtzclaw</b>	Field Tech	Responsible for Site Surveys, Installation, Maintenance
<b>Dave Ward</b>	Field Tech	Responsible for Site Surveys, Installation, Maintenance
<b>Dan Rasmussen</b>	Field Tech	Responsible for Site Surveys, Installation, Maintenance
<b>Lori Porchart</b>	Project Coordinator	Responsible for Site Surveys, Installation, Maintenance

---

## Central Issuance

### Section 4, Subsection 4.1 - REAL ID Compliance Objectives

**Section 4, Subsection 4.1.1** - Vendor should describe what specifications they would propose to address the REAL ID Act of 2005 standards, and how their solution will meet the initial "Photo First" requirements providing compliance with those standards. The Agency is requesting an in-depth description of how this can be handled in "real time", which should consist of a detailed system diagram illustrating server (physical/virtual) locations and on-site equipment at each Agency location.

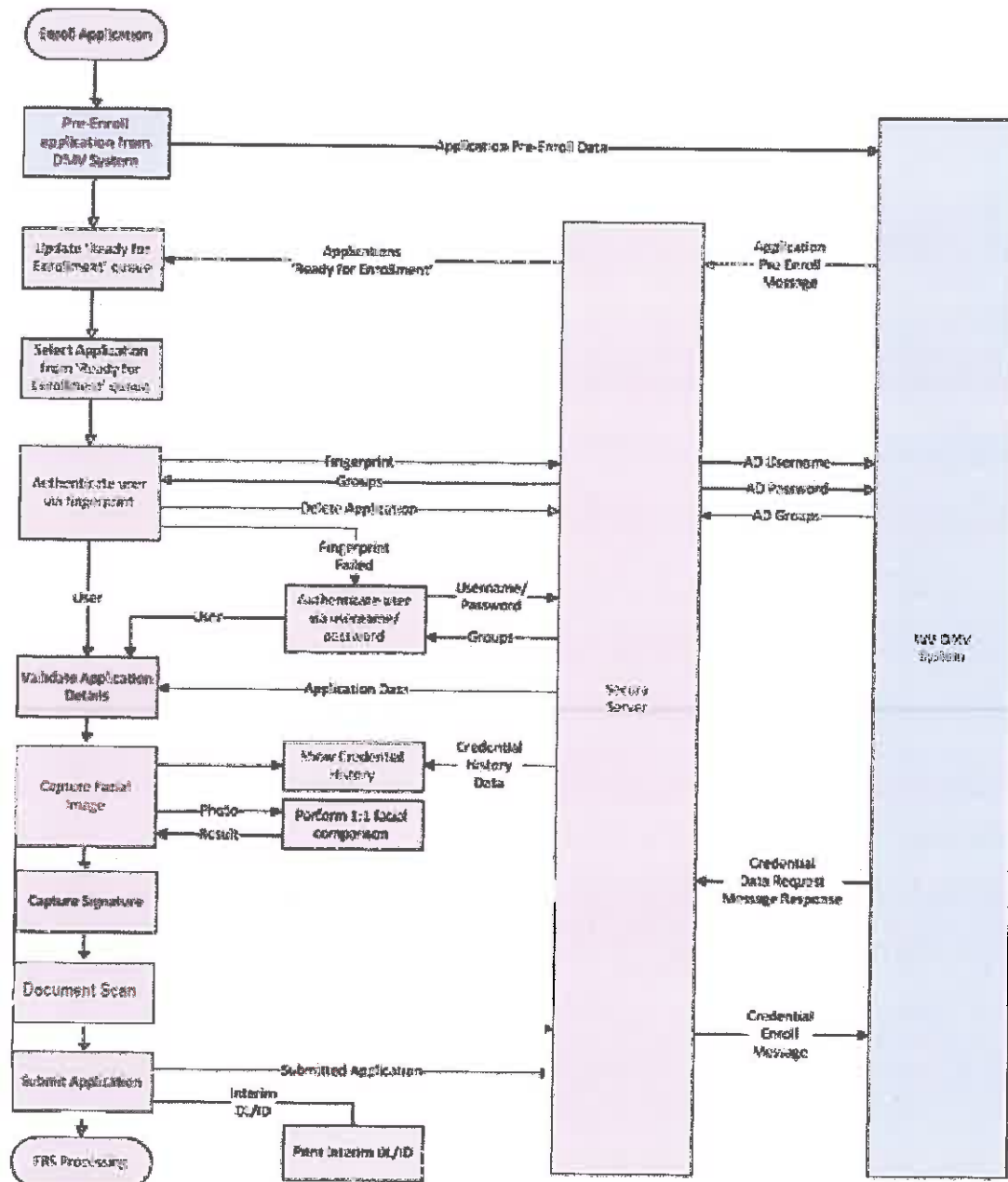
#### Vendor Response:

Taking the photo at the beginning of the enrollment process provides a visual record of the customer, even if they decide to discontinue the process later. This can be helpful when investigating fraudulent activities because individuals may decide to depart the facility if they feel they are arousing suspicion before completing the entire process. This process does not involve redundant steps or multiple cameras.

A general overview of the process is:

1. The operator enters or selects the applicant name and data of birth (new record or request from state system)
2. The operator captures the applicant photo
3. The operator completes the applicant enrollment and saves the completed record to the Secura database ("Enrolled")
  - a. Demographic data
  - b. Signature
  - c. Documents
  - d. 1:1 FRS Check

If the application process is not complete, the data collected, including photo and signature, is saved and is available for investigators.



**Section 4, Subsection 4.1.2** - Vendor should describe any available alert and notification mechanisms within their system, to "flag" image comparison and document authentication issues associated with the image captured during the "Photo First" process, in relation to the image currently on file (One-to-One, or One-to-Many, comparisons). This is intended for the purposes of reducing, or eliminating, the potential for identity fraud. This would generate a notification to the Agency's Investigation, Security and Support Services Unit ("IS&S"), identifying a potential security risk.

**Vendor Response:**

Our proposed solution complies.

The proposed facial recognition (FR) solution is the FaceVACS-DBScan solution from Cognitec. We use the Cognitec solution because it is the best in the industry. Cognitec's research and development specific to FR technologies has been in-use for government programs for over 20 years.

The 1:1 FR solution will be used during the image capture process. The 1:N FR solution will be used in near real time. There is an option available to authorized users with correct permissions assigned in Active Directory that allows a print request to by-pass the facial recognition checks for specialty card requests.

The system can notify the operator on screen prompts or popup dialogs. The exact method and business rules around it and use will be determined during the project design phase in collaborative meetings with the State and Veridos. The proposed solution can also print disguising marks on the temporary ID\DL if any of the checks fails.

Any records that fail checks are automatically routed to the adjudication or special handling queues for further scrutiny before they are sent to the bureau for production.

The screenshot displays the 'Enroll New Applicant' window. At the top, a progress bar shows four steps: 1. Application, 2. Signature, 3. Photo, and 4. Review. The 'Photo' step is currently active. Below the progress bar, the 'Capture Facial Image' section contains a 'Take Photo' button and a 'Credential History' button. Underneath, there are two columns: 'New Photograph' and 'On File Photograph'. The 'New Photograph' column shows a photo of a man with dark hair, labeled 'ICAO Compliant'. The 'On File Photograph' column shows a photo of a man with a shaved head. To the right of these photos, the 'Attributes' section displays a red error message: '1:1 Match Status: FAILED'. Below this message is a checkbox labeled 'Submit this application anyway', which is currently unchecked. At the bottom of the window, there are three buttons: 'Previous', 'Next', and 'Cancel'.

All records sent for card production will be run through a pre-production readiness check. The pre-production readiness check includes:

- Check each record and do not perform the 1:N check if the 'Confidential' flag is set
- Run the 1:N as each record is processed
- Set a potential match flag on any records identified by the facial recognition check to have issues sent for investigation
- Add confidential records back into the batch of records for production that do not require any investigation
- All records ready for production are sent to the card production bureau
- A report of all the records needing investigation is sent to the appropriate personnel

Once a suspect match is found, a case is created and the investigator uses the Examiner Module to adjust the case appropriately. State investigators can then use the tools provided with the Examiner Module to identify individuals from images captured. This includes not only the images captured with the Secura system, but also those that provided in special cases from crime scene photos, videos stills and sketches. All of these images can be used as a source probe image to determine if there are any matching facial images within the agency's image repository.

The Examiner Module toolset can enhance images for better comparison to the gallery. For example, image processing filters can improve the quality of images retrieved from low quality video footage. The pose correction filter uses 3D modeling technology to generate frontal views of faces taken under lateral angles. Examiner also provides a set of inspection tools that help identify the person by comparing images side by side or by measuring facial features.

#### Examiner: Side-by-Side Inspection



#### Examiner: Pose Correction



Operators can develop watch lists of potential matches while recording a full audit trail for each step in the process. Finding a suspect in a timely manner allows investigators to act upon the search results in the critical time period after a crime has been committed. All of these tools provide the State of West Virginia with a robust and comprehensive investigative solution.

---

#### Section 4, Subsection 4.2 - Central Issuance Facility Objective

Section 4, Subsection 4.2.1 - Vendor should describe a secure method allowing mobile device notifications for 'FOR FEDERAL' applicants, detailing the status of their credential from application to receipt.

---

#### Vendor Response:

Our proposed solution complies.

Our Central Issuance Facility includes an online portal, Engage, that tracks production status from application to receipt. All online services are accessible via the Veridos Online Portal web interface. The various applications provided to WVDMV allow authorized users on your staff to access the application simultaneously and query information 24 / 7. Veridos will provide an interface to this portal that provides a secure method allowing mobile device notifications for "FOR FEDERAL" applicants, detailing status of their credential from application to receipt.

Veridos' Online Portal enables WVDMV a self-service capability to query the processing status of individual personalization card orders, as well as to designate specific actions (redirect, pull, hold) for in-process card personalization. The Portal and Status Enquiry application are easily adapted for WVDMV's specific needs and offer 24/7/365 access to production status.

#### Status Enquiry Application

The *Status Enquiry* application provides reports regarding the date that a card request has been received or has been shipped in addition to DL/ID cards specific demographic

information such as: address, DL/ID card number, data received, batch ID, date shipped, mailing method of shipment.

The following objectives can be achieved by WVDMV by using this application:

- **Search Cards:** User can search for a card by configurable keys, i.e. DL/ID number (or other parameters)
- **View Card Details:** User can view the details of a card request
- **Select Cards for Pull:** User can select a card or more than one card to submit a pull request.



Veridos offers a mobile DL/ID application that can be coupled with this requirement to provide a richer citizen experience.

**My Identity Application (MIA)** offers West Virginia licensees with the ability to store all of their credentials securely on the cardholder's smartphone.

Not only does this offer West Virginia's citizens a convenient way to access and carry their DL / ID cards, but MIA contains significant security enhancements for both citizens and the WVDMV.

#### Benefits for Licensees:

My Identity Application only transfers the user approved, requested attributes, thus keeping the other attributes secure (although requests by law enforcement can be treated differently).

For example, for admission to an age-restricted event MIA only presents a picture (for identification) and that the person is older than the required age – it is not even necessary to display their birth date.

Access to the application can be protected by biometric, facial recognition or PIN code. Therefore even if the device is lost, access to the license is secure.

#### Benefits for WVDMV:

- Can reduce reliance on non-secure paper based temporary licenses.
- Integration of governmental (or law enforcement) ID databases
- Existing (digital) device infrastructure of law enforcement agencies (e.g. PCs, smartphones, tablets) can easily be integrated in the MIA application system
- Due to the highly modular structure of MIA, future changes can be rolled out easily and will be provided to the user via simple app updates

- Because of MIA's modular architecture, security protocols can easily be updated or new protocols can easily be integrated

The MIA.app is authenticated by the MIA.backend via client certificates, which are stored on the users' smartphone. The certificate is stored in a secure way by using state of the art security technologies offered by mobile operating systems such as the keychain (iOS) or keystore (Android).

All data transfers between the central MIA.backend and the MIA app are secured using Transport Layer Security (TLS). Due to the fact, that My Identity Application uses open and established standards, it is ensured that all security protocols are very well tested and therefore can be verified by independent security experts (e.g. in case of security audits).

No data are stored on the smartphone. Personal data is never transmitted directly between smartphones but is always queried from the connected data sources. Every data request must be approved by the person to whom the information belongs.

---

Section 4, Subsection 4.2.2 - Vendor should describe a method for electronic notification to the Agency which proves that the applicant has accepted delivery of the 'FOR FEDERAL' Driver's License or ID. Vendor should describe this process, including all security measures to be implemented.

---

---

#### Vendor Response:

Our proposed solution complies.

Our Central Issuance Facility includes an online portal, Engage, that tracks production status from application to receipt. All online services are accessible via the Veridos Online Portal web interface. The various applications provided to WVDMV allow authorized users on your staff to access the application simultaneously and query information 24 / 7. Veridos will provide an interface to this portal that provides a secure method allowing mobile device notifications for "FOR FEDERAL" applicants, detailing status of their credential from application to receipt.

Veridos offers a mobile DL/ID application that can be coupled with this requirement to provide a richer citizen experience.

**My Identity Application (MIA)** offers West Virginia licensees with the ability to store all of their credentials securely on the cardholder's smartphone.

Not only does this offer West Virginia's citizens a convenient way to access and carry their DL / ID cards, but MIA contains significant security enhancements for both citizens and the WVDMV.

**Benefits for Licensees:**

My Identity Application only transfers the user approved, requested attributes, thus keeping the other attributes secure (although requests by law enforcement can be treated differently).

For example, for admission to an age-restricted event MIA only presents a picture (for identification) and that the person is older than the required age – it is not even necessary to display their birth date.

Access to the application can be protected by biometric, facial recognition or PIN code. Therefore even if the device is lost, access to the license is secure.

**Benefits for WDMV:**

- Can reduce reliance on non-secure paper based temporary licenses.
- Integration of governmental (or law enforcement) ID databases
- Existing (digital) device infrastructure of law enforcement agencies (e.g. PCs, smartphones, tablets) can easily be integrated in the MIA application system
- Due to the highly modular structure of MIA, future changes can be rolled out easily and will be provided to the user via simple app updates
- Because of MIA's modular architecture, security protocols can easily be updated or new protocols can easily be integrated

The MIA.app is authenticated by the MIA.backend via client certificates, which are stored on the users' smartphone. The certificate is stored in a secure way by using state of the art security technologies offered by mobile operating systems such as the keychain (iOS) or keystore (Android).

All data transfers between the central MIA.backend and the MIA app are secured using Transport Layer Security (TLS). Due to the fact, that My Identity Application uses open and established standards, it is ensured that all security protocols are very well tested and therefore can be verified by independent security experts (e.g. in case of security audits).

No data are stored on the smartphone. Personal data is never transmitted directly between smartphones but is always queried from the connected data sources. Every data request must be approved by the person to whom the information belongs.

---

**Section 4, Subsection 4.2.3 – Vendor should describe the process for Agency designated personnel to inspect the central issuance facilities during the life of the contract.**

---

**Vendor Response:**

Our proposed solution complies.

Veridos' high-security facility in Twinsburg, Ohio is owned by Veridos' parent firm Giesecke & Devrient. Veridos and G+D are the only tenants.

The facility in Twinsburg is staffed and will be operated by our personnel. At no time will staffing be contracted to any outside parties.

Since Twinsburg is a short drive away, WVDMMV is always welcome to audit and review the facility; however, due to PCI, Mastercard and Visa compliance and certification regulations, we must note the following exceptions:

- A minimum of 24 hours advance notice must be provided prior to any site visit.
- All visitors must present valid government issued ID and be accompanied by a Veridos or G+D employee as an escort.
- No laptops or cellular devices will be permitted in the production area.
- Access to High Security Areas required 48 hours minimum notice. This is in keeping with both Veridos' internal security policies as well as our industry certifications.
- Visitor registration is completed through the Visitor Management System. The system will electronically capture the visitor name, signature, photo, visitor badge number, time and date of entry, time and date of departure, organization the visitor is representing and name of escort. Visitor registration will also include a biometric registration scan for access to select areas of the facility.

All audit control logs are kept for a minimum of 24 months.

---

#### **Section 4, Subsection 4.3 - Card Images**

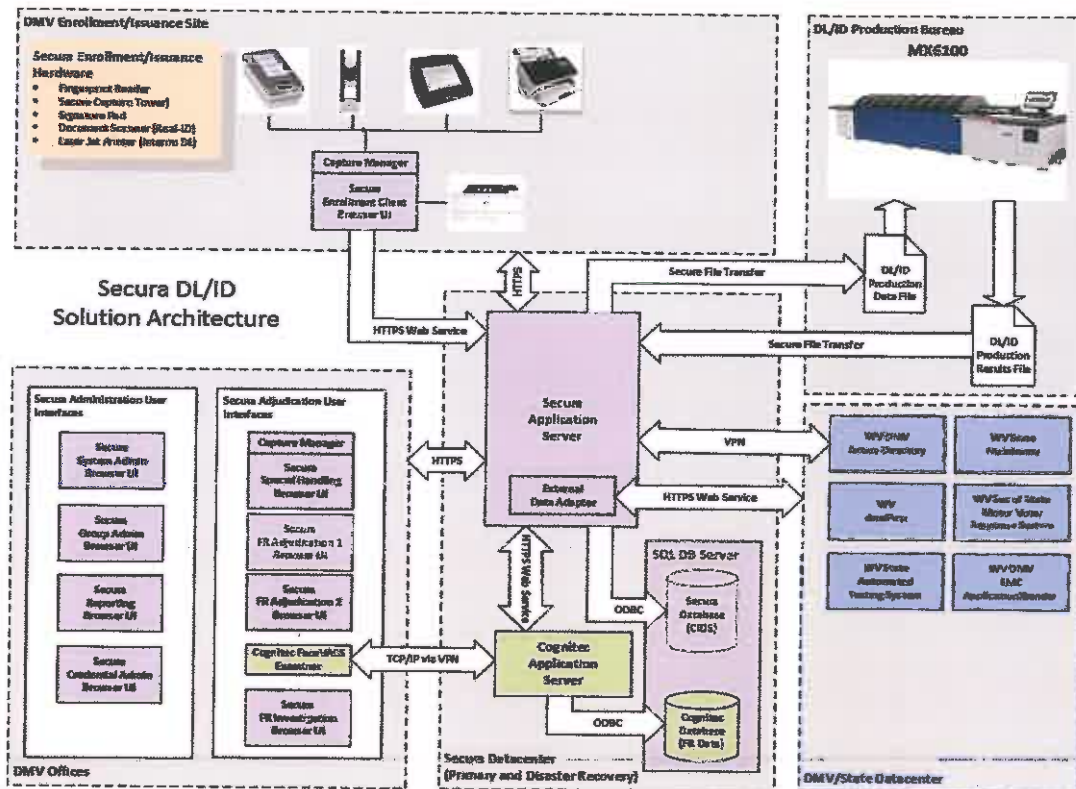
**Section 4, Subsection 4.3.1 - Vendor should describe how cards printed at the secure central issuance facility will be imaged (front and back) after printing and before being attached to the card carrier. Card images should be stored as JPG files as part of the credential issuance system (CIS), and should be retrievable as part of the customer's central issuance record.**

---

#### **Vendor Response:**

Our proposed solution complies.

During card production, the Quality Assurance Module of the MX6100 Card Personalization System captures a picture of the front and back of each card produced by the system. The images for each card will be returned to the WVDMMV via the sFTP servers. These images will be picked up from the sFTP servers and stored in the WVDMMV image repository with a pointer to the correct individual and production request. The images of the front and back of the card can then be accessed by other WVDMMV systems via the web service interface provided by our solution as noted in the diagram below.



#### Section 4, Subsection 4.4 - Card Design.

Section 4, Subsection 4.4.1 - While the specific designs for each card type will be determined during the planning phase after contract award. The Vendor should propose a solution for the FOR FEDERAL Driver's License and a FOR FEDERAL Identification Card for evaluation, based on 2016 AAMVA DL/ID Card Design Standard

(<http://www.aamva.org/2016CardDesignStandard/>) and West Virginia Code § Chapter 17B Motor Vehicle Driver's License (<http://www.legis.state.wv.us/wvcode/Code.cfm?chap=17b&art=1>)

#### Vendor Response:

Our proposed solution complies.

Veridos has prepared a total Real ID-compliant solution for WVDNMV. The total solution package being offered to West Virginia is designed to prevent tampering and counterfeiting. Our cards feature advanced security and production measures designed

to assist law enforcement use the cards during field operations while simultaneously providing attractive, long lasting cards to the citizens of West Virginia.

The proposed Driver's License is constructed of Polyester Enhanced Polycarbonate (PEC) that has been extensively tested and qualified by Veridos and third party laboratories. The card body is constructed of multiple layers, which include transparent and opaque materials which are a Veridos trade-secret and are not commercially available. Once assembled, the materials are laminated together under specific heat and pressure (without any adhesive or thermoplastics) to form a consistent card body which **cannot be delayered** as is possible using other substrates.

#### Card Overview

<b>Material:</b>	Polyester Enhanced Polycarbonate (PEC)
<b>Service Life:</b>	8 years of usage
<b>Dimensions:</b>	85.60 mm x 53.98 mm x 0.76 mm (nominal)
<b>ISO/IEC Spec:</b>	7810:2003 (Card Body)
<b>Color Photo:</b>	Thermal dye diffusion printing
<b>Data Elements:</b>	Laser Engraving



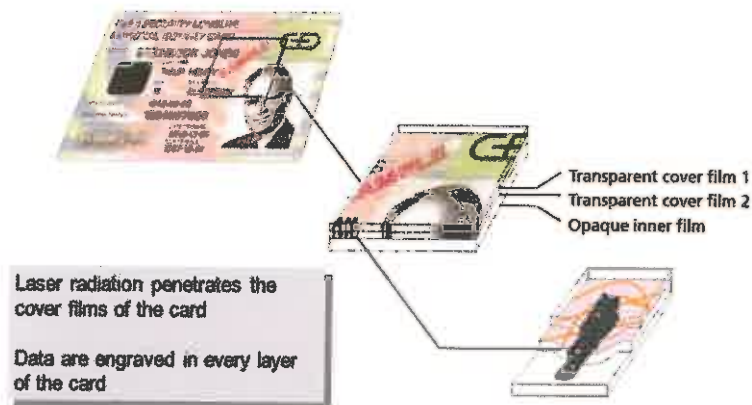
#### Benefits of Polyester Enhanced Polycarbonate (PEC)

- Durable PEC card body
- Color photo using thermal dye diffusion printing (D2T2)
- Laser engraving for secure data application
- Offers superior value at cost effective price
- Offers outstanding durability

- Similar technology to what is used in passports and National ID card programs
- Environmentally friendly material
- Protection against photo substitution
- Protection against counterfeits including types A1, A2, B1, and B2





Laser engraving means that all textual data is engraved 'into' the card body, where it cannot be altered. Laser engraving produces visual effects or images on cards that are permanent and highly secure. Multi-layer cards are laser engraved by passing a laser beam through the top clear layer of a card and focusing on a transparent laser receptive layer. It is here where the pigments react and form a black image as the layers react with each other. This process is often referred to as carbonizing. Additional energy is created with additional engraving time to create darker images and with sufficient energy; a tactile or raised image.

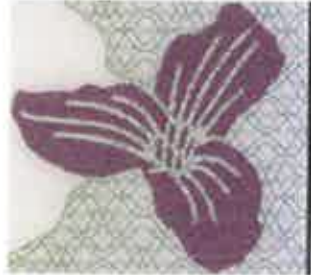
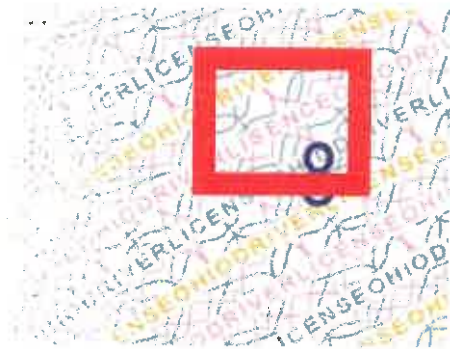
Cards will be laser engraved on both sides using an internal turning device, and multiple lasers can be used in sequence to laser engrave several cards at once to increase card throughput. Laser image quality is controlled by the internal software of the Datacard MX6100 card issuance systems. Card setups can control the type of laser engraving, the resolution (which can exceed 500 dpi), and the length of time the laser beam engraves a given area or pixel. Highly sensitive and accurate optical sensors control registration. Precise optics and mirrors ensure the accurate placement of laser engraved images.

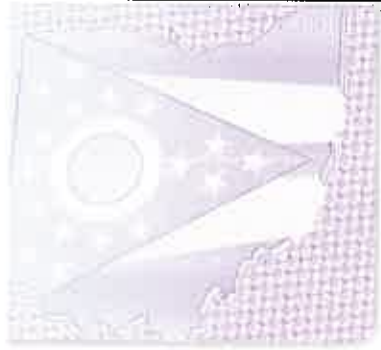





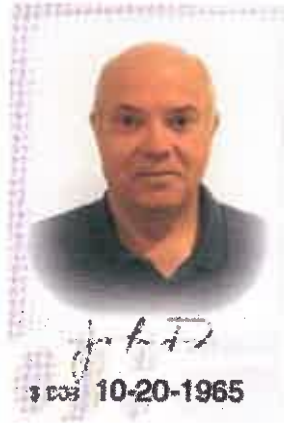
All cards will be personalized, affixed to carrier and mailed using Datacard MX6100 card personalization and mailing equipment. The MX6100 will laser engrave all personal data. The MX6100 is modular in design and can easily be expanded to accommodate technological advances in card production.



## Proposed Security Features

Microprinting / Nanoprinting	<p><b>Security Feature: Level 2</b></p> <p>Miniature lettering which is discernible under magnification. Incorporated into fine line backgrounds or placed to appear as bold lines. Continues to decrease in size as technology improves. Cannot be scanned or reproduced on commercially available printers.</p> <p>Microprint lettering has been embedded in numerous areas of our proposed card design for added security.</p>	 
Redundant Data	<p><b>Security Feature: Level 1,2</b></p> <p>The application of redundant data provides another obstacle in attempts to alter or compromise a card. The date of birth for example can be applied in multiple locations, one using tactile format. Changing either of these elements is impossible without damage to the card structure. These cards can also provide redundant data in the form of a ghost image applied to the front and back of the card, and a secondary signature to the front.</p>	
Rainbow Printing	<p><b>Security Feature: Level 1</b></p> <p>A printed feature demonstrating a controlled, subtle color shift in a linear, continuous fashion.</p> <p>In the second example, notice how the Microprinting shifts in color in parallel with the rear graphic.</p>	




Color Shifting Inks	<p><b>Security Feature: Level 1 (Optional)</b></p> <p>Special security inks containing microscopic pieces of metallic substances and arranged in such a manner as to change color when tilted to view. Very common in currency, travel and identity documents.</p>	
Undisclosed Third Level	<p><b>Security Feature: Level 3</b></p> <p>The third level security feature has been applied within the card design. These elements are for forensic analysis only, and will be discussed upon request. All such forensic features are unique to each jurisdiction, and thus due to the strictly confidential nature of the feature it can only be discussed in confidential meetings.</p>	
Deliberate Error	<p><b>Security Feature: Level 2</b></p> <p>Veridos' experience has taught us that designing the card as a total solution provides us with flexibility to meet future security and legislative needs. Since our cards are made of overlapping security features, individual features can be added, removed or reconfigured based on advances in technology and changes in standards, all without leaving any gaps in the solution or causing undue extra cost.</p>	
Security Background	<p><b>Security Feature: Level 1,2</b></p> <p>The designs for these cards have been created specifically for WV. and incorporate a secure background consisting of a fine, structured guilloche pattern. These patterns change in color across the card area, creating a rainbow</p>	

	<p>effect. These two features alone are virtually impossible to imitate. With the combination of all the blended security features, attempts to alter or change the document could be detected with minimal difficulty.</p>	
<p>Ultraviolet Text in Substrate</p>	<p><b>Security Feature: Level 2</b></p> <p>This feature is incorporated within the design on both sides of the card and is only visible under an ultraviolet (black light) source. These will fluoresce when exposed to the correct light source. Part of the blended security features within the microprint on the background will also fluoresce when exposed to the correct light source.</p>	
<p>Laser Engraving / Etching</p>	<p><b>Security Feature: Level 1</b></p> <p>A method of personalizing cards with photographs and variable personal data using focused laser energy. It also generates level 1 security by using extra laser energy to disturb the page surface, thus creating tactility.</p>	

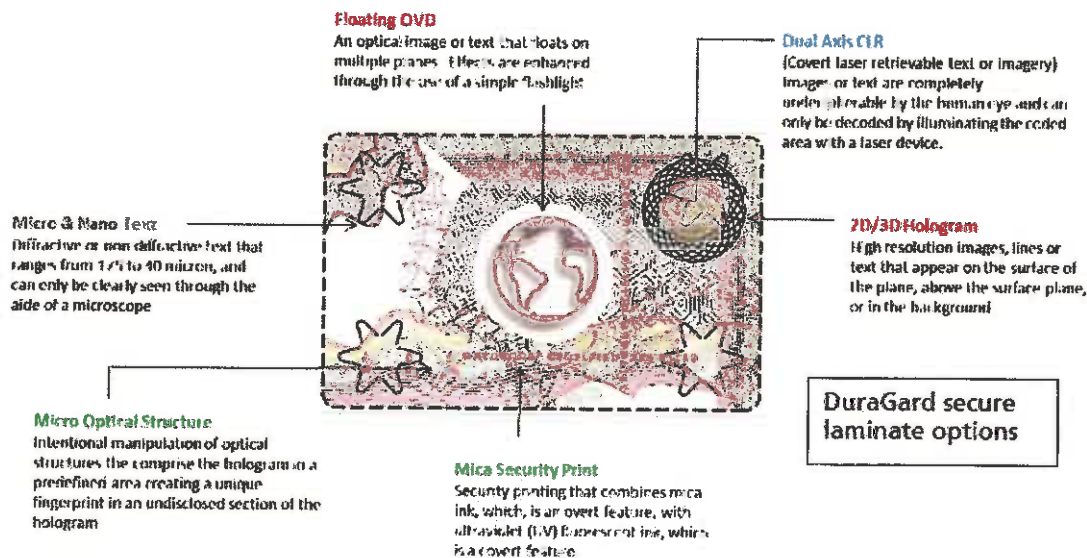
Tactile Data	<p><b>Security Feature: Level 1,2</b></p> <p>A proposed option for WV included in our base card as well as Option 2, is our clear laser feature. Clear laser combines both laser marking and secure indent to create an individually personalized clear security feature that is all but impossible to alter or and counterfeit. Overlap of this feature with the primary photo, with further prevent fraudulent attempts at image substitution. Our clear laser feature can also contain a pattern, design or outline that can be customized to WV for a level 2 security feature.</p>	 
Overlapping Data	<p><b>Security Feature: Level 1,2</b></p> <p>Overlapping of data fields adds increased difficulty to counterfeit attempts. This is accomplished during the data application process, with the primary signature overlapping the primary photo on the Driver's License and Identification card. Overlapping data has been found to be an effective deterrent against attempts at photo substitution style fraud.</p>	
PersoCurve / Laser Shadow	<p><b>Security Feature: Level 1,2 (Optional)</b></p> <p>PersoCurve combines unique variable large fonts, microprint, and biographical data, such as a name, document number etc. using laser engraving. The shape can be designed and customized in many different forms. For example:</p>	

	<p>to wrap around in a spiral manner or a wave shape.</p> <p>This variable text image is created automatically during the job run without requiring pre-conversion of stored images because it provides more flexibility and efficiencies to the process of using unique images, without having to extract from a pre-converted file in a database.</p> <p>LaserShadow uses a dithered laser engraving technology to create large backgrounds of variable text or images that overlap other personalized data fields.</p>	
<p>Security Background Overlapping the Portrait Image Area</p>	<p><b>Security Feature: Level 1,2</b></p> <p>To provide for optimum visibility of the photograph, there is little or no printing in the relevant areas of the card. The harmonious phasing out of the image into the background print and overlapping the portrait edges makes it difficult to alter or counterfeit. Veridos has intentionally designed the background design to overlap the defined photo area.</p>	



<p>Pre-Printed Serial Number on Card Backs – Document Control Number (DCN)</p>	<p><b>Security Feature: Level 1,2</b></p> <p>Veridos assigns each DL/ID card a DCN on the card back. The DCN is laser engraved and consists of a unique alphanumeric value consisting of two alpha characters and seven numeric characters.</p> <p>A database of these DCNs is recorded and provided to WVDMV prior to storage in the secure vault. Cards are then transported to the secure vault and fully inventoried. The secure vault has its own CCTV system and is always operated under dual custody. WVDMV will have access to the 'Vault DCN Report' which is a standard report generated by Veridos' Online Portal.</p>	
<p>Machine Readable Technology (MRT) (rear)</p>	<p>1D-barcode; Code-39, Verifies the authenticity of the document, the data or the person by the use of a reader and comparison of the stored data to other information.</p>	
<p>Machine Readable Technology (MRT) (rear)</p>	<p>2D-barcode; PDF-417, Verifies the authenticity of the document, the data or the person by the use of a reader and comparison of the stored data to other information.</p>	

DuraGard Laminate, applied to protect the printing of the color photo on the front of the card, offers multiple Level 1, Level 2 and Level 3 security options:



#### Section 4, Subsection 4.4.2 - Vendors card design solution should include a version number. Vendor Response

Our proposed solution complies.

All card designs include a paper and card proof with a version number for each design. With each substantial change and update to the proposed design, card proofs (either digital or physical) will be provided so that each stakeholder at WVDMV has an opportunity to review and provide feedback.

#### Section 4, Subsection 4.5 - Card Carriers

##### Section 4, Subsection 4.5.1 - The Vendor should provide at least one (1) card carrier design. Vendor Response:

Our proposed solution complies.

Below is an example of what the carrier design may look like. The final design will be developed in collaboration with WVDMV.



Here is your NEW West Virginia Driver's License

This is your permanent one piece driver's license. Please destroy the temporary duplicate license you received when you applied or renewed and only post driver's license photo card you will be by putting them into separate pieces.

**Protecting Your Personal Information**

The State of West Virginia is committed to protecting your privacy by keeping your personal information accurate, confidential, and secure.

Need more information?

- Call us! 1.800.942-9006

#### Section 4, Subsection 4.5.2 - System should affix the credential to the appropriate card carrier. Vendor Response:

Our proposed solution complies.

Our production system provides card affixing to the carriers, along with QA checks to ensure that the right card is attached to the right carrier. This is an in-line process used with Datacard Central Issuance machines. With both automated and manual Quality Control processes in place, various processing equipment is configured with features which ensure the accuracy and integrity of the production run, e.g. vision systems. With Veridos' automated matching system, the machine reads the barcode and a camera reads the corresponding barcode on the card carrier. If there is a match, the equipment will continue to process. Our process will ensure that 100% of cards are matched to the correct card carrier.

All cards will be personalized, affixed to carrier and mailed using Datacard MX6100 card personalization and mailing equipment. The MX6100 will laser engrave all personal data. The MX6100 is modular in design and can easily be expanded to accommodate technological advances in card production.



MX6100 System with MXD System & MXi Envelope Insertion System

**Section 4, Subsection 4.5.3 - Adhesive used to affix the card carrier should be strong enough to hold the card through the mailing process but be easily removed by the applicant.**

**Vendor Response:**

Our proposed solution complies.

Veridos uses a card industry best practices adhesive that will be strong enough to hold the card through mailing, while still being able to be easily removed by the applicant.

**Section 4, Subsection 4.5.4 - Changes to the card carrier designs should be allowed two (2) times per year. Vendor Response:**

Our proposed solution complies.

Veridos will provide changes to the card carrier designs up to two (2) times per year assuming that impacts to pre-printed carrier stock are done when volumes are low. Changes to variable print data on the carrier are easily accommodated using standard word processing software at our central issuance facility.

**Section 4, Subsection 4.6 - Card Durability**

**Section 4, Subsection 4.6.1 - Card materials should have a guaranteed life of five (5) years against breakage or significant deterioration or degradation of the data on the front and back of the card.**

**Vendor Response:**

Our proposed solution complies.

The proposed Driver's License is constructed of Polyester Enhanced Polycarbonate (PEC) that has been extensively tested and qualified by Veridos and third party laboratories. The card body is constructed of multiple layers, which include transparent and opaque materials which are a Veridos trade-secret and are not commercially available. Once

assembled, the materials are laminated together under specific heat and pressure (without any adhesive or thermoplastics) to form a consistent card body which **cannot be delayered** as is possible using other substrates.

#### Card Overview

<b>Material:</b>	Polyester Enhanced Polycarbonate (PEC)
<b>Service Life:</b>	8 years of usage
<b>Dimensions:</b>	85.60 mm x 53.98 mm x 0.76 mm (nominal)
<b>ISO/IEC Spec:</b>	7810:2003 (Card Body)
<b>Color Photo:</b>	Thermal dye diffusion printing
<b>Data Elements:</b>	Laser Engraving

#### Benefits of Polyester Enhanced Polycarbonate (PEC)

- Durable PEC card body
- Color photo using thermal dye diffusion printing (D2T2)
- Laser engraving for secure data application
- Offers superior value at cost effective price
- Offers outstanding durability
- Similar technology to what is used in passports and National ID card programs
- Environmentally friendly material
- Protection against photo substitution
- Protection against counterfeits including types A1, A2, B1, and B2

**Section 4, Subsection 4.6.2 - For any individual card not lasting the five (5) years, the Vendor's sole liability should be to provide a credit to a subsequent invoice.**

#### Vendor Response:

Our proposed solution complies and Veridos agrees to provide this credit for cards not lasting five (5) years under normal use.

All cards that are deemed unacceptable during manufacturing, personalization or fulfillment will be recorded and destroyed and Veridos will assume the cost of these cards. At no time shall the WVDMV be invoiced for cards which fail while in the Veridos

facility. WVDMV will only be billed for cards that have passed are quality requirements and inducted in the USPS.

## Section 4, Subsection 4.7 - Quality Assurance (QA)

Section 4, Subsection 4.7.1 - The Vendor QA process should guarantee that 100% of all cards mailed will be free from any defect in printed data or card design features, incorrect data, incorrect card type, and card materials must be free from any material defect.

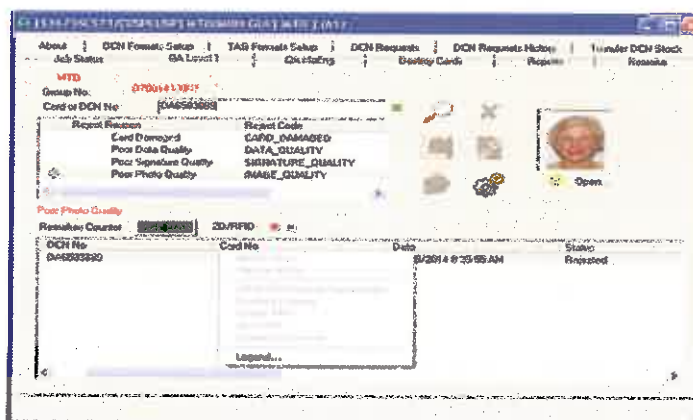
### Vendor Response:

Our proposed solution complies.

Veridos has a comprehensive Quality Assurance program in place throughout the Production environment. This program incorporates both **quality and security balancing procedures at each production step**. In addition to the in-process QA review, Veridos has an independent QA team that randomly samples all completed Production output to ensure the highest level of quality is maintained. The total Level of sampling amounts to over 12 million+ cards annually. All production rejects are logged in our Production System (SAP).

### Production Quality at a High Level

- Automatic quality checks are performed by central issuance equipment
- Cards identified as failed are separated and each is manually inspected
- Inspection is based on: cards damaged, poor data, signature and photo quality
- Damaged card status is updated on systems and cards are remade



An integral part of our QA process is the collection, analysis, and reporting of quality and service related incidents. As part of our continuous improvement initiative, we have implemented an incident tracking system that is utilized by **all areas of our Operation**. An incident is **anything that impacts a customer and / or production deliverable** regardless of the nature or root cause of the incident i.e. the issue can be the result of a customer initiated problem. Any WVDMV correspondence which raises a service and/or quality issue is also logged via the incident reporting system.

**Section 4, Subsection 4.7.2 - The Vendor QA process should ensure that the correct image is printed on the card and that the image quality meets or exceeds ICAO standards.**

### Vendor Response:

Our proposed solution complies.

To ensure that the image quality meets or exceeds ICAO standards, the solution has an internal ICAO-compliant quality checking algorithm, performed during the capture process that eliminates records being sent that would not be satisfactory for use in the FRS.

Automatic ICAO photo quality checks are performed on photos captured by the system. Images are rechecked for ICAO compliance if any manual cropping is performed.

The specific ICAO checks to be performed, and the acceptable threshold levels, are configurable by the System Administrator. This allows the solution to be tailored to WVDWMV's needs without interfering with the objective of capturing ICAO-complaint images.

An operator also has the ability to made adjustments the placement of the head in the window if necessary.

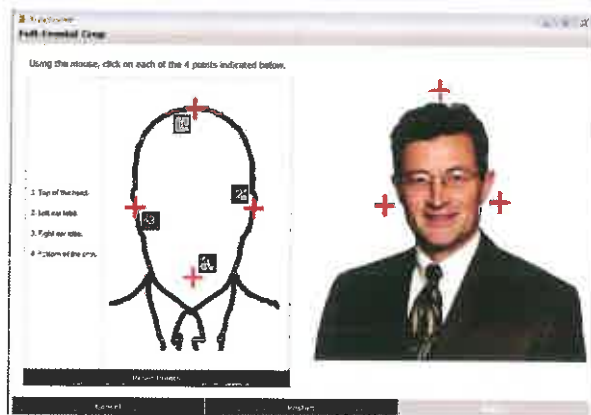
As shown in the screenshot below, the solution's quality check verifies pose, face position, lighting, feature points, and more. The image capture solution automatically crops images to meet ICAO and ISO 19794-5 full frontal specifications.



An optional Color Correction step can be provided in the workflow, if desired. This option would provide operators the ability to enhance the image quickly and easily by choosing one of the images in the left hand pane. All the ICAO and photo consistency checks are run on the chosen image to ensure the image meets the required quality specifications.



The system allows for the manual capture and retaking of images. The image checks performed include facial feature identification, image cropping, image placement, and checks for lighting. Users can also manually crop the image, at which time it is checked for ICAO compliance. A supervisory override is available, if required, to allow images of individuals who have unique characteristics that may show up in the background of an ID card photo; for example, a high-backed wheelchair in an accessible station.



#### Production Quality at a High Level

- Automatic quality checks are performed by central issuance equipment
- Cards identified as failed are separated and each is manually inspected
- Inspection is based on: cards damaged, poor data, **signature and photo quality**
- Damaged card status is updated on systems and cards are remade

Section 4, Subsection 4.7.3 - The Vendor QA process should guarantee that 100% of card carrier forms produced will be of high quality with professional printing, as determined by the Agency.

**Vendor Response:**

Our proposed solution complies.

Carrier stock used for card mailing will be of high quality and Veridos uses a third party professional printing firm to provide the carriers. The carrier design and quality will be approved by WVDMV.

Section 4, Subsection 4.7.4 - Card Carrier form should not be smudged, wrinkled, torn, or otherwise damaged during the production process.

**Vendor Response:**

Our proposed solution complies.

Carrier stock used for card mailing is of high quality and is quality checked before being inserted into the automated card affixing system.

Section 4, Subsection 4.7.5 - Envelopes for card mailing should be secure, properly sealed, and not smudged., wrinkled, torn, or otherwise damaged in the production process.

**Vendor Response:**

Our proposed solution complies.

Envelopes used for card mailing are of high quality and are quality checked before inserting them into the automated mailing system.

---

## ON-PREMISE

### Section 4, Subsection 4.8 - Facility Image & Signature Capture Workstation ("ICW") Objectives

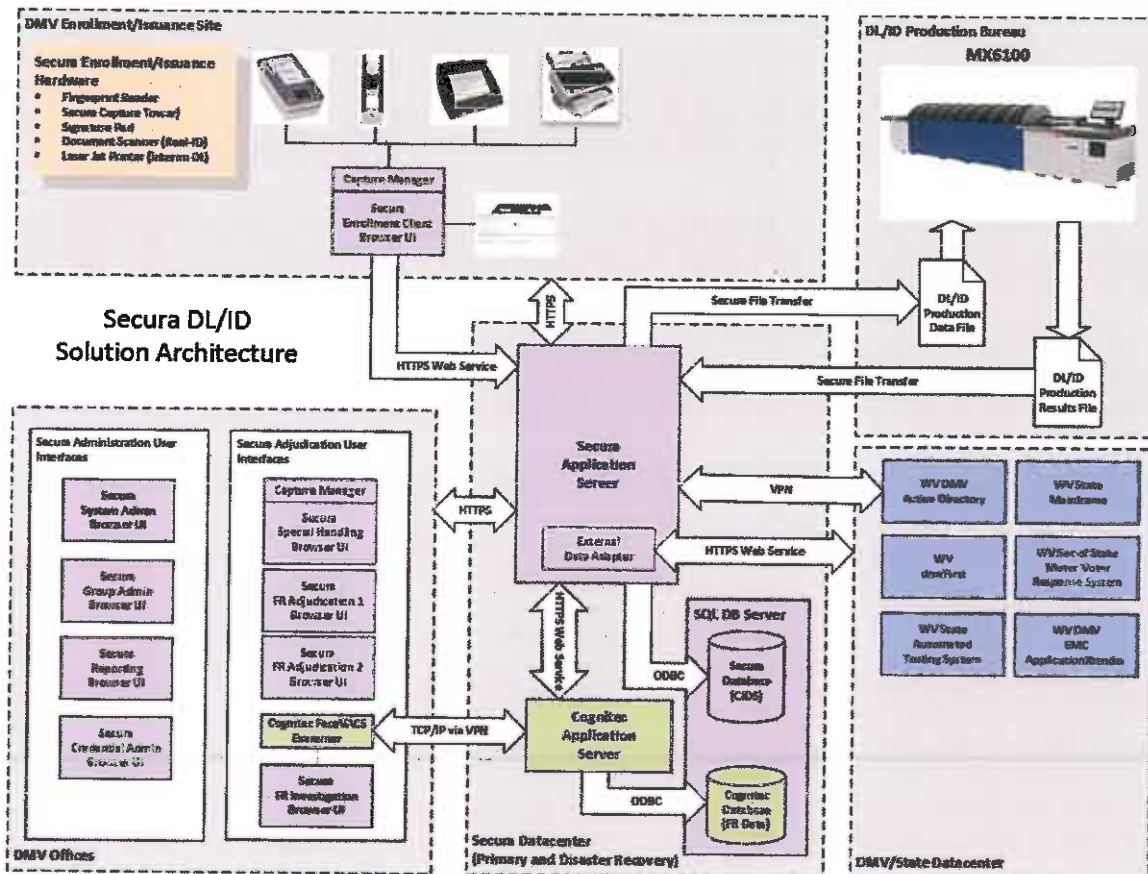
Section 4, Subsection 4.8.1 - Vendor should explain the entire process their proposed solution will use to handle new applicants. This should include what information will be collected, both digital and physical documents, and the equipment required to produce the secure temporary DLAD and the material used.

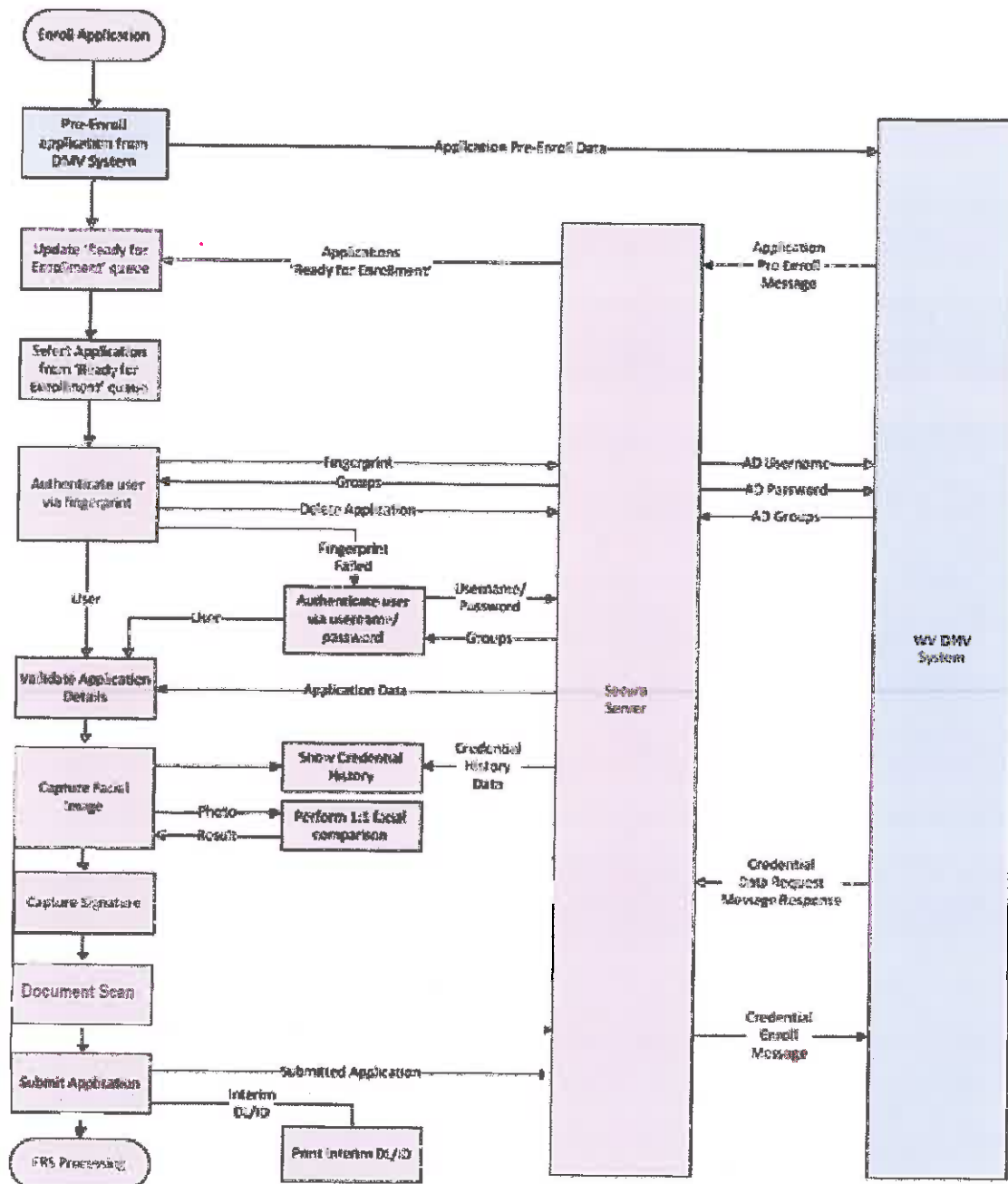
---

#### Vendor Response:

Our proposed solution complies.

The diagrams below provide an overview of the entire solution including the handling of new applicants.





Taking the photo at the beginning of the enrollment process provides a visual record of the customer, even if they decide to discontinue the process later. This can be helpful when investigating fraudulent activities because individuals may decide to depart the facility if they feel they are arousing suspicion before completing the entire process as well as meeting the Real ID process of the Federal government. This process does not involve redundant steps or multiple cameras.

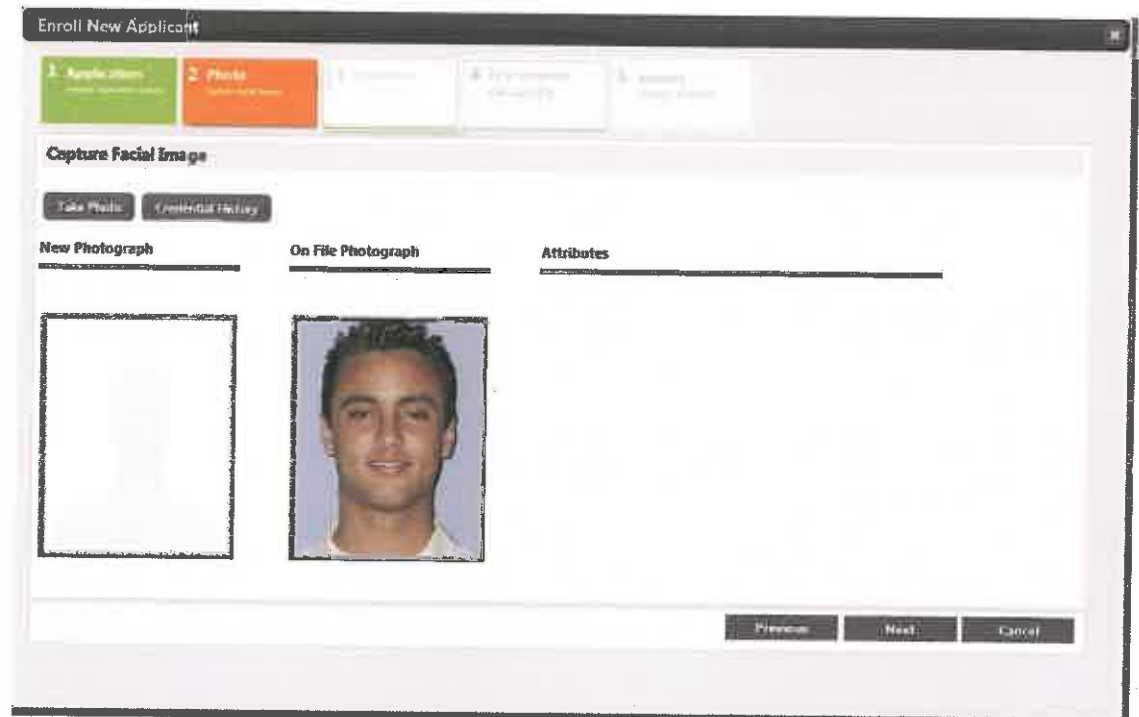
A general overview of the process is:

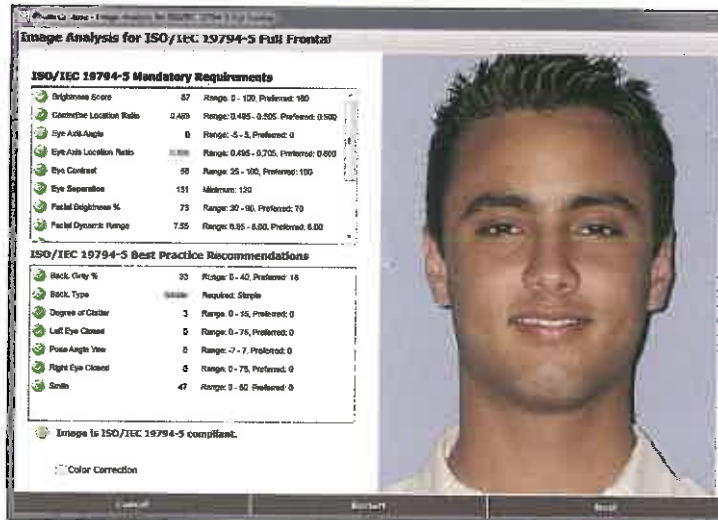
The operator enters or selects the applicant name and data of birth (new record or request from state system)

1. Demographic data



2. The operator captures the applicant photo





3. 1:1 FRS Check is done against the latest photo on file
4. The operator capture the Signature



5. The operator scans the required documents

Note: The exact documents to be captured will be determined during the design phase of the contract

6. The operator completes the applicant enrollment and saves the completed record to the Secura database ("Enrolled") and the Temporary Drivers License is automatically printed

If the application process is not complete, the data collected, including photo and signature, is saved and is available for investigators to review.

For document scanning, Secura has the ability to capture a number of different documents during the enrollment process. Veridos will work with the State to determine the most appropriate documents and the business rules around which type of documents are required given the other documents that already have been provided and come up with a matrix that the system will use to guide the operator and ensure that the Real ID requirements have been met.

The production deployment of the Secura FRS will consist of redundant 'Primary' and 'Disaster Recovery' environments which contain the Secura Datacenter components. These components consist of:

- Secura Application Server
- Cognitec Application Server
- SQL Database Servers (Application and FRS Engine)
  - (Primary and Disaster Recovery mirrored)

The servers will be virtualized and hosted by the WVDMV's datacenter, the exact requirements for disk space, memory, and processors will be determined via collaborative discussions during the design phase of the project.

An additional 'Test' environment will also be deployed to support User Acceptance Testing as well as the testing of future updates and system upgrades.

The following components will be used to capture images, signatures and documents, and for printing of the secure temporary DL/ID documents.

### Secure Image Capture Tower - Specifications



- Base plate: 8.0 in. x 8.0 in. (20.32 cm x 20.32 cm)
- Size - 13.0 in. x 8.0 in. x 32.0 inches in height.
- Weight - 22.0 lbs. (10.0 kg) system
- Power - 120 VAC / 60Hz
- Operating Temp - 60°F to 95°F (15°C to 35°C)
- Operating Humidity - 20% to 80% RH non condensing
- Storage - 5°F to 140°F (-15°C to 60°C)
- Flash Working Range - 3.0 to 12.0 feet (1.8<sup>m</sup> to 4.6<sup>m</sup>)
- Flash Cycles – rated for 250,000 cycles
- Flash, External - 100WS, 120 VAC Flash Recycle time – average of 5 seconds or less for re-take support
- Camera Resolution – 18.0 megapixel or greater digital SLR photo capture
- Camera Zoom – Digital Auto Zoom or Manual Zoom
- Camera Tower Range – Vertical Adjustment - 10 inches
- Camera Tower Range – Rotation – tilt range of 30 degrees - allows for seated or standing subjects



- Camera Tower Security – hardware mountable to a countertop – theft and vandalism resistant
- Camera API Compatibility – Windows XP or 7 via Datacard Secure Camera Tower iCap license
- Connectivity – USB 2.0 - Multiple USB ports in support of computer and peripheral connectivity
- Connectivity – Ease of Connectivity – Single Wire data connection with built in USB hub for peripherals

**Photo Backdrop – A Professional Photo Backdrop System consisting of:**



- Screen Size – 36" Wide x 48" or 48" Wide x 60" Tall when expanded
  - Size to be chosen subject to contract award and SOW
  - Includes clips for mounting to backdrops stands
- Frame Material – Internal Self Expanding Frame
- Storage / Transport Case – Zippered nylon case
- Color – Blue one side, White opposite side
- Operating Temp - 50° F to 120° F
- Support Hardware – Wall / Ceiling Clips – for mounting Backdrop clips to a wall or ceiling

**Signature Tablet - SigGem® 5.7 Color Display or Equivalent**



- Full-color TFT VGA (640x480) LCD Display
- Displays the signature on the signature pad, as well as the computer screen.
- Tempered glass signing surface w. internal high-performance E/M digitizer.

- Rated for 2 million signatures
- Pen Type - Active low-power, rugged E/M pen, battery-less
- Pen Settings - 1024 pressure level option
- Dimensions - 7.2" x 6.6" x 2.1" sloping (180 x 160 x 54 mm)
- Signing area - 4.6" x 3.4" (118mm x 86mm)
- 377 Points per second.
- 410 points per inch (programmable)
- Dual Serial / USB connectivity
- Encryption Capabilities - AES optional, FIPS-197 compliant
- APIs provide for interactive text, graphics, pen-tap hotspots and checkboxes
- Forensic-quality .SIG data capable of examination and authentication.
- FCC, RoHS, and WEEE compliant

**Document Scanner – Kodak Alaris – S2000 Series - ADF Type**



- Shown with and without Optional Passport Scanner
  - Scanning Technology - Camera Based Page Sensing
  - Daily Duty Cycle – 5000 scans per day
  - Pages Per Minute (PPM) - up to 50
  - Optical Resolution 600 dpi
- Output Resolution :
  - 175 / 100 / 150 / 200 / 240 / 250 / 300 / 400 / 500 / 600 / 1200
- Max / Min Document Size:
  - 216 mm x 356 mm (8.5 x 14 in.) / 52 mm x 52 mm (2.08 in. x 2.05 in.)
- Supports shared scanning from multi-workstations
- Handles Real ID breeder docs such as birth certificates, utility bills, etc
- Handles small documents such as ID cards, embossed hard cards, etc
  - Hard card (license) transport in both landscape or portrait
- Power – 120 / 240 Volt – 50 / 60 Hz
- Standby/Sleep mode/Network Standby: <36 Watts

- 1.5" Color Graphic Display
- Pause and resume or Jam resume modes
- Weight: 3.3 kg (7.2 lbs.)
- Depth: 204 mm (8.0 in.), not including input tray and output tray
- Width: 312 mm (12.3 in.)
- Height: 182.5 mm (7.2 in.), not including input tray
- Depth with Input Tray 269 mm (10.6 in.)
- Height with Input Tray 231.6 mm (9.1 in.)
- Paper Thickness and Weight 34-413 g/m<sup>2</sup>
- Feeder Up to 80 sheets of 80 g/m<sup>2</sup>
- Connectivity USB 3.0 (cable included)
- File Format Outputs - Single and multi-page:
  - TIFF, JPEG, RTF, BMP, PDF, TXT, PNG, CSV, Word and Excel
- Agency Approvals – Meets all UL, CSA, CE, and FCC requirements

#### **Document Scanner – Passport Reader Accessory**



#### **Passport Scanner Accessory - Kodak Alaris S2000 Series**

- Integrates directly into the primary S2000 Series ADF Scanner
  - No additional power cords or USB power required
- Docks directly beneath the primary scanner for a compact footprint
- Automatically triggers scanning when passport is placed into the scanner
- Able to scan two passport pages at once
- Able to scan both US and International passports of varying thicknesses
- Captures images in 2-3 seconds at 300 dpi settings
- Optical resolutions up to 1200 dpi
- Output resolutions 75, 100, 150, 200, 240, 250, 260, 300, 400, 500, 600 and 1200 dpi
- Supports reading of other small, fragile, or high value documents
- Max doc size 5" x 7.3 in" (27 x 186 mm)

- Height x width x length (2.8 x 12 x 10 in.) (72 x 306 x 255 mm)
- Weight 3.5 lbs. (1.6 kg )

**Paper Printer – HP LaserJet Pro – For Interim ID/DL**



- HP LaserJet Pro M402n – or equivalent - Laser Printer
  - Technology - Monochrome – laser
  - Resolution – HP FastRes 1200 dpi
  - Monthly duty cycle – up to 80,000 pages
  - Recommended volume – up to 4000 / month
  - Paper Trays - Standard – 2 (100 pg. and 250 pg.)
  - Connectivity USB 2.0, and 10,100,1000 Gb Ethernet
  - Printer Toner Cartridge – HP26A or Extended HP26X
  - Dimensions - WxDxH - 15 x 14.06 x 8.5 in
  - Weight - 18.92 lbs.

---

**Section 4, Subsection 4.8.2 - Vendor should describe the capabilities of the proposed image capture device. Description should include:**

---

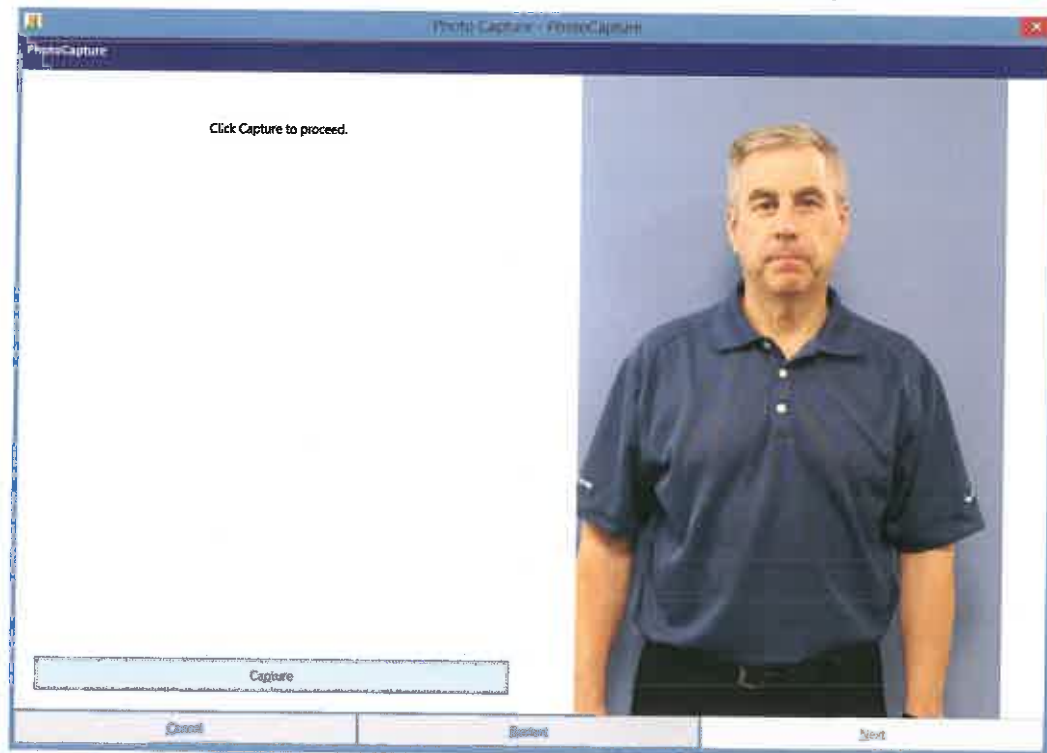
**4.8.2.1 How live video of the applicant will be displayed.**

Our proposed solution complies.

Operators see a live video image of the applicant, then point-and-click to capture.

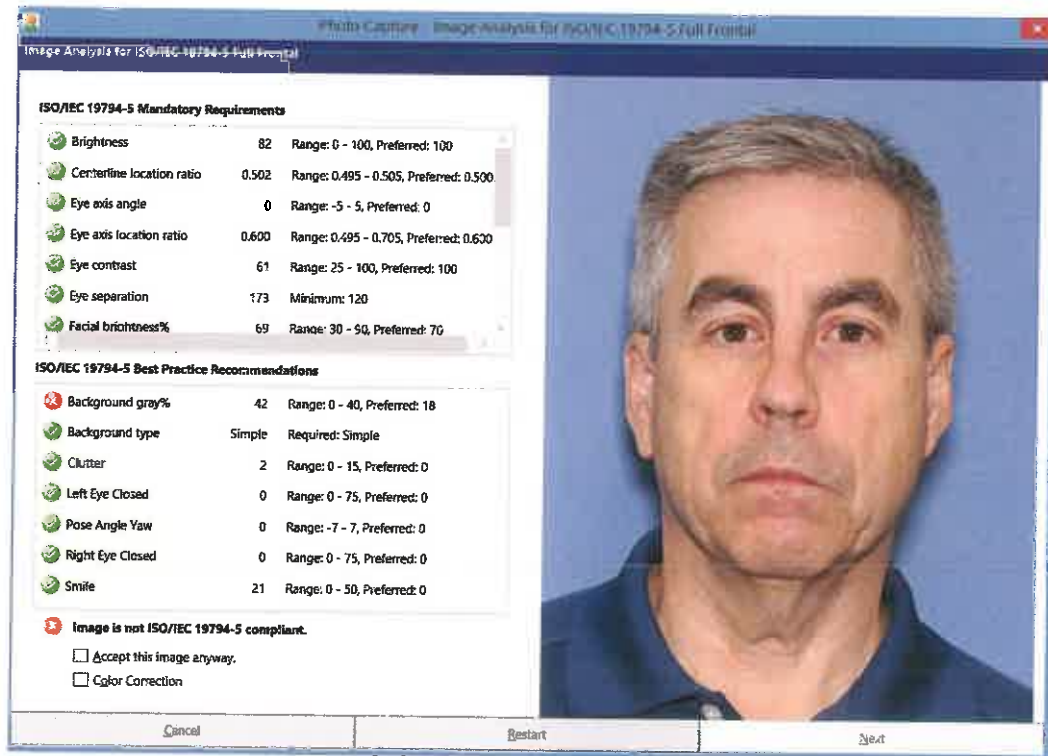


After clicking on 'Take Photo' the live video box below is displayed.



After the photo is captured, the face is found, cropped, and checked for ICAO compliance.

The cropped image then has 1:1 and 1:N checks performed and it is stored in the image repository.



The ICAO checks will be tailored to be the WVDMMV needs, if a blue backdrop is used as shown above, the Grayback Percentage check would be eliminated as thus showing the above image as acceptable.

#### 4.8.2.2 How the employee can perform configuration ICAO checks and how these results will be returned to the employee

Our proposed solution complies.

Automatic ICAO photo quality checks are performed on all photos captured by the system. Images are rechecked for ICAO compliance if any manual cropping is performed.

The specific ICAO checks to be performed, and the acceptable threshold levels, are configurable by a Secura system administrator. This allows the solution to be tailored to WVDMMV's needs without interfering with the objective of capturing ICAO-complaint images.

The photo capture follows a pre-defined workflow for each type of capture (photo, signature, document scanning). For photographs, the ICAO compliance check is performed as one of the last steps to ensure the photo being stored meets the needs of the WVDMV. The operator can be presented with a screen that shows all the checks that have passed and failed as shown below.

As shown in the screenshot below, the solution's quality check verifies pose, face position, lighting, feature points, and more. The image capture solution automatically crops images to meet ICAO and ISO 19794-5 full frontal specifications.



An optional Color Correction step can be provided in the workflow, if desired. This option would provide operators the ability to enhance the image quickly and easily by choosing one of the images in the left hand pane. All the ICAO and photo consistency checks are run on the chosen image to ensure the image meets the required quality specifications.

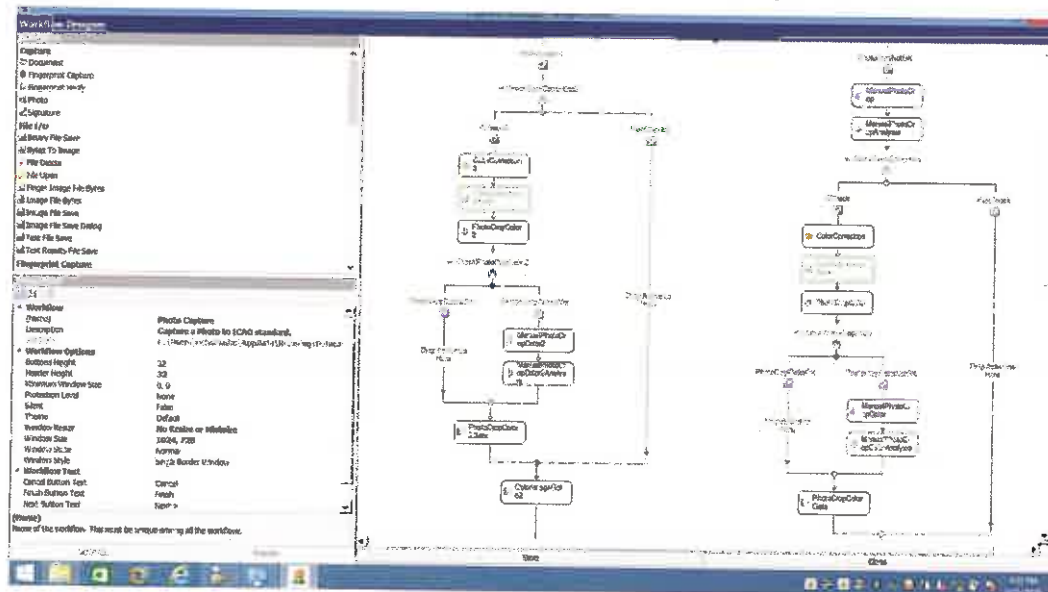


#### 4.8.2.3 How an employee can recheck for ICAO compliance after manual adjustments

Our proposed solution complies.

Capture Manager software, a subcomponent of the overall image capture solution, has a workflow management tool that allows the capture process to be tailored to a jurisdiction's specific needs. Commonly used activities within this tool set are photo capture, auto cropping, ICAO compliance checking, and manual photo cropping.

In many deployments, a workflow is provided that first attempts to automatically crop the image, if this fails the workflow automatically prompts the user to manually crop the image. After all cropping steps, an ICAO compliance check is performed.



Veridos will work with the WVDMV to tailor the photo capture process workflows to ensure images captured fit the needs of its unique environment. Once the photo capture process workflow is developed during the design phase of the project, each photo capture will be checked against the agreed upon standards. Operators will be shown the results of the checks and allowed to retake the image or use one of the correction tools. In the case of individuals wearing medical or religious headwear that meet the requirements for exemption from the process, operators will be allowed to accept the image anyway.

#### 4.8.2.4 How checks will be configurable to allow the Agency's system administrator to select the specific ICAO checks to be enabled.

Our proposed solution complies.

The specific ICAO checks to be performed, along with the acceptable threshold levels, are configurable by the System Administrator. This capability allows the solution to be tailored to WVDMV's needs without interfering with the objective of capturing ICAO-complaint images.

Changes to the ICAO checks made in the System Administration screen are automatically applied statewide.

---

4.8.2.5 How checks will be configurable to allow the Agency's system administrator to select the specific ICAO checks where overrides are allowed.

---

**Vendor Response:**

Our proposed solution complies.

The specific ICAO checks to be performed, along with the acceptable threshold levels, are configurable by the System Administrator on a menu within the back-office portal of the Secura solution.

A system administrator with the correct privileges will be able to enter the menu, select the configured ICAO parameters menu item and select the specific ICAO Checks to be performed as well as those checks that require supervisory overrides previous checks do not pass. This capability allows the solution to be tailored to WVDMV's needs without interfering with the objective of capturing ICAO-complaint images.

Changes to the ICAO checks made in the System Administration screen are automatically applied statewide.

---

Section 4, Subsection 4.8.3 - Vendor should explain the process and provide a detailed list of hardware the proposed solution will use to capture images and signatures when communication with the central image/demographic system is off-line. The system should be able to link new data and images to existing records when communication with the server is restored.

---

**Vendor Response:**

Our proposed solution complies.

If connectivity to the Secura server is disrupted, the Secura Enrollment solution can continue the capture process offline, and retain the data until the *connection is re-established*.

The credential data is then submitted/uploaded and associated with the driver's license number and stored in the Secura (CIS) database. If submission fails, an error is indicated, and the user can inform the appropriate support personnel. If the capture process is not successfully completed, the captured data is still stored in the Secura database, and the record is marked as 'incomplete'.

The following hardware is proposed for the ICWs. This hardware will be used for both online and offline transactions.

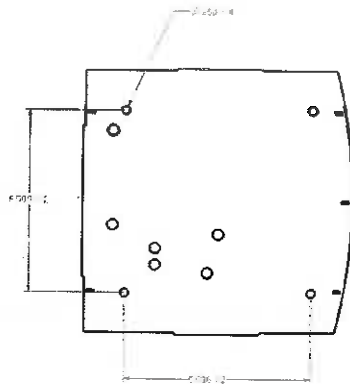
**Secure Image Capture Tower - Specifications**



- Base plate: 8.0 in. x 8.0 in. (20.32 cm x 20.32 cm)
- Size - 13.0 in. x 8.0 in. x 32.0 inches in height.
- Weight - 22.0 lbs. (10.0 kg) system
- Power - 120 VAC / 60Hz
- Operating Temp - 60°F to 95°F (15°C to 35°C)
- Operating Humidity - 20% to 80% RH non condensing
- Storage - 5°F to 140°F (-15°C to 60°C)
- Flash Working Range - 3.0 to 12.0 feet (1.8<sup>m</sup> to 4.6<sup>m</sup>)
- Flash Cycles – rated for 250,000 cycles
- Flash, External - 100WS, 120 VAC Flash Recycle time – average of 5 seconds or less for re-take support
- Camera Resolution – 18.0 megapixel or greater digital SLR photo capture
- Camera Zoom – Digital Auto Zoom or Manual Zoom
- Camera Tower Range – Vertical Adjustment - 10 inches
- Camera Tower Range – Rotation – tilt range of 30 degrees - allows for seated or standing subjects

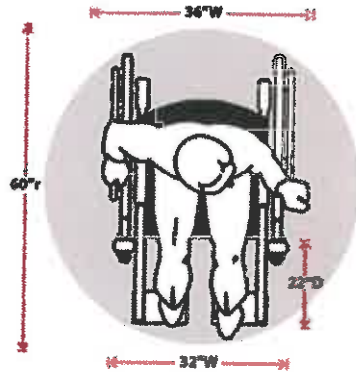
- Camera Tower Security – hardware mountable to a countertop – theft and vandalism resistant
- Camera API Compatibility – Windows XP or 7 via Datacard Secure Camera Tower iCap license
- Connectivity – USB 2.0 - Multiple USB ports in support of computer and peripheral connectivity
- Connectivity – Ease of Connectivity – Single Wire data connection with built in USB hub for peripherals

#### **Secure Capture Tower Mounting Specifications**

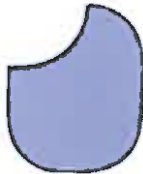


#### **Secure Capture Tower - ADA Compliant Workstation Recommendations: (not quoted)**

- 32"W minimum for leg space
- 22"D minimum for leg space
- 27"H clearance for under table knee space\*
- 60" diameter required for turning/maneuvering
- 36"W minimum for aisle space
- \*Since the size of people and wheelchairs vary, the guideline recommends the table top height should adjust from 28"H - 34"H.



**Photo Backdrop – A Professional Photo Backdrop System consisting of:**



- Screen Size – 36" Wide x 48" or 48" Wide x 60" Tall when expanded
  - Size to be chosen subject to contract award and SOW
  - Includes clips for mounting to backdrops stands
- Frame Material – Internal Self Expanding Frame
- Storage / Transport Case – Zippered nylon case
- Color – Blue one side, White opposite side
- Operating Temp - 50° F to 120° F

**Photo Backdrop Stand – Free Standing**



- Adjustable up to 110" in height
- Heavy duty light stands, with wide footprint.

- Black anodized, heavy gauge aluminum tube construction, with non-glare finish
- Holds up to 16.5 lbs.
- Air cushioned
- Weight 4 1/2lbs each
- Non-slip tips on each leg to prevent movement
- 5/8 universal light stand adapter
- Complete with carry bag
- Support Hardware – Wall / Ceiling Clips – for mounting Backdrop clips to a wall or ceiling

**Signature Tablet - SigGem® 5.7 Color Display or Equivalent**



- Full-color TFT VGA (640x480) LCD Display
- Displays the signature on the signature pad, as well as the computer screen.
- Tempered glass signing surface w. internal high-performance E/M digitizer.
- Rated for 2 million signatures
- Pen Type - Active low-power, rugged E/M pen, battery-less
- Pen Settings - 1024 pressure level option
- Dimensions - 7.2" x 6.6" x 2.1" sloping (180 x 160 x 54 mm)
- Signing area - 4.6" x 3.4" (118mm x 86mm)
- 377 Points per second.
- 410 points per inch (programmable)
- Dual Serial / USB connectivity
- Encryption Capabilities - AES optional, FIPS-197 compliant
- APIs provide for interactive text, graphics, pen-tap hotspots and checkboxes
- Forensic-quality .SIG data capable of examination and authentication.
- FCC, RoHS, and WEEE compliant

### **Document Scanner – Kodak Alaris – S2000 Series - ADF Type**



- Shown with and without Optional Passport Scanner
  - Scanning Technology - Camera Based Page Sensing
  - Daily Duty Cycle – 5000 scans per day
  - Pages Per Minute (PPM) - up to 50
  - Optical Resolution 600 dpi
- Output Resolution :
  - 175 / 100 / 150 / 200 / 240 / 250 / 300 / 400 / 500 / 600 / 1200
- Max / Min Document Size:
  - 216 mm x 356 mm (8.5 x 14 in.) / 52 mm x 52 mm (2.08 in. x 2.05 in.)
- Supports shared scanning from multi-workstations
- Handles Real ID breeder docs such as birth certificates, utility bills, etc
- Handles small documents such as ID cards, embossed hard cards, etc
  - Hard card (license) transport in both landscape or portrait
- Power – 120 / 240 Volt – 50 / 60 Hz
- Standby/Sleep mode/Network Standby: <36 Watts
- 1.5" Color Graphic Display
- Pause and resume or Jam resume modes
- Weight: 3.3 kg (7.2 lbs.)
- Depth: 204 mm (8.0 in.), not including input tray and output tray
- Width: 312 mm (12.3 in.)
- Height: 182.5 mm (7.2 in.), not including input tray
- Depth with Input Tray 269 mm (10.6 in.)
- Height with Input Tray 231.6 mm (9.1 in.)
- Paper Thickness and Weight 34-413 g/m2
- Feeder Up to 80 sheets of 80 g/m2
- Connectivity USB 3.0 (cable included)

- File Format Outputs - Single and multi-page:
  - TIFF, JPEG, RTF, BMP, PDF, TXT, PNG, CSV, Word and Excel
  - Agency Approvals – Meets all UL, CSA, CE, and FCC requirements

#### **Document Scanner – Passport Reader Accessory**



#### **Passport Scanner Accessory - Kodak Alaris S2000 Series**

- Integrates directly into the primary S2000 Series ADF Scanner
  - No additional power cords or USB power required
- Docks directly beneath the primary scanner for a compact footprint
- Automatically triggers scanning when passport is placed into the scanner
- Able to scan two passport pages at once
- Able to scan both US and International passports of varying thicknesses
- Captures images in 2-3 seconds at 300 dpi settings
- Optical resolutions up to 1200 dpi
- Output resolutions 75, 100, 150, 200, 240, 250, 260, 300, 400, 500, 600 and 1200 dpi
- Supports reading of other small, fragile, or high value documents
- Max doc size 5" x 7.3 in" (27 x 186 mm)
- Height x width x length (2.8 x 12 x 10 in.) (72 x 306 x 255 mm)
- Weight 3.5 lbs. (1.6 kg )

#### **Fingerprint Reader – for Operator Authentication**



- Crossmatch Verifier 300 LC Fingerprint scanner or Equivalent
  - Meets FBI Appendix F Certification

- Sensor Type - Optical
- Resolution: 500 ppi  $\pm$  1%
- Capture Speed: Very fast capture speed due to high frame rate (15fps)
- Linearity and Rectilinearity: Less than one pixel (average)
- Image Area: 1.2" x 1.2" (31 mm x 31 mm)
- Interface: Universal Serial Bus - (USB 2.0 HS)
- Power: Supplied through the USB 2.0 interface (500 mA @ 5V)
- Dimensions (H x L x W): 2.4" x 6.4" x 3.3" (62 x 162 x 83) mm
- Weight: 1.0 lbs (450 g)
- Mean time between failure (MTBF): 45,000 hours
- Operating Temperature Range: 35 °F to 104 °F
- Humidity Range: 10 - 90 % non-condensing

#### Paper Printer – HP LaserJet Pro – For Interim ID/DL



- HP LaserJet Pro M402n – or equivalent - Laser Printer
  - Technology - Monochrome – laser
  - Resolution – HP FastRes 1200 dpi
  - Monthly duty cycle – up to 80,000 pages
  - Recommended volume – up to 4000 / month
  - Paper Trays - Standard – 2 (100 pg. and 250 pg.)
  - Connectivity USB 2.0, and 10,100,1000 Gb Ethernet
  - Printer Toner Cartridge – HP26A or Extended HP26X
  - Dimensions - WxDxH - 15 x 14.06 x 8.5 in
  - Weight - 18.92 lbs.

If a robust full off-line enrollment offering/option is required, custom Secura licenses are required for additional fees. Features of custom license may include:

High Level Requirement	Feature	Functional Description
Off Line Enrollment	Continued query / transmit if server offline	Will continue to check for the server to come back online, on a configurable schedule.

	Continued query / transmit if workstation offline	If a workstation is not in active use, with no logged in users, the background service will continue to synchronize data with the server.
	Exception process notification if system is offline	Email notifications will enable configurable alerts to admins upon observed service outage.

#### Section 4, Subsection 4.9 - Secure Temporary DL/ID

Section 4, Subsection 4.9.1 - Vendor solution should produce a secure temporary driver's license with the applicant's image and signature.

#### Vendor Response:

Our proposed solution complies.

Our solution provides for the printing of temporary DL/ID documents at the end of a successful enrollment and data capture process. The secure temporary driver's license will be designed specifically for WVDMV and will include the applicant's image and signature.

Once the operator has successfully captured the required photos, signature, documents, and all business rules have been fulfilled, the solution triggers the printing of the interim DL/ID from the capture workstation. The temporary DL can easily be reprinted using the solution's web portal from the capture station or another PC with the required web browser and printers installed.

Section 4, Subsection 4.9.2 - Vendor solution should print a temporary DL/ID from the Vendor's image and signature capture workstation or from a Vendor web application accessed from the Agency's workstations.

#### Vendor Response:

Our proposed solution complies.

Our solution provides for the printing of temporary DL/ID documents at the end of a successful enrollment and data capture process. Once the operator has successfully captured the required photos, signature, documents, and all business rules have been fulfilled, the solution triggers the printing of the interim DL/ID from the capture workstation. The temporary DL can easily be reprinted using the solution's web portal from the capture station or another PC with the required web browser and printers installed.

**Section 4, Subsection 4.9.3 If the print request is triggered from the ICW, the printing of the temporary DL/ID should be automatic and should not require employee action.**

**Vendor Response:**

Our proposed solution complies.

Our solution for WVDMV provides for the printing of temporary DL/ID documents at the end of a successful enrollment and data capture process. Once the operator has successfully captured the required photos, signature, documents, and all business rules have been fulfilled, the solution triggers the printing of the interim DL/ID from the capture workstation. If WVDMV desires, the Windows print dialogue box on the workstation can be suppressed so employee action is not required.

The temporary DL can easily be reprinted using the solution's web portal from the capture station or another PC with the required web browser and printers installed.

**Section 4, Subsection 4.9.4 - In event of a printing error, the Vendor solution should include a function for reprinting the temporary DL.**

**Vendor Response:**

Our proposed solution complies.

The temporary DL can easily be reprinted on the solution's web portal from the capture station or from another PC with the required web browser and printers installed.

**Section 4, Subsection 4.10 - Consumables for Secure Temporary DL**

**Section 4, Subsection 4.10.1 - Vendor should provide a system for electronically ordering and tracking the secure paper stock for use in each of the Agency's 27 locations.**

**Vendor Response:**

Our proposed solution complies.

Our proposed solution will generate a report reflecting issuance count by location on a weekly basis for the first six months. After the first six months the report will be run the first of each month. All consumable orders would be shipped out with 24 hours of receiving the order.

For emergency orders, a support phone number will be set up for WVDMV and email monitored for orders. All emergency orders would be shipped either the same day as the order is received or by Noon Eastern the following morning via Next Day Air.

---

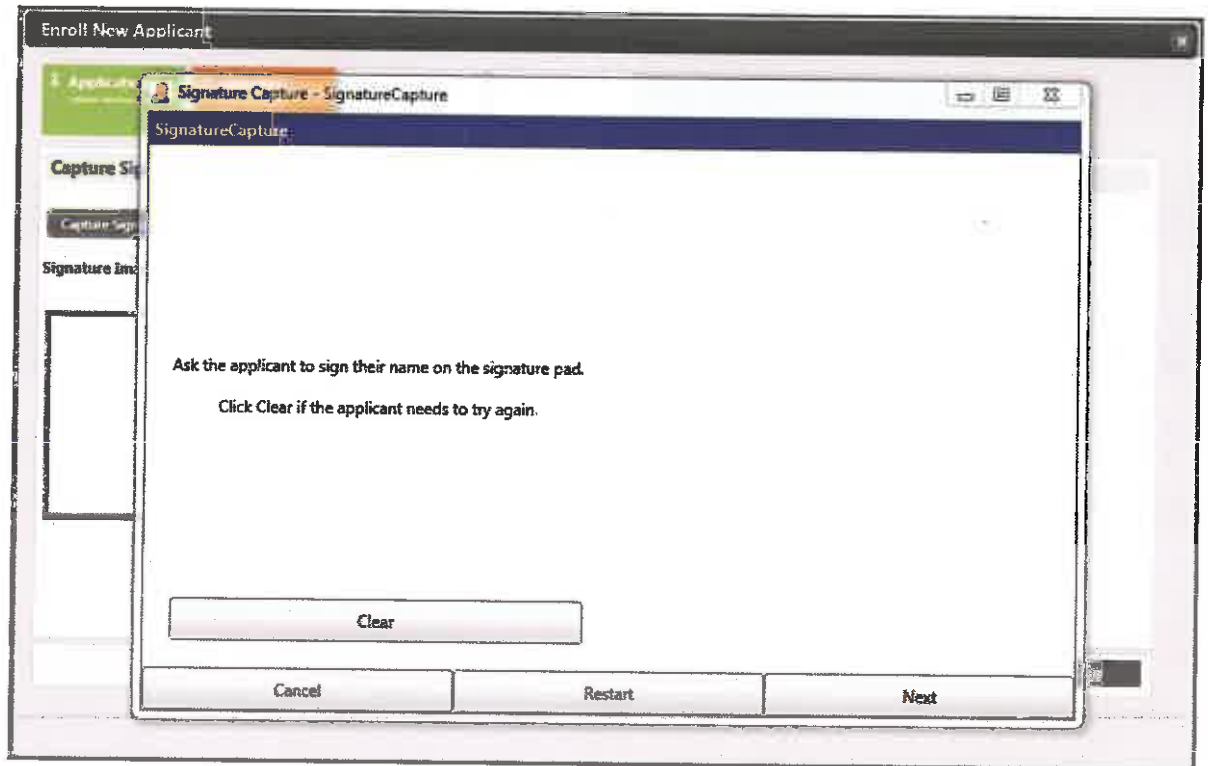
#### Section 4, Subsection 4.11 - Signature Capture

Section 4, Subsection 4.11.1 - Vendor solution should allow for the capture of a true representation of the applicant's written signature.

Our proposed solution complies.

When the signature capture process is initiated, the following will occur:

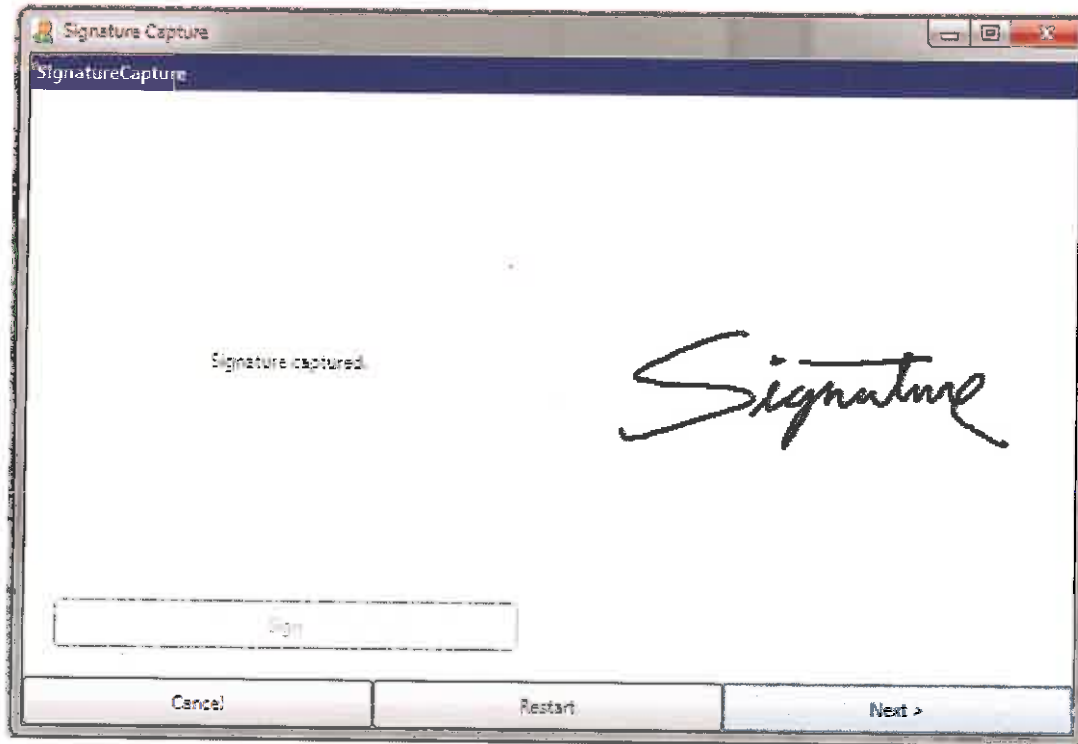
- The signature pad will be automatically initialized and the 'Signature Capture Screen - 1' will be displayed.
- The signature pad captures the applicant signature from the signature pad and displays it in the 'Signature Image' box in true representation of the applicant's written signature.

**SIGNATURE CAPTURE SCREEN – 1**

The first Signature Capture screen is displayed while the customer is signing the digital signature pad. The signature pad will be activated when this screen is displayed.

- Click 'Clear' to clear the current signature displayed on the signature pad, allowing the customer to re-sign
- Click 'Next' to capture the digital signature when the customer has finished signing the signature pad and move to the 'Signature Capture – 2' screen
  - The signature pad will be deactivated after the signature is captured
- Click 'Cancel' to cancel the signature capture and return to the 'Capture Signature' screen
  - The signature pad will be deactivated
- Click 'Restart' to restart the signature capture process
  - The signature pad will be re-activated

The second Signature Capture screen displays the captured digital signature.

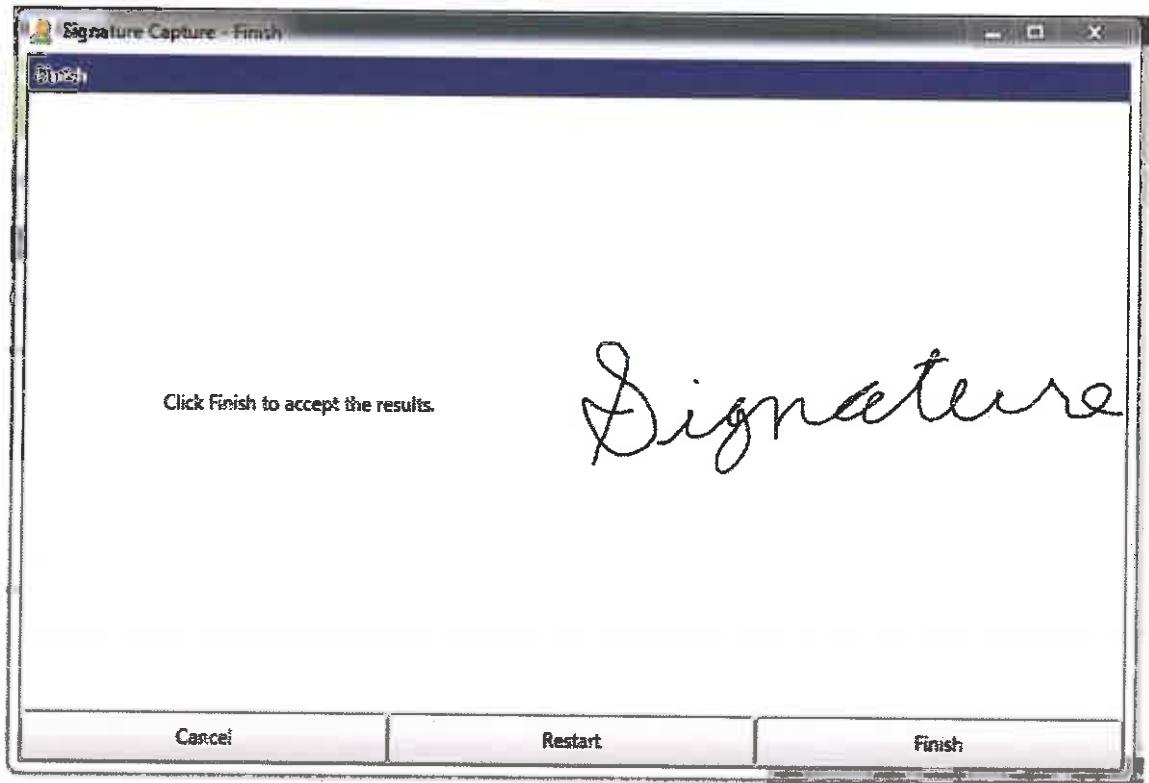


**Actions:**

- Click 'Cancel' to cancel the signature capture and return to the 'Capture Signature' screen
  - Click 'Restart' to restart the signature capture process
  - Click 'Next' to move the 'Signature Capture Finish' screen

### SIGNATURE CAPTURE FINISH SCREEN

The Signature Capture screen allows the user to validate acceptance of the captured digital signature.



#### Actions:

- Click 'Cancel' to cancel the signature capture and return to the 'Capture Signature' screen
- Click 'Restart' to return to the 'Signature Capture - 1' screen and restart the signature capture process
- Click 'Finish' to return to the 'Capture Signature' screen and proceed to the next step in the work flow.

## VERIFY CAPTURED SIGNATURE

Enroll New Applicant

1 Application 2 Signature 3 Photo 4 Review

**Capture Signature**

Capture Signature

Signature Image

Signature

Previous Next Cancel

### Actions:

- Click 'Previous' to move to the 'Validate Application Details' screen
- Click 'Next' to move to the 'Capture Photo' screen
- Click 'Cancel' to return to the 'Applications for Enrollment Queue' screen

**Section 4, Subsection 4.11.2 – Vendor solution should allow applicant to clear and sign again. Vendor Response:**

Our proposed solution complies.

A Restart button is displayed to both the operator and applicant and can be used to clear the pad and allow the applicant to sign again as necessary.

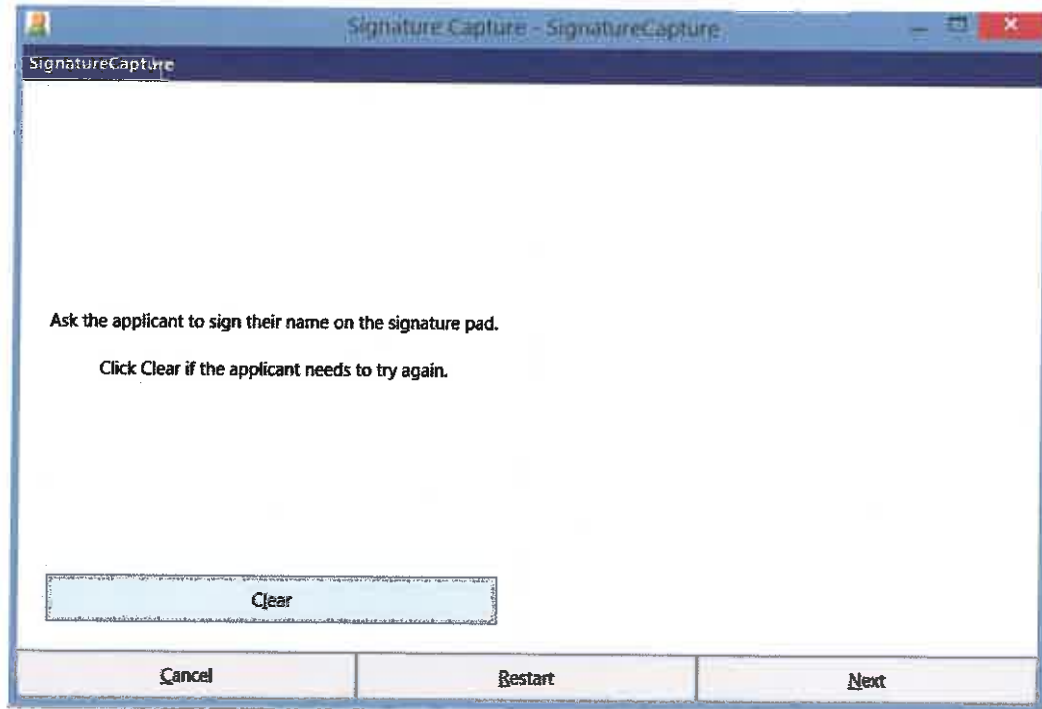


Section 4, Subsection 4.11.3 - Vendor solution should display a live signature on the workstation for the employee to view.

#### Vendor Response:

Our proposed solution complies.

The operator can see the signature live as it is being captured.



The 'OK' and 'Clear' buttons are displayed on the signature pad to allow users to clear or accept the signature.

The 'Restart' button clears the display and the display on the signature pad, and allows the applicant to sign again.

---

Section 4, Subsection 4.11.4 - Vendor solution should allow employee to freeze and accept signature on the workstation, over-riding the clear selection on the signature pad.

---

**Vendor Response:**

Our proposed solution complies.

The signature is captured when the operator clicks 'Next' or 'Finish.' The 'Clear' button on the signature pad itself is overridden at this point and the signature that has been captured at this point is stored with the record.

---

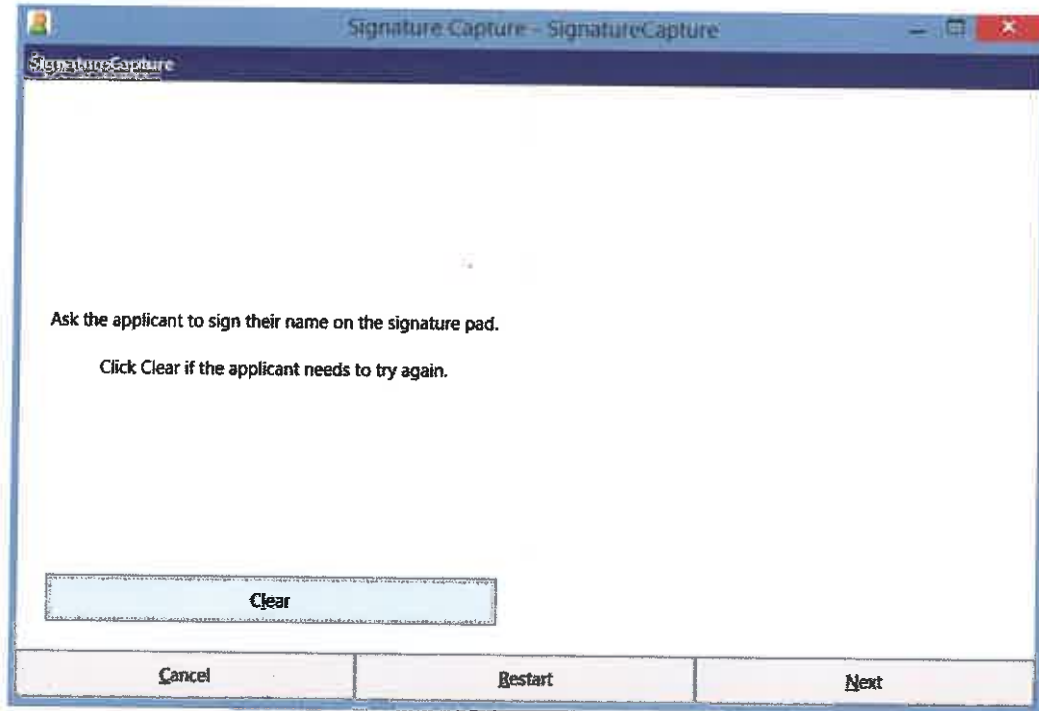
Section 4, Subsection 4.11.5 - Vendor solution should allow employee to clear signature to allow the applicant to sign again.

---

**Vendor Response:**

Our proposed solution complies.

A 'Restart' button is displayed on the signature pad to allow users to clear the signature.



**Actions:**

- Click 'Cancel' to cancel the signature capture and return to the 'Capture Signature' screen
- Click 'Restart' to restart the signature capture process
- Click 'Next' to move the 'Signature Capture Finish' screen.

---

Section 4, Subsection 4.11.6 - Vendor solution should allow employee to select "Unable to Sign" for those applicants who are unable to provide a signature.

---

**Vendor Response:**

Our proposed solution complies.

A check box on the form allows the operator to select 'Unable to Sign.'

---

Section 4, Subsection 4.11.7 - Vendor solution should allow for the display and recording of responses to questions prompted on the signature capture device.

---

**Vendor Response:**

Our proposed solution complies.

Questions displayed to the applicant and the answers captured are part of our proposed solution for WVDMV. Customized questions will be displayed on the signature pad for the applicant to answer. These answers will be stored in the database and are retrievable in receipt and/or report forms. For example, applicant information related to the Motor Voter application process is collected and stored through the signature capture device and solution software.

#### Section 4, Subsection 4.12 - Credential Issuance System (CIS) Objectives

Section 4, Subsection 4.12.1 - Vendor should describe how their proposed solution will handle image and data retrieval for business related inquiries. This description should include:

4.12.1.1 How wildcard searches can allow for all data elements, including first character searches. Search results should be returned in a format that allows for easy sorting and selection of individual records to view.

Our proposed solution complies.

The operator can enter search criteria including a wild card character into any of the fields shown on that particular screen. The results can be sorted by clicking on the headers of any of the fields and dynamically toggling between ascending and descending for the field that was chosen.

For example, clicking on the 'Last Name' header below would sort the results by the last name, toggling between ascending and descending order on each click of the 'Last Name' field header.

Create Date	Cust No.	Lic ID	Last Name	First Name	Type
06/22/2017 11:33:45	0000000	0000000	Thompson	Mary	1%
06/22/2017 04:24:54	0000000	0000000	Anderson	James	14%
06/22/2017 04:25:06	0000000	0000000	James	James	3%
06/22/2017 04:25:08	0000000	0000000	James	James	1%

Showing 1 to 4 of 4 entries

4.12.1.2 How the application can allow for easy navigation between the search results list, individual detail records, and back to the search results list without searching again.

Our proposed solution complies.

To see the detail of any particular record displayed in the search results, the operator clicks on the relevant record. The record details are displayed as appropriate for the process the operator is performing.

The screenshot shows the 'Enrollment' screen in the Veridos system. It features a search bar at the top with a dropdown menu set to 'DL Number' and a search button. Below the search bar is a table with columns: Last Name, DL Number, First Name, Date of Birth, Address, City, and DL Class. The table contains 10 rows of data. At the bottom of the table, it says 'Showing 1 to 10 of 10 entries'. Below the table, there is a label 'Select a row and click Update:' followed by two buttons: 'Update Applicant Data' and 'New Applicant'.

Last Name	DL Number	First Name	Date of Birth	Address	City	DL Class
McCooper	OR521987	James	1954-12-27	1240 Oregon Ave	Salem	Oregon
Drake	OR123123	Donald	1964-12-04	2143 Main	Salem	Oregon
Jenkins	OR12313	Bob	1966-01-10	111 Iron Road	Portland	Oregon
Paulson	OR23422	Jenny		1231 Star Rd		
Dua	OR324324	Nancy	1954-12-19	1231 Main	Portland	Oregon
Anderson	OR325745	Paula		234 Fox Rd		
Jackson	OR43213	Martha	1959-12-14	42345 First Lane	Salem	Oregon
Harrison	OR44444	Marvin	1964-12-14	123 Happy Street	Portland	Oregon
Hillman	OR88888	Andy	1954-12-14	444 Happy Street	Salem	Oregon
Anderson	OR99999	Doug	1964-12-06	333 Main St	Salem	Oregon

4.12.1.3 How the record detail screen can default to display data for the most recent issuance but allow selection of detail for historical issuances.

#### Vendor Response:

Our proposed solution complies.

The proposed solution allows an operator to see the current data from the selected record after selecting it from the search results. The fields display will be determined during the project planning phase in collaboration between Veridos and WVDMV. The 'Credential History' button displays a list of all credentials which have been issued to the specified customer and the details of the selected credential from the list.

The 'Credential History' button can be access both from the 'Application' screen and the facial image capturing 'Photo' screen, as shown below.

#### VALIDATE APPLICATION DETAILS SCREEN

The screenshot shows the 'Enroll New Applicant' window with the 'Validate Application Details' screen. The 'Credential History' button is circled in red.

**Enroll New Applicant**

**1 Application** **2 Photo** **3 Review** **4 Complete**

**Validate Application Details**

**Driver Photograph**

**Application Details**

**Address**

**More Photo Required**

**Signature Required**

**Credential History**

**Next** **Cancel**

Application Details	
Customer ID	11111111
Assurance ID	11111111
DOB	11/11/11
First Name	John
Date of Birth	11/11/11
Card Holder	John Doe
Expire Date	11/11/11
Issue Date	11/11/11
Renewal Date	11/11/11
License Class	1
Endorsement	1
Restrictions	1
Gender	1
Height	1.11
Weight	111
Eye Color	111
Complexion	1
Version	1
Order ID	11111111
Order ID Date	11/11/11
Order ID	11111111
Order ID Date	11/11/11

Address	
Address Line 1	11111111
Address Line 2	11111111
City	11111111
State	11111111
Zip Code	11111111


## CAPTURE FACIAL IMAGE SCREEN

The screenshot shows a software window titled "Enroll New Applicant". At the top, there are four colored tabs: 1. Application (green), 2. Enrollment (green), 3. Photo (orange), and 4. Review (white). The "Photo" tab is currently selected. Below the tabs, the main area is titled "Capture Facial Image". Under this title, there are two buttons: "Take Photo" and "Cancel Photo". The "Cancel Photo" button is circled in red. Below the buttons, there are three sections: "New Photograph", "On File Photograph", and "Attributes". The "New Photograph" section contains a large, empty white square. The "On File Photograph" section contains a small, square portrait of a young man with dark hair. The "Attributes" section is currently empty. At the bottom right of the window, there are three buttons: "Previous", "Next", and "Cancel".

**Credential History**

Customer:

Date	Time	Issuance ID	Location	Flag	Status
08/22/2017	04:25 AM	11123478	125	0	Blank
08/22/2017	04:24 AM	11123477	125	0	Blank

  
*Signature*  
**APPROVED**

Anderson, James	Heading:	Driver License
345 Elm Street	Class:	C
Apt 17	Endorsements:	HZ
Portland OR, 55101	Restrictions:	N
	DOB:	1991-09-21
	Sex:	M
	Height:	67
	Weight:	220
	Expire Date:	2020-02-03

Credential Action:

**CREDENTIAL HISTORY DIALOG**

An operator can see the different data from the previous credentials by selecting it from the list which is sorted by date with the newest on the top.

**Section 4, Subsection 4.12.2 - Vendor should describe how their proposed solution will recover after power outages or communication failures. This description should include:**

**4.12.2.1 How in-process transactions in system queues will be able to restart.**

Our proposed solution complies.

Our solution is designed to fully recover after power outages or communication failures. The queues are all managed at the server level during online communications. When power is restored and the system comes back up, and the operator logs in they will see all of the records in each queue that are ready to be processed and also those that haven't been fully completed. The operator can then choose the records they wish to work on and process as they were before the power outage, and complete all remaining steps.

**4.12.2.2 How the system will roll back, if a transaction cannot be restarted.**

Our proposed solution complies.

The proposed system does not update the system of record databases until the transaction is complete. In the event that a transaction is not able to be completed, the data for that specific record in the main datastore will not have been altered.

**4.12.2.3 How pending data will be stored locally and uploaded to the image server, once power or communication is restored.**

**Vendor Response:**

Our proposed solution complies.

Secura uses a built in store and forward architecture, and stores the data temporarily and securely to ensure it is not lost. It then transmits the data to the long-term data storage location(s). Once the record is processed and the data is successfully saved into the long-term storage solution, Secura automatically deletes it from its internal working database. This includes ALL demographic and image data.

The automatic and verifiable removal of cardholder data and other PII, when no longer required to complete a transaction, perform a function, or produce cards, is a core feature of our information systems. Deletion of data based on industry and client retention limits is regularly performed and audited to meet client commitments and to satisfy the requirements of our multiple security certifications.

---

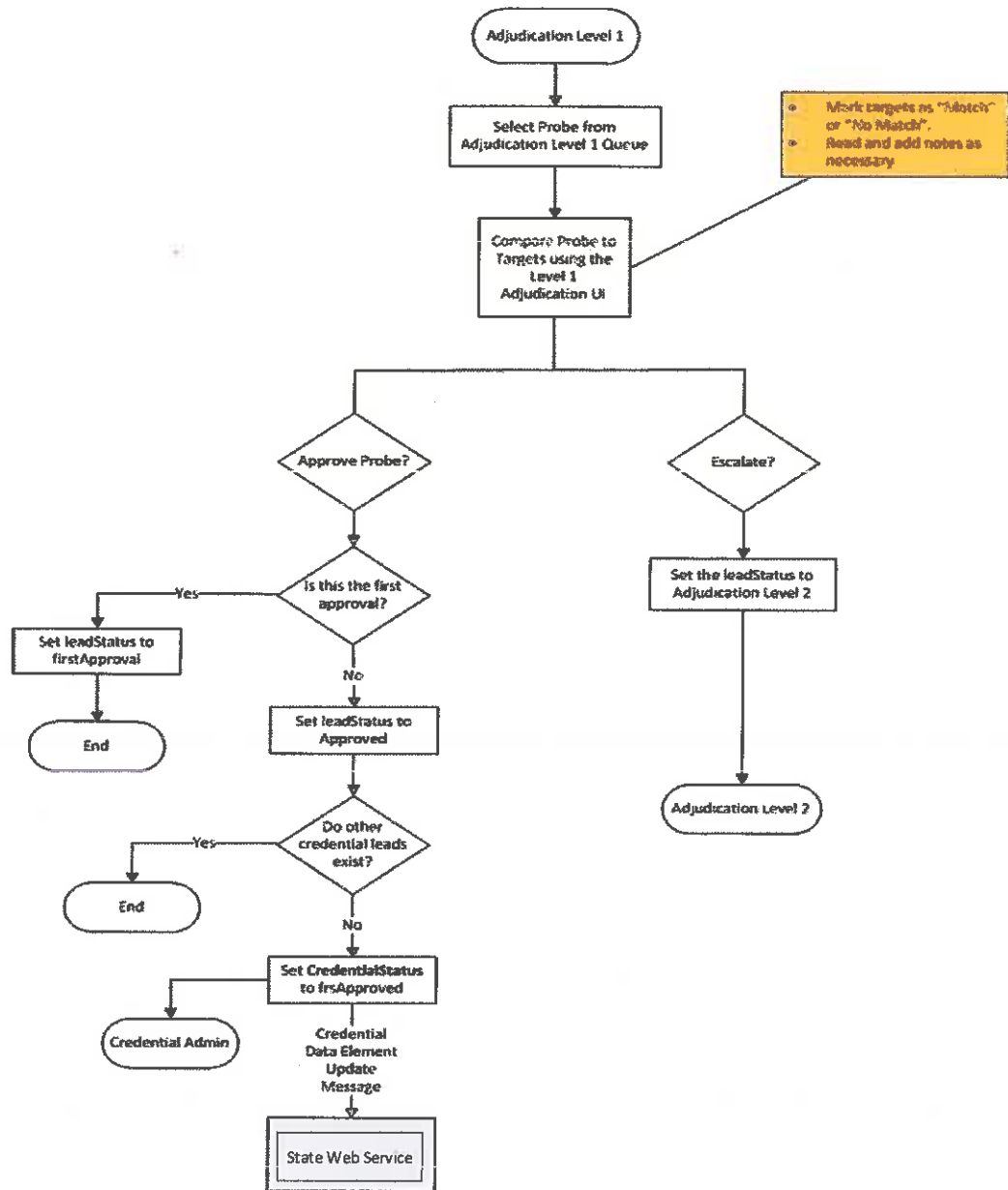
Section 4, Subsection 4.123 - Vendor should describe how their proposed solution will handle Review and Fraud Case Management. This description should include:

---

4.12.3.1 How the solution can provide a multi-tiered workflow for the manual review of match and non-match records, including priority queues,

Our proposed solution complies.

Once the system has detected a potential match for a record during the enrollment process, the system routes that record to the adjudication queues which are used for the manual review of the records. This flow is shown in the diagram below.



Records that are set for expediting will follow the same process, but in the expedited queues which allow the operators to easily identify records that require immediate processing.

The level 1 adjudication queue is used for:

- i) Displaying the queue of 1:N and 1:R leads which require level 1 adjudication

- ii) Displaying the photo and demographic details for the probe and target(s) of the selected lead
- iii) Viewing the probe credential history
- iv) Marking the target photos as 'Match' or 'No Match' to the probe photo
- v) Adding notes to the probe and target(s) customer records
- vi) Approving or Escalating the lead to the 'Adjudication Level 2' workflow

## USER INTERFACE SCREENS

### ADJUDICATION LEVEL 1 QUEUE

Create Date	Cust No	Iss ID	Last Name	First Name	Type
06/22/2017 04:51:45	11113479	11113479	Thompson	Mary	1:N
06/22/2017 04:24:58	11113477	11113477	Anderson	James	1:N
06/22/2017 04:29:06	11113477	11113478	James	Harold	1:N
06/22/2017 04:29:06	11113477	11113478	James	Harold	1:N

The Adjudication Level 1 Queue contains the credential applications that have failed the Secura FRS 1:N or 1:R comparison and have not been adjudicated by the current user (Level 1 Adjudicator). If the current operator escalates the application for further adjudication, it will then be shown in the Adjudication Level 2 Queue. If the current operator approves the application and no other level 1 user has adjudicated the application yet, it will no longer be shown to the current operator in the Level 1 Queue, but still remain at level 1 and visible to other Level 1 Adjudicators. Once another Level 1 Adjudicator either approves or escalates the application, it will then no longer appear in the level 1 queue.

Once a record is selected an operator is presented with the following screen:

## ADJUDICATION LEVEL 1 DETAILS

Probe Details	Target Details
<p>Customer No: 11123477 Last Name: James First Name: Harold Date of Birth: 1993-09-21</p> <p>Heading: Driver License Issue Date: 2015-02-03 Service Location: 123 Station User ID: smfhr</p>  <p>Signature</p> <p>Insurance ID 11123478 Lead Type A-M</p> <p>Notes Aug 25, 2017 7:12:16 PM: ss : Adjudication Level 1 note</p> <p>New Note (Max 255 Characters)</p> <p>Save Note</p> <p>History Escalate Approve Cancel</p>	<p>Showing Target 2 of 2</p> <p>Customer No: 10123478 First Name: Mark Last Name: Nelson Date of Birth: 1993-09-21</p> <p>Heading: Driver License Issue Date: 2015-02-03 Service Location: 456 Station User ID: jonest</p>  <p>Signature</p> <p>Insurance ID 10123478 Match Score 1.0</p> <p>Notes</p> <p>New Note (Max 255 Characters)</p> <p>Save Note</p> <p>Target Filter: <input checked="" type="radio"/> All <input type="radio"/> Matches <input type="radio"/> Non Matches</p> <p>Match No Match First Prev Next Last</p>

Credential applications to be adjudicated at Level 1 require approvals by two Level 1 Adjudicators to be approved by the Secura FRS. The 'Match/No Match' settings of the first adjudicator are not seen by the second adjudicator. The exact fields of data to be shown on these screens is determined during the project planning stage in collaborative meetings between Veridos and WVDMMV.

An Operator can use the navigation buttons in the lower left hand corner to browse through each of the potential matches before determining to either approve or escalate the lead. Each potential match must be set to 'non match' before a record can be approved.

## INVESTIGATION QUEUE

**Search Criteria**

ISSUANCE ID:  CUSTOMER NUMBER:  LAST NAME:  FIRST NAME:

**Results**

Create Date	Cust No.	ID ID	Last Name	First Name	Type
08/22/2017 04:06:21	10123788	10123788	Stevens	Cesar	1:N
08/22/2017 04:12:18	10123787	10123786	Bauman	Linda	1:N
08/22/2017 04:21:08	11123477	11123476	James	Harold	1:N & 1:R

Showing 3 of 3 results

## INVESTIGATION DETAILS SCREEN

The Investigation Details Screen displays the details of the 1:N and 1:R leads that exist for the selected credential.

**Probe Details**

Customer No: 10123477  
Last Name: James  
First Name: Linda  
Date of Birth: 1981-09-21

Headings: Driver License  
Issue Date: 2015-04-10  
Service Location: 123  
Status: User ID: 12345

**Examiner File**

Person ID: 10123476  
Adjudication Level: Pending Appeal

**Notes**

Aug 22 2017 10:18 AM: ADJUDICATION LEVEL 2 Note

**Target Details 1:1:N**

Customer No: 10123478  
Last Name: Stevens  
First Name: Cesar  
Date of Birth: 1992-10-21

Headings: Driver License  
Issue Date: 2015-04-10  
Service Location: 123  
Status: User ID: 12345

**Examiner File**

Person ID: 10123479  
Adjudication Level: Pending Appeal

**Notes**

Aug 22 2017 10:18 AM: ADJUDICATION LEVEL 2 Target Note

**Target Details 1:1:R**

Customer No: 11123477  
Last Name: James  
First Name: Harold  
Date of Birth: 1972-09-22

Headings: Driver License  
Issue Date: 2015-04-10  
Service Location: 123  
Status: User ID: 12345

**Examiner File**

Person ID: 11123477  
Adjudication Level: Pending Appeal

**Notes**

Aug 22 2017 10:18 AM: ADJUDICATION LEVEL 2 Target Note

## Actions:

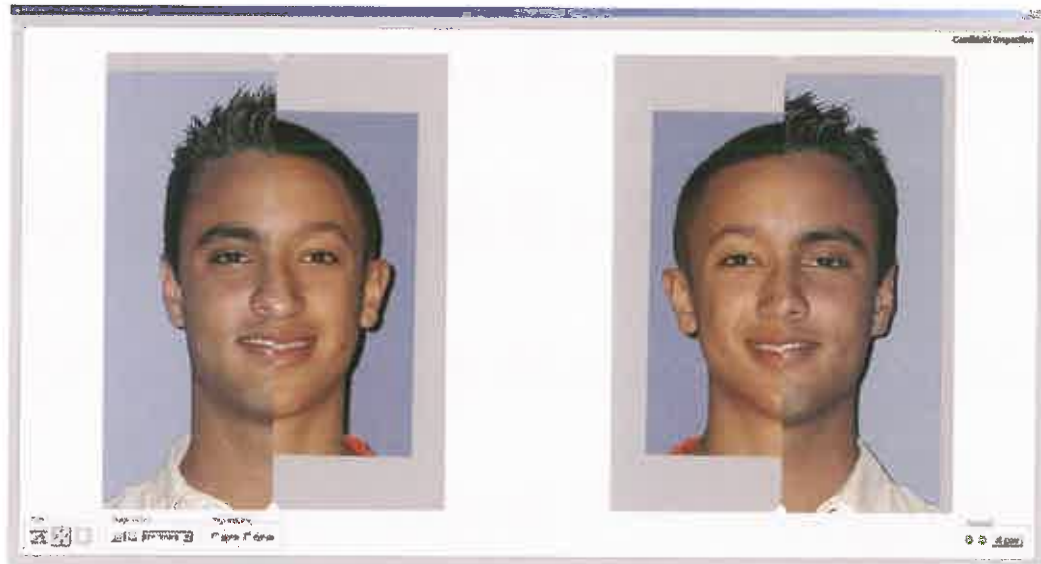
- Click 'Examiner File' to create a specially formatted file identifying the current credential (Probe or Target) which can be opened in the FaceVACS-DBScan Examiner application to perform in-depth analysis of the credential photo (refer to the description of the FaceVACS-DBScan Examiner Screens in the Adjudication Level 2 section)

Veridos' FRS solution's Examiner Mode provides WVDMV with an interface to display all required information to complete a manual verification.

The potential matches are displayed below, with the probe image ranked from highest potential to lowest, left to right. The individual score is shown below each potential match.



The operator can then select a potential match to review more in-depth, once chosen the probe and the potential match are shown in the inspection screen.



The operator can use the overlay feature to get a better view if the potential match is indeed something that requires further investigation using the overlay view and measuring specific points like from the tip of the nose to a distinguishing mark.



---

**4.12.3.2 How all expedited records that have matches can go to a separate priority queue for same day manual review.**

Our proposed solution complies.

Expedited records will have their own adjudication and investigative queues with the same flows, but will separate the records that need to be processed quickly to make is easy for an operator to prioritize their work. An operator will simply click on the expedited tab to see the records in that particular queue of each step of the process.

---

**4.123.3 How all match and non-match records can display the facial image, signature and demographic information formatted in such a way as to highlight the differences in data between the records.**

---

**Vendor Response:**

Our proposed solution complies.

Secura has the option to highlight text that differs from probe record as a way to make it easier for operators to distinguish the differences in the records they are reviewing as shown in the screenshot below.

The screenshot displays a side-by-side comparison of two identity records in the Veridos Identity Solutions software. The interface is divided into two main panels: 'Probe Details' on the left and 'Target Details' on the right. Both panels show a photo of a man, a signature, and personal information including Customer No. (10123477 for Probe, 10123478 for Target), First Name (Jason), Last Name (Hartley), Date of Birth (1993-02-21), Heading (Driver License), Issue Date (2015-02-03), Service Location (123 for Probe, 456 for Target), and Station User ID (jason). The Target panel also displays an 'Issuance ID' (10123478) and a 'Match Score' of 1.0. Below the photos, there are 'Notes' sections with a text area and a 'New Note (Max 255 Characters)' field. At the bottom, there are buttons for 'History', 'Locate', 'Approve', 'Cancel', 'Match', 'No Match', 'First', 'Prev', 'Next', and 'Last'. A 'Target Filter' section at the bottom right shows 'All Matches' selected.

Section 4, Subsection 4.12.4 - Vendor should describe how the proposed solution will manage manual image enrollment applications. This description should include:

4.12.4.1 How the Vendor solution will allow images that were not captured by the image and signature capture workstation to be uploaded to the system for comparison against images in the database.

Our proposed solution complies.

Secura has the option for uploading images from files such as JPG, BMP, or other common file types for live photo capture. This can be provided to all operators or only certain operators that have a special privilege set in their access control group.

**4.12.4.2 How the system will allow images of various file types to be uploaded into the manual enrollment application, including JPG, GIF, TIF, PNG, and BMP.**

Our proposed solution complies.

Secura allows for the uploading of image files as well as live image capture. An operator that has access to this feature would be shown a button on the display that say Manual Upload. The system would prompt the user to select the image they would like to associate with the record and then the system would check in the image for ICAO compliance. The same cropping and image adjusting features can be provided for the manual uploading of files as is provided for the live photo capture process.

**4.12.4.3 How the system will allow user to choose to keep uploaded images permanently enrolled in the facial recognition system with appropriate demographic data.**

**Vendor Response:**

Our proposed solution complies.

Secura allows for the uploading of image files as well as live image capture. An operator that has access to this feature would be shown a button on the display that say Manual Upload. The system would prompt the user to select the image they would like to associate with the record and then the system would check in the image for ICAO compliance. The same cropping and image adjusting features can be provided for the manual uploading of files as is provided for the live photo capture process.

**Section 4, Subsection 4.12.5 - Vendor should describe the applications reporting capabilities, including description and examples of all standard system reports. This description should also include:**

Our proposed solution complies.

The proposed enrollment software, Secura, includes an Administration User Interface that supports standard system reports. The following DPL reports are readily accessible to administrators:

- Transaction by Operator Report
- Transaction by Workstation Report
- Transaction by DLO
- Transaction by Customer Report
- Transaction by Date Report
- Failed Fingerprint Check Report
- Failed Facial Recognition Report
- Failed 3rd Party Vetting Report

Once records are batched for card production, they are strictly accounted for and monitored. The following events are monitored and status is provided to WVDMV, either in real-time or at a pre-defined time:

- Cards stock manufactured status
- Transmitting DL/ID card requests (batches or web requests) success and failure
- Data balancing status (received batch quantity does not balance) failure and success
- Data format status failure and success
- Data requests rejected
- Transfer stock status (for example, to DRP location)
- Pull request status failure and success
- Card damaged and its remake status
- Cards QA status
- Cards produced status
- Cards packages mailed /shipped status (include quantity and dates)
- Expedited requests status
- Request on Hold status
- Requests purged/destroyed status

The Secura Report User Interface supports:

- 1) Entering reporting search criteria
- 2) Displaying the report in the browser
  - a) Audit Event – Report Viewed

**Reports**

Report Close: Transaction Summary-Monthly [View](#) [Export as PDF](#) [Export as CSV](#) [Print](#)

**Filter:**

Year: 2016 Month: April

Show: 10 entries

Month/Date	Enrollments	Leads Created	L1B Leads Approved	L2B Leads Approved	L2B Leads Escalated	L1B Leads Approved	L2B Leads Approved	L2B Leads Escalated	Claimed Further Investigation
01-04-2016	0	0	0	0	0	0	0	0	0
02-04-2016	0	0	0	0	0	0	0	0	0
03-04-2016	0	0	0	0	0	0	0	0	0
04-04-2016	0	0	0	0	0	0	0	0	0
05-04-2016	0	0	0	0	0	0	0	0	0
06-04-2016	0	0	0	0	0	0	0	0	0
07-04-2016	40	32	6	3	4	4	3	1	0
08-04-2016	0	0	0	0	0	0	0	0	0
09-04-2016	0	0	0	0	0	0	0	0	0
10-04-2016	0	0	0	0	0	0	0	0	0

Showing 1 to 10 of 31 entries

Filter(s):

Start: 2016-03-01 00:00 End: 2016-04-21 23:59

Search: 2016 Mar

Search

SV

Date

Category

Time 00:00

Hour

Minute

Now Done

(All dates will be displayed in the format mm-dd-ccyy. The screens shot examples below may show a different date format.)

- 3) Exporting report data to CSV file
  - a) Audit Event – Report Exported to CSV

	A	B	C	D	E	F	G	H	I	J	K	L
1	Transaction Summary-Monthly											
2	MonthDate	Enroller	Leads	Cred	L1 N-Lead	L2 N-Lead	L2 M-Lead	L1 R-Lead	L2 R-Lead	L2 R-Lead	Cleared	Further Investigation
3	2016-01-04	0	0	0	0	0	0	0	0	0	0	
4	2016-02-04	0	0	0	0	0	0	0	0	0	0	
5	2016-03-04	0	0	0	0	0	0	0	0	0	0	
6	2016-04-04	0	0	0	0	0	0	0	0	0	0	
7	2016-05-04	0	0	0	0	0	0	0	0	0	0	
8	2016-06-04	0	0	0	0	0	0	0	0	0	0	
9	2016-07-04	40	32	6	3	4	4	3	1	1	0	
10	2016-08-04	0	0	0	0	0	0	0	0	0	0	
11	2016-09-04	0	0	0	0	0	0	0	0	0	0	
12	2016-10-04	0	0	0	0	0	0	0	0	0	0	
13	2016-11-04	1	2	0	0	1	0	0	0	0	0	
14	2016-12-04	0	0	0	0	0	0	0	0	0	0	

- 4) Exporting report to PDF
  - a) Audit Event – Report Exported to PDF

Transaction Summary-Monthly									
MonthDate	Enrollments	Leads Created	L1 N-Leads Approved	L2 N-Leads Approved	L2 N-Leads Escalated	L1 R-Leads Approved	L2 R-Leads Approved	L2 R-Leads Escalated	Cleared Further Investigation
01-04-2016	0	0	0	0	0	0	0	0	0
02-04-2016	0	0	0	0	0	0	0	0	0
03-04-2016	0	0	0	0	0	0	0	0	0
04-04-2016	0	0	0	0	0	0	0	0	0
05-04-2016	0	0	0	0	0	0	0	0	0
06-04-2016	0	0	0	0	0	0	0	0	0
07-04-2016	20	32	0	3	3	4	3	1	0
08-04-2016	0	0	0	0	0	0	0	0	0
09-04-2016	0	0	0	0	0	0	0	0	0
10-04-2016	0	0	0	0	0	0	0	0	0
11-04-2016	1	2	0	0	1	0	0	0	0
12-04-2016	0	0	0	0	0	0	0	0	0
13-04-2016	0	0	0	0	0	0	0	0	0
14-04-2016	0	0	0	0	0	0	0	0	0
15-04-2016	0	0	0	0	1	0	0	0	0
16-04-2016	0	0	0	0	0	0	0	0	0
17-04-2016	0	0	0	0	0	0	0	0	0
18-04-2016	2	2	0	0	0	0	0	0	0
19-04-2016	0	0	0	0	0	0	0	0	0
20-04-2016	1	1	0	0	0	0	0	0	0
21-04-2016	0	0	0	0	0	0	0	0	0
22-04-2016	0	0	0	0	0	0	0	0	0
23-04-2016	0	0	0	0	0	0	0	0	0
24-04-2016	0	0	0	0	0	0	0	0	0
25-04-2016	0	0	0	0	0	0	0	0	0
Month: 4									
Year: 2016									
User: ss									
Report Date: 2016-04-29 11:18									

MonthDate	Enrollments	Leads Created	L1 N-Leads Approved	L2 N-Leads Approved	L2 N-Leads Escalated	L1 R-Leads Approved	L2 R-Leads Approved	L2 R-Leads Escalated	Cleared Further Investigation
26-04-2016	0	0	0	0	0	0	0	0	0
27-04-2016	0	0	0	0	0	0	0	0	0
28-04-2016	0	0	0	0	0	0	0	0	0
29-04-2016	0	0	0	0	0	0	0	0	0
30-04-2016	0	0	0	0	0	0	0	0	0
Total	24	37	0	3	0	4	3	1	0

## Audit Reports

The Secura audit reports display information regarding the Secura audit events which occur during the Secura FRS process. The audit entries recorded in the Secura FRS are never purged and are always available for reporting purposes.

Three audit report perspectives are supported:

- Credential – all events related to a specified credential (Issuance ID)
- Customer – all events related to a specified customer ID (all credentials associated with the customer)
- User – all events release to events initiated by the specified user (Secura user name)

Each of the audit reports support the following columns:

- **Logged** – The timestamp of when the event was logged
- **User** – The Secura user associated with the event
- **Issuance ID** – The credential issuance ID associated with the event (when applicable)
- **Customer Number** – The customer number associated with the event (when applicable)
- **Event Type** – The event type of the entry (refer to the Audit Event Type table below)
- **Event Data** – Additional data associated with the event (when applicable)

### Credential Audit Report

The credential audit report shows Secura FRS audit events associated with a specified credential (Issuance ID) over a specified date range. The filter parameters for the credential audit report are:

- **Start Date** – The starting timestamp for entries to include in the report
- **End Date** – The ending timestamp for entries to include in the report
- **Issuance ID** – The credential issuance ID for entries to include in the report
- **Sort Order** – The order to sort the 'Logged' timestamp column (Ascending or Descending)

Logged	User	Issuance ID	Customer Number	Event Type	Event Data
27-07-2016 10:53:10.143	ee	106612	10661	ICAD Complaint	
27-07-2016 10:53:19.707	ee	106612	10661	FRS Enrolled	
27-07-2016 10:53:20.080	ee	106612	10661	is Lead Created	
27-07-2016 11:19:49.563	ssa	106612	10661	Set as Match	Matched Against: Issuance ID: 106611, Customer Number: 1066. Logged From: AdjLevel1Details
27-07-2016 11:19:53.707	ssa	106612	10661	L1 N Lead Escalated	
27-07-2016 11:20:42.300	ssa	106612	10661	Set as No Match	Did Not Match Against: Issuance ID: 106611, Customer Number: 1066. Logged From: AdjLevel2Details
27-07-2016 11:20:56.613	ssa	106612	10661	L2 N Lead Approved	
27-07-2016 11:20:56.630	ssa	106612	10661	Credential Approved	

Showing 1 to 8 of 8 entries

### Customer Audit Report

The customer audit report shows Secura FRS audit events associated with a specified customer over a specified date range. The filter parameters for the customer audit report are:

- **Start Date** – The starting timestamp for entries to include in the report
- **End Date** – The ending timestamp for entries to include in the report
- **Customer Number** – The customer number for entries to include in the report

- **Sort Order** – The order to sort the 'Logged' timestamp column (Ascending or Descending)

**Reports**

Report Query: **Audit Report - Customer**

**Files:**

Start Date:  End Date:  Customer No:  Sort Order: **ASC**

Logged	User	Issuance ID	Customer Number	Event Type	Event Data
27-07-2016 10:53:19.143	oe	106612	10661	ICAD Compliant	
27-07-2016 10:53:19.707	oe	106612	10661	FRS Enrolled	
27-07-2016 10:53:20.080	oe	106612	10661	N Lead Created	
27-07-2016 11:19:42.223	ssa	106612	10661	Credential Accessed	AdLevel1Queue
27-07-2016 11:19:49.583	ssa	106612	10661	Sei as Match	Matched Against Issuance ID 106611, Customer Number 1066, Logged From: AdLevel1Details
27-07-2016 11:19:53.707	ssa	106612	10661	L1 N Lead Escalated	
27-07-2016 11:20:01.473	ssa	106612	10661	Credential Accessed	AdLevel2Queue
27-07-2016 11:20:14.863	ssa	106612	10661	Created Examiner File	Examiner File Created for Probe, Logged From: AdLevel2Details
27-07-2016 11:20:42.300	ssa	106612	10661	Sei as No Match	Did Not Match Against Issuance ID 106611, Customer Number 1066, Logged From: AdLevel2Details
27-07-2016 11:20:56.613	ssa	106612	10661	L2 N Lead Approved	
27-07-2016 11:20:56.630	ssa	106612	10661	Credential Approved	

Showing 1 to 14 of 14 entries

### User Audit Report

The user audit report shows Secura FRS audit events associated with a specified user over a specified date range. The filter parameters for the user audit report are:

- **Start Date** – The starting timestamp for entries to include in the report
- **End Date** – The ending timestamp for entries to include in the report
- **User** – The Secura user ID for entries to include in the report (free form text box) This report only logs audit events created by users in Secura
- **Sort Order** – The order to sort the 'Logged' timestamp column (Ascending or Descending)

The screenshot shows the 'Reports' section of the Veridos application. It includes a search bar with filters for 'Time' (Monday, January 21, 2016) and 'User' (John Doe). Below the search bar is a table with columns: 'Time', 'User', 'License ID', 'Cardholder Name', 'Event Type', and 'Event Date'. The table contains multiple rows of data, including events like 'Report: New Card', 'Report: Card Renewal', 'Report: Card Deactivation', and 'Report: Card Activation'. Each row has a corresponding 'Event Date' and a 'Report' link.

### Summary Reports

The Secura summary reports display daily summary information related to the number of occurrences of Secura audit events which occur during the Secura FRS process.

Four time period perspectives are supported:

- **Date Range** – the start and end date timestamps of the period of interest are entered in the filter criteria

**Filter:**

Start Date: 2016-07-21 00:00:00

End Date: 2016-07-28 23:59:00

- **Monthly** – the start and end date timestamps are set by selecting the year and the month of interest

**Filter:**

Month: January

Year: 2016

- **Quarterly** – the start and end date timestamps are set by selecting the year and the quarter of interest

Filter:

Year: 2016 ▼ Quarter: First ▼

- Yearly – the start and end date timestamps are set by selecting the year of interest

Filter:

Year: 2016 ▼

The last line of each summary report is a 'TOTAL' line containing the sum of each column in the report.

### Enrollment Summary Reports

The enrollment summary report contains columns displaying the number of occurrences for each day of the following events:

- Date – The timestamp of when the event occurred
- Attempted Enrollments – The number of credential enrollment attempted for this day
- Validation: 'Attempted Enrollments' = 'FRS Enrollments' + 'Failed FRS Enrollments'
- FRS Enrollments – The number of successful FRS enrollments for this day
- Validation: 'FRS Enrollments' = 'Passed FRS Checks' + '1N Leads Created'
- Failed FRS Enrollments – The number of failed FRS enrollments (requiring manual FRS enrollment) for this day
- Manual Enrollments – The number of manual FRS enrollment performed for this day
- Passed FRS Checks – The number of credentials which passed the FRS checks immediately following FRS enrollment (no leads generated)
- 1N Leads Created – The number of credential enrollments which generated a 1:N lead for this day
- 1R Leads Created – The number of credential enrollments which generated a 1:R lead for this day
- 1N and 1R Leads Created – The number of credential enrollments which generated both a 1:N and a 1:R lead for this day

Home

Reports

Report Query:

Enrollment Summary - Date Range

View

Export as PDF

Export as CSV

Print

Filter:

Start Date: 2016-07-23 00:00:00

End Date: 2016-07-29 23:59:00

Show	to	columns	Search						
Date	Approved / Escalations	PAS / Escalations	Failed PAS / Escalations	Manual / Escalations	Passed PAS Checks	1:N Leads Created	1:N Leads Escalated	1:N and 1:N Created	
23-07-2016	0	0	0	0	0	0	0	0	
24-07-2016	0	0	0	0	0	0	0	0	
25-07-2016	0	1	1	0	0	0	0	0	
26-07-2016	0	0	0	0	0	0	0	0	
27-07-2016	7	1	0	0	5	2	1	1	
28-07-2016	0	0	0	0	0	0	0	0	
29-07-2016	0	0	0	0	0	0	0	0	
TOTAL	9	7	2	0	5	2	1	1	

Showing 1 to 2 of 2 entries

### N Lead Summary Reports

The N Lead summary report shows a summary of the number of occurrences each day of adjudication events for 1:N leads during the specified time period. This report contains the following columns:

- Date – The timestamp of when the event occurred
- L1 Approved – A 1:N lead at adjudication level 1 has been approved
- L1 Escalated – A 1:N lead at adjudication level 1 has been escalated to L2 status
- L2 Approved – A 1:N lead at adjudication level 2 has been approved
- L2 Escalated – A 1:N lead at adjudication level 2 has been escalated to Investigation status

**Reports**

Report Query: **R Lead Summary - Date Range**

**Filter:**

Start Date:  End Date:

Show: 10 entries

Date	L1 Approved	L1 Escalated	L2 Approved	L2 Escalated	Admin Error	L1 Approved	L1 Escalated Internal Review	L1 Escalated SUI Review
22-07-2016	0	1	1	0	0	0	0	0
23-07-2016	0	0	0	0	0	0	0	0
24-07-2016	0	0	0	0	0	0	0	0
25-07-2016	0	0	2	0	0	0	0	0
26-07-2016	0	0	0	0	0	0	0	0
27-07-2016	0	1	1	0	0	0	0	0
28-07-2016	0	0	0	0	0	0	0	0
29-07-2016	0	0	0	2	0	0	0	0
TOTAL	0	2	2	2	0	0	0	0

Showing 1 to 9 of 9 entries

### R Lead Summary Reports

The R Lead summary report shows a summary of the number of occurrences each day of adjudication events for 1:R leads during the specified time period. This report contains the following columns:

- Date – The timestamp of when the event occurred
- L1 Approved – A 1:R lead at adjudication level 1 has been approved
- L1 Escalated – A 1:R lead at adjudication level 1 has been escalated to L2 status
- L2 Approved – A 1 R lead at adjudication level 2 has been approved
- L2 Escalated – A 1:R lead at adjudication level 2 has been escalated to Investigation status

**Reports**

Report Query: **R Lead Summary - Date Range**

**Filter:**

Start Date:  End Date:

Show: 10 entries

Date	L1 Approved	L1 Escalated	L2 Approved	L2 Escalated	Admin Error	L1 Approved	L1 Escalated Internal Review	L1 Escalated SUI Review
22-07-2016	0	0	0	0	0	0	0	0
23-07-2016	0	0	0	0	0	0	0	0
24-07-2016	0	0	0	0	0	0	0	0
25-07-2016	0	0	0	0	0	0	0	0
26-07-2016	0	0	0	0	0	0	0	0
27-07-2016	0	0	0	0	0	0	0	0
28-07-2016	0	0	0	0	0	0	0	0
29-07-2016	2	2	0	2	0	1	0	0
TOTAL	2	2	0	2	0	1	0	1

Showing 1 to 9 of 9 entries

## Investigation Summary Reports

The investigation summary report contains columns displaying the number of occurrences for each day of the following events:

- Date – The timestamp of when the event occurred
- Investigation Cleared – A credential has had the investigation of 'potential fraud' cleared
- Confirmed Fraud - PROBE – The probe credential in a lead has been marked as 'confirmed fraud'
- Confirmed Fraud - TARGET – A target credential in a lead has been marked as 'confirmed fraud'

**Reports**

Report Query: Investigation Summary - Date Range View Export as PDF Export as CSV Print

Filter:

Start Date: 2016-07-22 00:00:00 End Date: 2016-07-29 23:59:00

Date	Investigation Cleared	Confirmed Fraud - PROBE	Confirmed Fraud - TARGET
22-07-2016	0	0	0
23-07-2016	0	0	0
24-07-2016	0	0	0
25-07-2016	0	0	0
26-07-2016	0	0	0
27-07-2016	0	0	0
28-07-2016	0	0	0
29-07-2016	2	1	1
<b>TOTAL</b>	<b>2</b>	<b>1</b>	<b>1</b>

Showing 1 to 9 of 9 entries

## Management Reports

### Group Permission Report

The Group Permission report shows the complete list of permissions for each group and last update details.

**Reports**

Report Query: User Roles Summary View Export as PDF Export as CSV Print

Filter:

Username	First Name	Last Name	Created On

## Exception Reports

### Special Handling Summary Report

Each of the special handling summary report shows history and status of the credentials which have gone through the special handling screen. This report contains the following columns:

- Created On – The timestamp of when the event was created
- Customer Number – The customer number associated with the event
- Issuance ID – The credential issuance ID associated with the event
- Reason Code – The reason code of why this credential is in special handling
- ICAO Non Compliance Reason – If the reason code is 'Non ICAO', the details non-ICAO details sent when the credential was enrolled
- Issuer Code – The issuer code of the enrollment location from where the credential was enrolled
  - *Note: This will be changed to 'SRVC\_CNTR\_NUM'*
- Action Taken – The action which has been taken (if any yet) to resolve the special handling condition

The screenshot shows the 'Reports' section of the Veridos portal. A dropdown menu is set to 'Special Handling Summary'. Below this, there are fields for 'Start Date' (2016-07-22 00:00:00) and 'End Date' (2016-07-29 23:59:00). A table displays the results with columns: Created On, Customer Number, Issuance ID, Reason Code, ICAO Non Compliance Reason, Issuer Code, and Action Taken. Two rows of data are visible, both showing 'Failed Enrollment' as the reason code and 'Enrolled' as the action taken.

Created On	Customer Number	Issuance ID	Reason Code	ICAO Non Compliance Reason	Issuer Code	Action Taken
26/07/2016 21:51:58	18005	180051	Failed Enrollment		321	Enrolled
27/07/2016 18:00:45	1021	1021	Failed Enrollment		321	Pending Action

Veridos' Online Portal enables WVDMV a self-service capability to query the processing status of individual personalization card orders, as well as to designate specific actions (redirect, pull, hold) for in-process card personalization.

Some of the most common reports queried are listed in the table below.

Report Name	Report Purpose/Description	List of Data Elements contained in Report
Vault DCN Inventory	Vault DCN inventory status for primary & backup sites for all cards which includes new manufactured cards being added to the vault(s)	DCN start # & end #, stock balance, new cards manufactured, cards in use, rejected, destroyed, removed from vault, moved to backup facility or primary facility & totals
Card Production	Monitors the card production volumes from WV receiving the order to the final event status	Orders Received by WV, Successful Pulled broken down by reason, mailed broken down by reason, Final Production Failure broken down by

Report Name	Report Purpose/Description	List of Data Elements contained in Report
		reason, total destroyed & percentage, total purged & percentage for each WV State, card, run type and for a date (day, week, month, quarter, year or defined period)
Spoilage	To provide a total number of spoiled cards by card type and WV during any point of the card lifecycle	DCN, Card Type, Date/Time
Lost Card	Listing of all cards lost  This is an e-mail alert.	DCN, Card Type, Date/Time, BatchID
Personnel attendance by shift	Listing of personnel attendance	Name, User ID, Shift, Attendance, date/time
Delivery Component	Listing of delivery components	Delivery Component, Quantity, Description, date/time
Daily Order Files	Used to track order batch filenames, corresponding request batch filename, order batchID, order record count and Card Production Centre Status	Request batch filename, order batch ID, order record count, date/time
Access Control Logs	Lists all accesses for computer and compartmental areas	Date/Time, User ID, Access, Computer, Compartmental area
Card Production Failure	Lists all item orders/cards that have failed and ensure that every DCN is accounted for and items.	DCN, Card Type, Date/Time, Failure Type
Reconciliation Invoice	Provides a monthly total broken down by each week for each WV card, for mailed, pulled & reprints. Totals for all cards, GST and grand total.	DCN, Time, # of cards charged with associated cost broken for the month and weeks within the month
Detailed Reconciliation Invoice (by day)	Provides a detailed listing for reconciliation that is broken down by week and then by day with the same details as the Reconciliation Invoice.	Same as above and broken down by week, day and individual DCN
Pulled Status	To provide a listing of all pulled requests from the web-based application and status	DCN, Card Type, Date/Time, Status
Daily Merge Failures	Used to track image merge failures.	File type, DL/ID, Spare #, value, date mismatch and status, grand total of failures
Inventory Usage Report by card	Track full inventory and usage	To provide a listing broken down by card that shows the inventory items and quantities used for processing item orders
Unsuccessful Print/Reprint Requests	Track all unsuccessful requests for reconciliation	Listing of all reprints that are processed at no charge

Report Name	Report Purpose/Description	List of Data Elements contained in Report
Backlog Item Orders	This is an e-mail alert for tracking all backlog items	Listing of all outstanding item orders that have not been processed in the required timeframe
Inventory Planner - collateral	Weekly (or flexibly set by basis) report providing collateral inventory status	Listing all collateral items, Qty, 90 day usage
Inventory Planner - Plastics	Weekly (or flexibly set by basis) report providing plastics inventory status	Listing all plastic items, Qty, 90 day usage

**4.12.5.1 How, in addition to any standard reports the solution offers, proposal should allow Agency to add a determined number of custom reports at no additional charge over the life of the contract.**

Our proposed solution complies.

Veridos will work with WVDMV to determine if additional reports are required to support WVDMV's business and administrative services. These custom reports will be included with our proposed solution over the life of the contract at no additional charge.

**4.12.5.2 How can the Agency generate custom ad hoc reports?**

Our proposed solution complies.

The system provides a flexible interface that allows operators to choose various items included data ranges and other search criteria to create ad hoc reports as needed.

The screenshot displays the 'Reports' section of the Veridos system. At the top, there is a 'Report Query' dropdown set to 'Audit Report - Credential', with buttons for 'View', 'Export as PDF', 'Export as CSV', and 'Print'. Below this is a 'Filter' section with input fields for 'Start Date' (2016-07-20 00:00:00), 'End Date' (2016-07-27 23:59:59), 'Issuance ID' (106612), and 'Sort Order' (ASC). The main area shows a table of results with columns: 'Issued', 'User', 'Issuance ID', 'Customer Number', 'Event Type', and 'Event Info'. The table contains 8 rows of data, with the last two rows highlighted in red. The first row is '2016-07-20 10:55:18 143' issued by 'aa' for '106612' to customer '10661', with event type 'ICAO Complaint'. The second row is '2016-07-20 10:55:18 143' issued by 'aa' for '106612' to customer '10661', with event type 'FRS Enrolled'. The third row is '2016-07-20 10:55:18 143' issued by 'aa' for '106612' to customer '10661', with event type 'N Lead Created'. The fourth row is '2016-07-20 10:55:18 143' issued by 'aa' for '106612' to customer '10661', with event type 'Set as Match'. The fifth row is '2016-07-20 10:55:18 143' issued by 'aa' for '106612' to customer '10661', with event type 'L1 N Lead Escalated'. The sixth row is '2016-07-20 10:55:18 143' issued by 'aa' for '106612' to customer '10661', with event type 'Set as No Match'. The seventh row is '2016-07-20 10:55:18 143' issued by 'aa' for '106612' to customer '10661', with event type 'L2 N Lead Approved'. The eighth row is '2016-07-20 10:55:18 143' issued by 'aa' for '106612' to customer '10661', with event type 'Credential Approved'. The 'Event Info' column contains details for the last two rows: 'Matched Against Issuance ID: 106611, Customer Number: 1066, Logged From: AdjLevelDetails' and 'Did Not Match Against Issuance ID: 106611, Customer Number: 1066, Logged From: AdjLevelDetails'.

Issued	User	Issuance ID	Customer Number	Event Type	Event Info
2016-07-20 10:55:18 143	aa	106612	10661	ICAO Complaint	
2016-07-20 10:55:18 143	aa	106612	10661	FRS Enrolled	
2016-07-20 10:55:18 143	aa	106612	10661	N Lead Created	
2016-07-20 10:55:18 143	aa	106612	10661	Set as Match	Matched Against Issuance ID: 106611, Customer Number: 1066, Logged From: AdjLevelDetails
2016-07-20 10:55:18 143	aa	106612	10661	L1 N Lead Escalated	
2016-07-20 10:55:18 143	aa	106612	10661	Set as No Match	Did Not Match Against Issuance ID: 106611, Customer Number: 1066, Logged From: AdjLevelDetails
2016-07-20 10:55:18 143	aa	106612	10661	L2 N Lead Approved	
2016-07-20 10:55:18 143	aa	106612	10661	Credential Approved	

#### 4.12.5.3 How reports displayed for view on the screen can be printable and properly formatted.

Our proposed solution complies.

All reports can be viewed on the screen, Exported to a PDF, Exported to a CSV file, or printed. The system automatically formats the data for the chosen method to view the data.

The screenshot shows a web application interface for reports. At the top, there's a 'Reports' section with a 'Report Query' dropdown set to 'Employment Summary - Date Range'. Below this are buttons for 'View', 'Export to PDF', 'Export to CSV', and 'Print'. A 'Filter' section contains 'Start Date: 2016-07-25 00:00:00' and 'End Date: 2016-07-29 23:59:00'. The main area displays a table with 10 columns: 'Report Name', 'Date Range', 'Total', 'Valid', 'Expired', 'Suspended', 'Revoked', 'Lost', 'Found', and 'Total and Valid'. The table has 8 rows of data, with the last row labeled 'TOTAL'.

Report Name	Date Range	Total	Valid	Expired	Suspended	Revoked	Lost	Found	Total and Valid
23-07-2016		0	0	0	0	0	0	0	0
24-07-2016		0	0	0	0	0	0	0	0
25-07-2016		0	0	0	0	0	0	0	0
26-07-2016		0	0	0	0	0	0	0	0
27-07-2016		7	1	0	0	0	0	0	1
28-07-2016		0	0	0	0	0	0	0	0
29-07-2016		0	0	0	0	0	0	0	0
TOTAL		7	1	0	0	0	0	0	1

Showing 1 to 8 of 8 entries

#### 4.12.5.4 How the report data can be displayed on screen in such a way as to limit the need to navigate through multiple pages.

##### Vendor Response:

Our proposed solution complies.

Our solution provides search parameters that limit the data returned in the report as well as exporting any reports data to CSV where it can be sorted and filtered as desired.

A sample report is provided below.

Reports

Report Query: FN Lead Summary - Date Range View Export as PDF Export as CSV Print

Filter:

Start Date: 2016-07-22 00:00:00 End Date: 2016-07-29 23:59:00

Show / 10 entries

Date	1.1 Approved	1.1 Escalated	1.2 Approved	1.2 Escalated	Admin Entry	4.3 Approved	4.3 Escalated Initial Review	4.3 Escalated Initial Review
22-07-2016	0	0	0	0	0	0	0	0
23-07-2016	0	0	0	0	0	0	0	0
24-07-2016	0	0	0	0	0	0	0	0
25-07-2016	0	0	0	0	0	0	0	0
26-07-2016	0	0	0	0	0	0	0	0
27-07-2016	1	0	1	0	0	0	0	0
28-07-2016	0	0	0	0	0	0	0	0
29-07-2016	0	0	0	0	0	0	0	0
TOTAL	0	2	2	2	0	0	0	3

Showing 1 to 8 of 8 entries

**Section 4, Subsection 4.12.6 - Vendor should return a confirmation file to the Agency upon receipt of the standard production print files.**

#### Vendor Response:

Our proposed solution complies.

The Veridos Data Processing Systems (DPS) at the Central Issuance Location allows for the receipt of files from WVDMV at set times of the day and as many days per week as required. The receipt of files is configurable and is based on West Virginia's record format information. The system will notify WVDMV of files receipt via confirmation (event/audit) files.

**Section 4, Subsection 4.12.7 - Confirmation files should include the number of print requests received for validation by the Agency against the number of print requests sent.**

#### Vendor Response:

Our proposed solution complies.

The confirmation (event/audit) files include the number of print requests received to be validated by WVDMV against the number of print requests sent. This is a standard operating procedure for Veridos.

---

## SYSTEM ADMINISTRATION

### Section 4, Subsection 4.13 - User Account Management

---

Section 4, Subsection 4.13.1 - Vendor should describe the account management functions as part of their system administration module. This description should include:

Our proposed solution complies.

Secura has a User Management portal that all allows operators, with the correct permissions assigned to their account, to perform many tasks that include but are not limited to:

- User Account Management
- Creation and Assignment of Security Groups
- Reporting
- Review system errors
- Enrollment workstation configuration

---

#### 4.13.1.1 How you may view last login date/time for each user.

Our proposed solution complies.

Secure provides the user audit reports that can be filtered by any log-in event including date/time.

#### User Audit Report

The user audit report shows Secura FRS audit events associated with a specified user over a specified date range. The filter parameters for the user audit report are:

- Start Date – The starting timestamp for entries to include in the report
- End Date – The ending timestamp for entries to include in the report
- User – The Secura user ID for entries to include in the report (free form text box)
  - This report only logs audit events created by users in Secura
- Sort Order – The order to sort the 'Logged' timestamp column (Ascending or Descending)

The screenshot shows a web application interface for 'Reports'. At the top, there are tabs for 'Users', 'Reports by Role', and 'Reports by User'. Below these is a search bar and a 'Filter' button. The main area displays a table with columns: 'User ID', 'User Name', 'User Email', 'User Role', 'User Status', 'User Created', and 'User Last Login'. The table contains several rows of user data. Below the table, there are 'Add New User' and 'Export to CSV' buttons.

User ID	User Name	User Email	User Role	User Status	User Created	User Last Login
10000000000000000000	John Doe	john.doe@veridos.com	Admin	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000001	Jane Smith	jane.smith@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000002	Bob Johnson	bob.johnson@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000003	Alice Brown	alice.brown@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000004	Charlie White	charlie.white@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000005	Diana Prince	diana.prince@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000006	Edward Nigma	edward.nigma@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000007	Fiona Glenanne	fiona.glenanne@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000008	Gordon Gump	gordon.gump@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000009	Helen Parr	helen.parr@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000010	Ivan Drago	ivan.drago@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000011	Jarvis Davis	jarvis.davis@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000012	Kyle Reese	kyle.reese@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000013	Larry Fink	larry.fink@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000014	Melvin Platter	melvin.platter@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000015	Nigel Short	nigel.short@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000016	Oliver Queen	oliver.queen@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000017	Peter Parker	peter.parker@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000018	Quentin Beck	quentin.beck@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000019	Rachel Green	rachel.green@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000020	Samuel Smith	samuel.smith@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000021	Tina Turner	tina.turner@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000022	Victor Stone	victor.stone@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000023	Wade Wilson	wade.wilson@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000024	Xavier Woods	xavier.woods@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000025	Yara Flor	yara.flor@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00
10000000000000000026	Zoe Lomon	zoe.lomon@veridos.com	User	Active	2010-01-01 10:00:00	2010-01-01 10:00:00

#### 4.13.1.2 How to manage user permissions.

Our proposed solution complies.

The proposed solution uses permission-based access control (PBAC) as part of the system security architecture. PBAC is a method to control which users have access to system resources based on the roles assigned to them. This security feature protects stored data from unauthorized viewing and modifications. PBAC security is transparent to users. This means that after users identities are verified, they are only allowed to view data and execute authorized operations based on their defined roles and permissions. The PBAC method protects data and system security by making sure that users cannot misuse their access rights and privileges.

User accounts with the System Administrator privilege are used to manage other user account permissions. A system Administrator uses the Users and Roles tab of the web client to configure authorized users and define how they access the system. The Roles tab lets you manage permissions assigned to Secura roles.

##### Users

Users reside inside the enterprise LDAP and are created within the system. To ensure system integrity, each user is identified based on a User ID/ Password authentication mechanism. A system administrator assigns each user to one or more roles (with all of the corresponding permissions). The roles assigned to each user determine what activities they are allowed to perform and what information they can access.

##### Permissions

Permissions enforce the actions and activities that users are allowed to perform within their assigned roles. A system administrator associates each role with specific permissions for specific tasks; therefore, the roles assigned to each user determine which permissions (authorized actions) they are granted.

#### 4.13.13 How the ability to view partial or full SSN data in all applications will be achieved based on permissions or role.

Our proposed solution complies.

The solution provides a role-based user account management system that allows for specific fields to be accessible only by individuals with the correct roles assigned to their user account. The SSN will be set up to be accessible by the approved roles.

### Section 4, Subsection 4.14 - System Usage Dashboard

Section 4, Subsection 4.14.1 - Vendor should describe how the system administration module may display the current view of system usage including items such as:

#### 4.14.1.1 Number of users currently logged into FRS & ICW applications

Our proposed solution complies.

There are six different System Administration Module options available. They are Problem Applications, Manage Workstations, Scheduled Actions, Audit, Notifications and Configuration.

Secura has a portal that can be used to perform a query to show the history or current user's account usage. This portal also shows the number of users currently logged into Secura and the FRS.



User data can be shown on the screen or printed out on paper. A user of the proposed system with the correct privileges assigned to their account can search for users by name, location, or group as well as specify specific timeframes/date ranges to return results.

#### 4.14.1.2 Number of records pending in all queues in FRS.

Our proposed solution complies.

The proposed solution includes a Dashboard that shows graphically how many records are in each of the individual queues. The dashboard automatically updates itself every 3 minutes when the screen is being viewed. The Dashboard also shows graphically how many users are logged into the system at any given time.

#### 4.14.1.3 Central production facility statistics.

##### Vendor Response:

Our proposed solution complies.

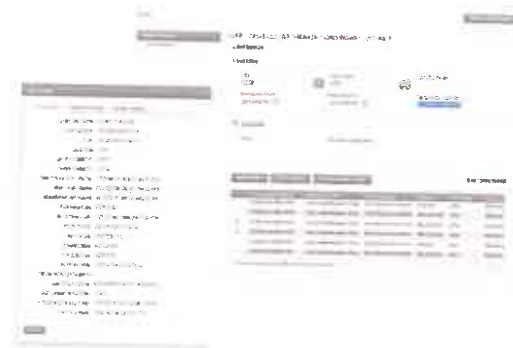
Veridos' Online Portal enables WVDMV a self-service capability to query the processing status of individual personalization card orders, as well as to designate specific actions (redirect, pull, hold) for in-process card personalization. The Portal and Status Enquiry application are easily adapted for West Virginia's specific needs and offer 24/7/365 access to production status.

##### Status Enquiry Application

The *Status Enquiry* application provides reports regarding the date that a card request has been received or has been shipped in addition to DL/ID cards specific demographic information such as: address, DL/ID card number, data received, batch ID, date shipped, mailing method of shipment.

The following objectives can be achieved by WVDMV by using this application:

- **Search Cards:** User can search for a card by configurable keys, i.e. DL/ID number (or other parameters)
- **View Card Details:** User can view the details of a card request
- **Select Cards for Pull:** User can select a card or more than one card to submit a pull request.



#### Section 4, Subsection 4.15 - Management of Central Issuance Records

##### Section 4, Subsection 4.15.1 - Vendor solution should allow for status queries on individual card print records. Vendor Response:

Our proposed solution complies.

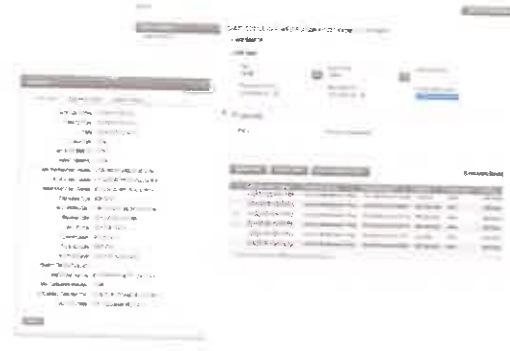
Veridos' Online Portal enables WVDMV a self-service capability to query the processing status of individual personalization card orders, as well as to designate specific actions (redirect, pull, hold) for in-process card personalization. The Portal and Status Enquiry application are easily adapted for West Virginia's specific needs and offer 24/7/365 access to production status.

##### Status Enquiry Application

The *Status Enquiry* application provides reports regarding the date that a card request has been received or has been shipped in addition to DL/ID cards specific demographic information such as: address, DL/ID card number, data received, batch ID, date shipped, mailing method of shipment.

The following objectives can be achieved by WVDMV by using this application:

- **Search Cards:** User can search for a card by configurable keys, i.e. DL/ID number (or other parameters)
- **View Card Details:** User can view the details of a card request
- **Select Cards for Pull:** User can select a card or more than one card to submit a pull request.



**Section 4, Subsection 4.15.2 - Vendor solution should allow for holds to be placed on individual card print records prior to the start of processing.**

#### Vendor Response:

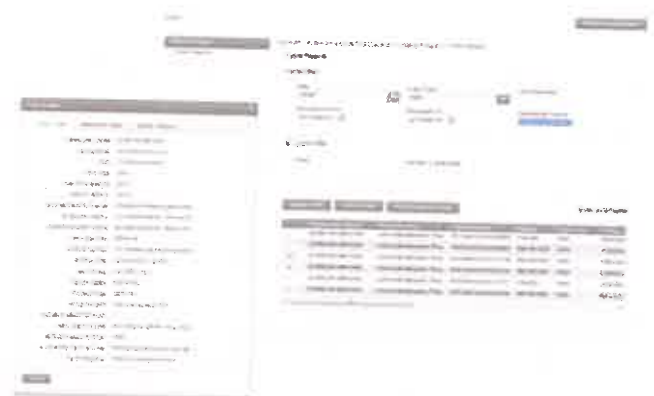
Our proposed solution complies.

Our online portal allows WVDMV to place holds on individual card print records prior to the start of processing.

Our Reports Online application within the Online Portal provides an easy to use tool that allows the State to access reports generated as a result of personalization file processing, inventory planner report, or customer specific reports that are created based on customer specific requirements.

#### Some examples include:

- Cards stock manufactured status
- Transmitting DL/ID card requests success and failure
- Data balancing status (received batch quantity does not balance) failure and success
- Data format status failure and success
- Data requests rejected



- Transfer stock status (ex: to DRP location)
- Pull request status failure and success
- Card damaged and remake status
- Cards QA status
- Cards produced status
- Cards shipped status
- Expedited requests status
- Request on Hold status
- Requests purged/destroyed status

In situations when time does not allow for the use of Online Portal, your dedicated Relationship Manager can be contacted to escalate the matter to Veridos' Operations and QA teams.

**Section 4, Subsection 4.15.3 - Vendor solution should allow for priority flags to be set on individual card print records which must trigger expedited processing.**

**Vendor Response:**

Our proposed solution complies.

Our online portal allows WVDMV to set priority flags on individual card print records prior to the start of processing that will trigger expedited processing.

Veridos' Data Processing System (DPS) is capable of receiving and processing West Virginia's files daily, as well as receiving expedited files separately, or as a single transmission. The special handling requests are indicated by the submitting party through selection of 'Priority' DL/ID, triggering expedited card production.

Veridos' proposed solution also allows West Virginia to send an 'Expedite' file to the Veridos System where batched records are received via batch file transfer. The request will indicate card # and the required change of status (i.e. expedite).

Section 4, Subsection 4.15.4 - Vendor solution should allow for tracking information, to be available for expedited print request records.

**Vendor Response:**

Our proposed solution complies.

To expedite delivery to the individual cardholder, we provide multiple services where we send the card by courier directly to the client, or we can also send the card back to the individual location for customer pick-up. Expedited service is a fundamental part of the Veridos service and we work with all courier companies should West Virginia desire a particular courier provider. Tracking information to be provided for each courier package.

**Section 4, Subsection 4.16 - Reports**

Section 4, Subsection 4.16.1 - Vendor solution should capture audit data for all images, data captured, and temporary DLs produced and made available in detail and summary reports.

**Vendor Response:**

Our proposed solution complies.

Our solution provides a robust reporting and audit capabilities that allow a user to view both detailed and higher level summary reports such as the N Leads summary report.

The N Lead summary report shows a summary of the number of occurrences each day of adjudication events for 1:N leads during the specified time period. This report contains the following columns:

- Date – The timestamp of when the event occurred
- L1 Approved – A 1:N lead at adjudication level 1 has been approved
- L1 Escalated – A 1:N lead at adjudication level 1 has been escalated to L2 status
- L2 Approved – A 1:N lead at adjudication level 2 has been approved
- L2 Escalated – A 1:N lead at adjudication level 2 has been escalated to Investigation status

Reports									
Reports									
Report Query: All Lead Summary - Date Range									
View Export as PDF Export as CSV Print									
Filter:									
Start Date: 2016-07-22 00:00:00 End Date: 2016-07-29 23:59:00									
Show 10 entries									
Date	L1 Approved	L1 Escalated	L2 Approved	L2 Escalated	Admin Error	L3 Approved	L3 Escalated Internal Review	L3 Escalated MU Review	Search
22-07-2016	0	0	1	0	0	0	0	0	
23-07-2016	0	0	0	0	0	0	0	0	
24-07-2016	0	0	0	0	0	0	0	0	
25-07-2016	0	0	0	0	0	0	0	0	
26-07-2016	0	0	0	0	0	0	0	0	
27-07-2016	0	1	1	0	0	0	0	0	
28-07-2016	0	0	0	0	0	0	0	0	
29-07-2016	0	0	0	2	0	0	0	3	
TOTAL	0	1	2	2	0	0	0	3	
Showing 1 to 9 of 9 entries									

#### Section 4, Subsection 4.16.2 - Vendor solution should produce daily reconciliation reports. Vendor Response:

Our proposed solution complies.

Our solution supports a number of summary/reconciliation reports that can be queried on a yearly, quarterly, monthly or ad hoc (daily or more frequently) basis.

Reconciliation Invoice	Provides a monthly total broken down by each week for each WV card, for mailed, pulled & reprints. Totals for all cards, GST and grand total.	DCN, Time, # of cards charged with associated cost broken for the month and weeks within the month
Detailed Reconciliation Invoice (by day)	Provides a detailed listing for reconciliation that is broken down by week and then by day with the same details as the Reconciliation Invoice.	Same as above and broken down by week, day and individual DCN

#### Section 4, Subsection 4.16.3 - Vendor solution should be able to request reports for specific date or date ranges. Vendor Response:

Our proposed solution complies.

Secura reporting allows the operators to choose a specific date or date ranges for reports as shown below.

**Reports**

Report Query: Transaction Summary-Monthly View Export as PDF Export as CSV

Filter:

Year: 2016 Month: April

Show 10 entries

Month/Date	Enrollment	Leads Created	11 M Leads Approved	12 M Leads Approved	12 M Leads Localized	11 M Leads Approved	12 M Leads Approved	12 M Leads Localized	Closed Leads (Investigation)
01-04-2016	0	0	0	0	0	0	0	0	0
02-04-2016	0	0	0	0	0	0	0	0	0
03-04-2016	0	0	0	0	0	0	0	0	0
04-04-2016	0	0	0	0	0	0	0	0	0
05-04-2016	0	0	0	0	0	0	0	0	0
06-04-2016	0	0	0	0	0	0	0	0	0
07-04-2016	40	32	5	3	4	4	3	1	0
08-04-2016	0	0	0	0	0	0	0	0	0
09-04-2016	0	0	0	0	0	0	0	0	0
10-04-2016	0	0	0	0	0	0	0	0	0
11-04-2016	0	0	0	0	0	0	0	0	0

Showing 1 to 10 of 21 entries

Filter(s):

Start: 2016-03-01 00:00

End: 2016-04-21 23:59

Search

2016 Mar

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Time 00:00

Hour

Minute

Now Done

Date

Category

**Section 4, Subsection 4.16.4 - Vendor solution should print to Agency network printers. Vendor Response:**

**Our proposed solution complies.**

### Section 4, Subsection 4.17 - Controlled Use

**Section 4, Subsection 4.17.1 - Vendor solution should be able to log unauthorized attempts to access the system software.**

**Vendor Response:**

**Our proposed solution complies.**

Secura logs both successful and unsuccessful login attempts. These attempts can be reviewed using the User Audit reporting functions.

## User Audit Report

The user audit report shows Secura FRS audit events associated with a specified user over a specified date range. The filter parameters for the user audit report are:

- **Start Date** – The starting timestamp for entries to include in the report
- **End Date** – The ending timestamp for entries to include in the report
- **User** – The Secura user ID for entries to include in the report (free form text box)
  - This report only logs audit events created by users in Secura
- **Sort Order** – The order to sort the 'Logged' timestamp column (Ascending or Descending)

[illegible]

---

#### Section 4, Subsection 4.18 - Protection

---

---

##### Section 4, Subsection 4.18.1 - Vendor solution should have security protection to prevent unauthorized access. Vendor Response:

---

Our proposed solution complies.

All software provided is industry-best practices open architecture using TCP/IP, HTTP or HTTPS and other protocols including but not limited to SOAP or REST services, Public Key Infrastructure (PKI), Virtual Private Networks (VPN) and other encryption for protecting data while in movement or at rest.

The system also uses Active Directory for user login authentication to prevent unauthorized access to the system. The proposed solution also has a feature that allows for configurable time frames to be established that prevents the image capture application from being logged into even with authorized accounts during non-business hours, such as 10pm – 5 am.

---

#### Section 4, Subsection 4.19 - Data Management

---

---

##### Section 4, Subsection 4.19.1 - The system administration module should include data management functions. Describe how these data management functions will address:

---

---

###### 4.19.1.1 Removing records with data or image errors

---

Our proposed solution complies.

The proposed system provides a portal that operators, with the correct privileges, can access that allows for the update and/or deletion of records. This portal is used to remove records that have data and image errors.

---

###### 4.19.1.2 Marking records that are to be used for testing purposes

---

Our proposed solution complies.

The system provides for test records to be flagged as such within the system so that they are not mistaken for real production requests.

#### 4.19.1.3 Access to system audit logs

##### Vendor Response:

Our proposed solution complies.

##### Audit Reports

The Secura audit reports display information regarding the Secura audit events which occur during the Secura FRS process. The audit entries recorded in the Secura FRS are never purged and are always available for reporting purposes.

Three audit report perspectives are supported:

- Credential – all events related to a specified credential (Issuance ID)
- Customer – all events related to a specified customer ID (all credentials associated with the customer)
- User – all events release to events initiated by the specified user (Secura user name)

Each of the audit reports support the following columns:

- Logged – The timestamp of when the event was logged
- User – The Secura user associated with the event
- Issuance ID – The credential issuance ID associated with the event (when applicable)
- Customer Number – The customer number associated with the event (when applicable)
- Event Type – The event type of the entry (refer to the Audit Event Type table below)
- Event Data – Additional data associated with the event (when applicable)

##### Credential Audit Report

The credential audit report shows Secura FRS audit events associated with a specified credential (Issuance ID) over a specified date range. The filter parameters for the credential audit report are:

- Start Date – The starting timestamp for entries to include in the report
- End Date – The ending timestamp for entries to include in the report
- Issuance ID – The credential issuance ID for entries to include in the report
- Sort Order – The order to sort the 'Logged' timestamp column (Ascending or Descending)

**Reports**

Report Query: Audit Report - Customer

Filters:

Start Date: 2016-07-26 00:00:00 End Date: 2016-07-27 23:59:30 Issuance ID: 106612 Sort Order: ASC

Timestamp	User	Issuance ID	Customer Number	Event Type	Event Data
27-07-2016 10:23:19.342	ee	106612	10661	ICAO Complete	
27-07-2016 10:23:19.767	ee	106612	10661	FRS Enrolled	
27-07-2016 10:53:20.040	ee	106612	10661	N Lead Created	
27-07-2016 11:19:49.583	saa	106612	10661	Set as Match	Matched Against Issuance ID: 106611 Customer Number: 1066 Logged From: AdLe-v2Details
27-07-2016 11:19:53.707	saa	106612	10661	L1 N Lead Escalated	
27-07-2016 11:20:42.500	saa	106612	10661	Set as No Match	Did Not Match Against Issuance ID: 106611 Customer Number: 1066 Logged From: AdLe-v2Details
27-07-2016 11:20:56.613	saa	106612	10661	L2 N Lead Approved	
27-07-2016 11:20:56.613	saa	106612	10661	Credential Approved	

Showing 7 to 8 of 8 entries

### Customer Audit Report

The customer audit report shows Secura FRS audit events associated with a specified customer over a specified date range. The filter parameters for the customer audit report are:

- **Start Date** – The starting timestamp for entries to include in the report
- **End Date** – The ending timestamp for entries to include in the report
- **Customer Number** – The customer number for entries to include in the report
- **Sort Order** – The order to sort the 'Logged' timestamp column (Ascending or Descending)

**Reports**

Report Query: Audit Report - Customer

Filters:

Start Date: 2016-07-27 00:00:00 End Date: 2016-07-27 23:59:30 Customer No: 10661 Sort Order: ASC

Timestamp	User	Issuance ID	Customer Number	Event Type	Event Data
27-07-2016 10:52:19.143	ee	106612	10661	ICAO Complete	
27-07-2016 10:53:19.767	ee	106612	10661	FRS Enrolled	
27-07-2016 10:53:20.040	ee	106612	10661	N Lead Created	
27-07-2016 11:19:49.583	saa	106612	10661	Credential Accessed	AdLe-v2Cue
27-07-2016 11:19:49.583	saa	106612	10661	Set as Match	Matched Against Issuance ID: 106611 Customer Number: 1066 Logged From: AdLe-v2Details
27-07-2016 11:19:53.707	saa	106612	10661	L1 N Lead Escalated	
27-07-2016 11:20:42.500	saa	106612	10661	Credential Accessed	AdLe-v2Cue
27-07-2016 11:20:42.500	saa	106612	10661	Created Examiner File	Examiner File Created for Probe. Logged From: AdLe-v2Details
27-07-2016 11:20:56.613	saa	106612	10661	Set as No Match	Did Not Match Against Issuance ID: 106611 Customer Number: 1066 Logged From: AdLe-v2Details
27-07-2016 11:20:56.613	saa	106612	10661	L2 N Lead Approved	
27-07-2016 11:20:56.613	saa	106612	10661	Credential Approved	

Showing 1 to 11 of 11 entries

### User Audit Report

The user audit report shows Secura FRS audit events associated with a specified user over a specified date range. The filter parameters for the user audit report are:

- **Start Date** – The starting timestamp for entries to include in the report
- **End Date** – The ending timestamp for entries to include in the report

- **User** – The Secura user ID for entries to include in the report (free form text box)
  - This report only logs audit events created by users in Secura
- **Sort Order** – The order to sort the 'Logged' timestamp column (Ascending or Descending)

[illegible]

## Section 4, Subsection 4.20 - Audit functions

Section 4, Subsection 4.20.1 - Vendors solution should store the username for every transaction completed on the image and signature capture workstation. Re-authentication upon the printing of each temporary driver's license may be needed and should be configurable.

### Vendor Response:

**Our proposed solution complies.**

**Secura tracks all user activities within the system.**

Each of the operator actions creates an entry in the audit logs with the follow data:

- **Logged** – The timestamp of when the event was logged
- **User** – The Secura user associated with the event
- **Issuance ID** – The credential issuance ID associated with the event (when applicable)
- **Customer Number** – The customer number associated with the event (when applicable)
- **Event Type** – The event type of the entry
- **Event Data** – Additional data associated with the event (when applicable)

Secura has the option to have the operator re-authenticate at many points within the workflow, the most common being the printing of the temporary DL/ID card. The re-authentication is configurable to meet WVDMV's specific needs.

---

#### Section 4, Subsection 4.21 - Equipment installation

Section 4, Subsection 4.21.1 - To minimize clutter, prevent damage, and prevent easy removal, the Vendors solution should consist of only the workstation components that are necessary for capturing the applicant's image, validating DL credentials and signature.

---

#### Vendor Response:

Our proposed solution complies.

The Veridos Capture Solution is optimized to secure and minimize the desktop capture workstation footprint and clutter.

Examples include:

- The Secure Photo Capture Tower is designed on a small 8"x 8" base (see diagram in Section 4.41.1.5)
- The Secure Capture Tower is designed to be bolted to a desktop if desired/required (see diagram in Section 4.41.1.5)
- The Secure Photo Capture Tower is designed with a built in USB hub to power other capture devices
- The Signature Capture Device is a combination device that will support signature capture as well as Queries related to Voter Registration, etc
- The Document Scanning device for Real ID breeder documents is an ADF type that feeds automatically with a smaller footprint than a flatbed scanner
- The Document Scanning device is available with a dedicated passport scanner option that fits underneath the ADF reader



---

## CARD DESIGN AND SECURITY FEATURES REQUIREMENTS

---

### Section 4, Subsection 4.22 - Secure Temporary Driver's License and ID's

Section 4, Subsection 4.22.1 - Vendor should explain how their solution will produce a secure temporary driving credential for applicant use while waiting for the card to be printed at the secure central production facility; including any secure consumables, such as laminate, and/or paper, and recommended printing equipment.

---

#### Vendor Response:

Our proposed solution complies.

The interim DL/ID will be printed from the capture workstation or from Secura's web application. If the print request is triggered from the ICW, it will print automatically on a printer already assigned to that workstation. The system includes a function for reprinting the temporary DL/ID, with supervisor override capability, if necessary.

Our proposed printer for the temporary DL/ID is specified below:

**Paper Printer – HP LaserJet Pro – For Interim ID/DL**

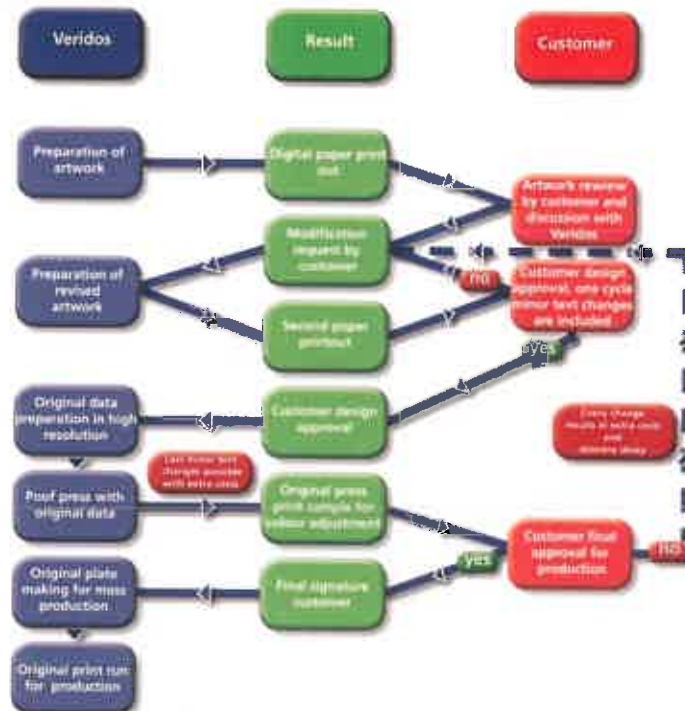


- HP LaserJet Pro M402n – or equivalent - Laser Printer
  - Technology - Monochrome – laser
  - Resolution – HP FastRes 1200 dpi
  - Monthly duty cycle – up to 80,000 pages
  - Recommended volume – up to 4000 / month
  - Paper Trays - Standard – 2 (100 pg. and 250 pg.)
  - Connectivity USB 2.0, and 10,100,1000 Gb Ethernet
  - Printer Toner Cartridge – HP26A or Extended HP26X
  - Dimensions - WxDxH - 15 x 14.06 x 8.5 in
  - Weight - 18.92 lbs.











The design of the Temporary DL/ID will be generated according to WVDMV specifications. The design, creation, origination and approval process is illustrated below and the respective steps can be deduced from it. The following steps will be part of the approval process:

- 1) Approval of design artwork (graphical)
- 2) Approval of origination

This process is outlined below.



The proposed paper includes the following features:

Element	Description	Verification level
	<b>High-security paper</b> <ul style="list-style-type: none"> <li>The paper of the Interim Driver License is composed of paper with 100% cellulose.</li> <li>The paper does not contain optical brighteners (dull, non-fluorescent).</li> <li>This paper is restricted to high-security applications and the material is not available to the public on the open market.</li> <li>The paper allows for high-resolution inkjet personalization.</li> </ul>	<div>1 </div> <div>1 </div> <div>2 </div>
	<b>Protection against chemical erasure</b> <ul style="list-style-type: none"> <li>The paper contains a chemical agent which reacts strongly on contact with acids, alkalis, bleaching agents and organic solvents, producing a visible stain. These chemicals are frequently used by counterfeiters in an attempt to remove information from the Interim Driver License.</li> </ul>	<div>2 </div>
	<b>UV security fibers</b> <ul style="list-style-type: none"> <li>Invisible fibers in the paper, which become visible in bright colors in blue, red and green when the paper is exposed to ultraviolet light. This feature is not available for ordinary office paper.</li> </ul>	<div>2 </div>
	<b>Visible security fibers</b> <ul style="list-style-type: none"> <li>Visible fibers, which are easily recognizable by the human eye, are integrated with the paper.</li> </ul>	<div>1 </div>

---

#### Section 4, Subsection 4.23 - Card Design Changes

Section 4, Subsection 4.23.1 - Vendor should describe how they propose handling security format changes to cards made post-implementation, based on reported or identified security gaps.

---

#### Vendor Response:

Our proposed solution complies.

Veridos will work with West Virginia to maintain and participate an active Card Design Security Program through the duration of the contract. Veridos offers cards that meet all current standards and will also work with the WVDMV to ensure your cards stay current with AAMVA and industry standards as they evolve.

We will work closely with the WVDMV and West Virginia law enforcement to hold bi-annual meetings to review the cards and explore ways to enhance or introduce new security features.

Our proposed card solution for West Virginia is designed to be a "platform" that can adapt to changing requirements and emerging technologies such as alterations to substrate or the inclusion of a chip module. We also provide ongoing partnership, including the Card Review Committee to address ongoing redesigns and security upgrades throughout the full term of the contract. This approach ensures that the cards' integrity and security remain highly resistant to fraud.

Veridos' card products are routinely subject to independent testing for their durability and adherence to design standards. The results of these tests will be made available to the WVDMV at no cost. Veridos will warrant that all cards provided under contract to West Virginia will exceed the five-year lifespan required by this RFP under normal use.

Our commitment to the ongoing security of the West Virginia DL/ID program is reflected in our everyday partnership. The WVDMV will have a dedicated Relationship Manager who is available at any time to discuss individual concerns. The Relationship Manager also reports directly to the Account Executive who will routinely discuss recommendations for additional design changes to combat evolving threats.

Veridos takes pride in being at the forefront of innovative technology to be one step ahead of fraudulent attempts to replicate Driver's Licenses and national forms of identification. Our R&D department is focused on developing new security features and card enhancements that allow the card to be refreshed over a long-term contract. We work closely with law enforcement and our customers to hold bi-annual meetings to review the cards and explore ways to enhance or introduce new security features.

In addition, our internal graphics department is current on all standards to ensure that correct specifications are being adhered to before the card goes to print. To facilitate these efforts we have allowed for the design of the card to be flexible in the sense that

new security features can be incorporated without transforming the entire image. All cards manufactured and produced adhere to AAMVA standards and requirements; this applies to card body features and also to personalized features such as barcode, etc.

---

#### PROJECT MANAGEMENT

Section 4, Subsection 4.24 - The Vendor project manager should be involved in every detail of the project from start to finish. High level oversight will not be acceptable.

---

#### Vendor Response:

Our proposed solution complies.

Our dedicated proposed Project Manager for WVDMV is **Anastasia Koulis**. Anastasia will be involved in every detail of the project from start to finish.

Anastasia has 25 years of experience in delivering highly secure solutions in both the financial and government solutions industries. Anastasia has been a regular, fulltime employee with Veridos and our parent firm G+D since 2014.

Anastasia will function as the Lead Project Manager and is responsible for the successful delivery of the project, coordination of WVDMV activities, Veridos and third party resources as well as ongoing communication and strategy.

Anastasia has recently implemented several large projects of a similar scope and size to the requirements of this RFP.

Brief summaries of Anastasia's recent projects are highlighted below.

Project Reference #1	
Company Name:	Saskatchewan Government Insurance
Company Address:	2260 11 <sup>th</sup> Avenue, Regina, Saskatchewan, S4P 0J9
Contact Name:	Randy Stoneham, - Manager, Issuer and Customer Support Services.
Contact Telephone Number:	306-751-3757
Contact Email:	Rstoneham@sgi.sk.ca
Date Work Undertaken:	April 2016



Nature of Assignment:	<ul style="list-style-type: none"> <li>• Large scale project to introduce a brand new Driver's License and Identification card &amp; Capture Manager system by a specific set launch date, as well as a Facial Recognition System</li> <li>• High level of complexity involved to manage deliverables from numerous partners, and work streams, multi-phased approach, extensive documentation and testing</li> <li>• Duration of the project was 16 months – May 2015-Aug 2016</li> </ul>
-----------------------	--

Project Reference #2	
Company Name:	Manitoba Public Insurance
Company Address:	912-234 Donald Street, PO Box 6300, Winnipeg, Manitoba
Contact Name:	Brad Bunko - Vice President; Information Technology
Contact Telephone Number:	204-985-8770 EXT 7481
Contact Email:	bbunko@mpi.mb.ca
Date Work Undertaken:	Current – May 2017
Nature of Assignment:	<ul style="list-style-type: none"> <li>• Large scale project to in upgrade a Capture Management system and launch a Facial Recognition System</li> <li>• High level of complexity involved to manage deliverables from numerous partners, documentation and testing</li> <li>• Duration of project was 15 months – May 2015 – Aug 2016</li> </ul>

Section 4, Subsection 4.25 - The Vendor project manager should follow project phases from project initiation through acceptance, including requirements gathering and analysis. The Vendor project manager should be prepared and capable of facilitating requirements gathering meetings with the Agency staff.

**Vendor Response:**

Our proposed solution complies.

Veridos' Project Management Methodology is described below at a high-level and is designed to provide a substantive and objective framework for the reporting and review of projects to stakeholders. We will adapt our Methodology to coincide with the State of West Virginia's reporting methodology as needed. Our Project Management Methodology is straightforward, requiring minimal training for State team members to complete their work according to the Statement of Work (SOW).

Our Project Management Methodology is built upon seven (7) core fundamental activities:

- 1) Documenting business requirements
- 2) Developing a project plan and resource allocation
- 3) Establishing a process to assess and manage any risks and/or gaps identified throughout the project lifecycle
- 4) Establishing a process to manage and resolve project issues
- 5) Establishing a process to manage and approve change requests (Change Management)
- 6) Quality Assurance and Testing throughout the project's lifecycle
- 7) On-going support and training

While the methodology described provides a foundation, it is through a detailed collaborative approach throughout the lifecycle of the project that the team will be able to capture the nuances embedded within each of the business requirements. It is the customized collaborative approach that ensures the ultimate success of each project. Veridos has followed this methodology and approach with each of its implementations successfully.

With the implementation of each project, the lessons learned and gained are continually reinvested to refine this proven and successful approach. The benefits of our Project Management Methodology are many; five are presented below.



### Complete and Comprehensive Understanding of Requirements:

The Business Requirements Definition phase has proven to be one of the most significant stages in the development of a successful implementation and transition of a Project. Our Project Managers have been trained and are experienced in ensuring that the appropriate focus and time is given during this stage. This is a disciplined approach of ensuring all of the business requirements are gathered and fully understood from end-to-end. This process would involve the participation of individuals representing all areas of the project. As this project involves the migration of the card production to our facility, this process would allow for our team of experts to provide a full consultative review of the business requirements versus our operational capabilities. This consultative review would provide WVDMV with potential opportunities for efficiencies and/or cost reductions, as well as the operational capabilities to improve security and/or client communication requirements. This latter point may be of significance to WVDMV, as the project will be introducing a new card platform to the residents of West Virginia, which will place a greater emphasis on educating and reassuring West Virginia's citizens on the rationale for the new card platform.

This phase also provides the benefit of ensuring the proper coordination of activities with the existing contractor. There will be a need to have an understanding of both environments in order to ensure a smooth migration. Veridos has extensive experience in migrating clients from another vendor to our own environment.

### Ensuring Timelines are Met and Allocation Resources

Once the full scope of the business requirements have been defined, detailed task dependencies and project timelines will be outlined. Based on the tasks required to be completed and the timeline associated with that task, resources are then allocated to the project team. A complete review of the project timelines versus the business requirements is then completed. Should project timelines be outside of the business requirements/expectations, a complete review of project resources and timeline dependencies is then undertaken in order to bring the project on plan.

Our Project Managers are trained and experienced in analyzing potential gaps within project plans and business requirements. This expertise, coupled with the availability of our resources and robust operational capabilities, provides additional flexibility and comfort in ensuring that sufficient resources are provided and time lines are met. The benefit to the project is **"ON BUDGET and ON TIME."**

Veridos has assigned a skilled Project Manager, supported by a robust team of skilled experts representing both technical and business subject matter. The experience of this team will ensure that all business requirements have been addressed within the Project Plan.

---

Section 4, Subsection 4.26 - The Vendor project manager should be involved in the technical details of the design, development, and testing phases of the project, and should not expect the Vendor technical lead to fully manage those activities.

---

**Vendor. Response:**

Our proposed solution complies.

The Business Requirements Definition phase has proven to be one of the most significant stages in the development of a successful implementation and transition of a Project. Our Project Managers have been trained and are experienced in ensuring that the appropriate focus and time is given during this stage. This is a disciplined approach of ensuring all of the business requirements are gathered and fully understood from end-to-end. This process would involve the participation of individuals representing all areas of the project. As this project involves the migration of the card production to our facility, this process would allow for our team of experts to provide a full consultative review of the business requirements versus our operational capabilities. This consultative review would provide WVDMV with potential opportunities for efficiencies and/or cost reductions, as well as the operational capabilities to improve security and/or client communication requirements. This latter point may be of significance to WVDMV, as the project will be introducing a new card platform to the residents of West Virginia, which will place a greater emphasis on educating and reassuring West Virginia's citizens on the rationale for the new card platform.

The assurance of any successful project is centered on its ability to dedicate a sufficient amount of time to testing, supported by a robust test strategy. As testing is one of the last phases prior to the implementation of a project, the temptation may exist to cut this phase short in order to meet an implementation date. Our implementation methodology is to ensure that the integrity of the testing phase remain in place without affecting the implementation date. This is achieved by strong Project Management discipline throughout the lifecycle of the project; utilizing tools such as the Issue Management Process, Escalation Management Process and the Change Management Process to ensure early on that the project remains on plan. As mentioned, strong Project Management is supported by a robust Test Strategy. Veridos incorporates Alpha Testing throughout the various components of the project. In addition, robust collaborative Beta Tests are performed. These tests are completed with input by the client, and involve full regression testing of all components of the solution.

Where possible, it is also recommended that in addition to Beta Testing, an internal staff trial be incorporated into the testing phase. This would provide the comfort of

ensuring that any potential errors not caught during either the Alpha or Beta Tests are captured prior to market release.

In addition to the above, testing can be further augmented by a controlled market/field trial of the proposed solution. This would provide WVDMV an added level of comfort, ensuring that all lessons learned relative to market acceptance issues can be incorporated into the full implementation phase.

---

#### Section 4, Subsection 4.27 - Communication

Section 4, Subsection 4.27.1 - The Vendor project manager should manage the work by establishing and maintaining communications with all groups related to the project. The activities of the Vendor's project team should be directed, coordinated, and communicated with the Agency Project Manager to ensure that the project progresses per the project work plan and is completed on schedule.

---

#### Vendor Response:

Our proposed solution complies.

We believe that a key section within the Project Plan is the Communications Plan to define communication requirements of the project and how information will be distributed to ensure project success. Each milestone and deliverable is discussed by the team. In our experience, a solid Communications Plan has helped avoid project problems. Our Communications Plans include the following sections:

- Communication requirements based upon roles
- What information will be communicated
- How the information will be communicated
- When the information will be distributed
- Who receives the communication
- Conduct of the communications

Our Project Manager will take the lead in ensuring effective communications for this project. The following chart is an example of a guide within the Communications Plan that we have used in past/current projects.

Communication Type	Description	Frequency	Format	Participants/ Distribution	Deliverable	Owner
Weekly Status Report	Email summary of project status	Weekly	Email	Project Sponsor, Team and Stakeholders	Status Report	Project Manager
Weekly Project Team Meeting	Meeting to review action register and status	Weekly	In Person	Project Team	Updated Action Register	Project Manager
Project Monthly Review (PMR)	Present metrics and status to team and sponsor	Monthly	In Person	Project Sponsor, Team, and Stakeholders	Status and Metric Presentation	Project Manager
Project Gate Reviews	Present closeout of project phases and kickoff next phase	As Needed	In Person	Project Sponsor, Team and Stakeholders	Phase completion report and phase kickoff	Project Manager
Technical Design Review	Review of any technical designs or work associated with the project	As Needed	In Person	Project Team	Technical Design Package	Project Manager

**Section 4, Subsection 4.27.2 - The Vendor project manager should communicate with the Agency project manager daily for resolution of issues, decisions, or just to report project status.**

#### **Vendor Response:**

Our proposed solution complies.

In addition to a formal Communications Plan, our project manager will communicate with WVDMV's project manager on a daily basis. The relationship between the two project managers needs to be strong and collaborative. Our proposed project manager has years of experience working with customer project management and understands the importance of daily communications.

The project kickoff is included in our overall Project Plan and will take place in West Virginia prior to project commencement. Following project kick-off, Anastasia will align with the WVDMV's Project Manager to ensure common project documents and objectives moving forward.

---

#### Section 4, Subsection 4.28 - Status Reporting

Section 4, Subsection 4.28.1 - During project design and implementation, Vendor's Project Manager should facilitate weekly project status reviews to ensure measurable progress is being achieved and the Vendor's project team is following the agreed upon work plan.

---

#### Vendor Response:

Our proposed solution complies.

Our Project Manager and team will follow the Governance structure defined by the State of West Virginia. Veridos will track and monitor performance metrics and standards for the project, quickly identifying and resolving project issues. The Project Team will produce status reports on a weekly basis, at minimum, in a mutually agreed format. In addition, Veridos recommends quarterly Executive Meetings between our Executive Sponsor, WVDMV's Executive Sponsor and the Project Management team in order to keep the executives informed of the project status. Please see our response to Section 4.27.1 for additional information on reporting and communications.

Veridos will structure its team, project documents and communications to minimize risk to the WVDMV throughout this very important project.

---

Section 4, Subsection 4.28.2 - Additional meetings should be scheduled as required by the Agency Project Manager or the Vendor. The Vendor's Project Manager and personnel should be available to provide information, reports, or audits as required by the Agency Project Manager.

---

#### Vendor Response:

Our proposed solution complies.

As reflected in our responses to Section 4.27.1, additional meetings will be scheduled by the project managers as needed. Our Project Manager and team members will be available to provide information, reports and audits as required by WVDMV.

---

Section 4, Subsection 4.28.3 - The following deliverables should be included prior to each status meetings:

---

4.28.3.1 Updated project workplan indicating progress for each task

4.28.3.2 Identify and report the status of all tasks that have fallen behind schedule, the reason for the delay, the projected completion date and project impact

4.28.3.3 Identify and summarize all risks and problems identified by the Vendor, which may affect the project:

4.28.3.3.1 For each risk and issue, identify the action and person(s) responsible for mitigating the risk and resolving the issue, and the time required to implement avoidance and/or mitigation actions.

4.28.3.3.2 For each risk and issue identified, state the impact to the project schedule discuss and identify all personnel, equipment, facilities, and resources of the Agency that will be required for the Vendor to perform the project work plan tasks at least two (2) weeks in advance of the need.

---

**Vendor Response:**

Our proposed solution complies.

In addition to the Microsoft Project deliverable, we will provide a detailed and well-planned Project Management Plan. For all of our credential projects, Veridos provides a Project Management Plan that includes the items listed above, at minimum. A very brief summary of how we address each section is provided below:

- Project Integration – Veridos typically refers to this section as the Project Management Approach that outlines the roles, responsibilities and authority of project team members, including resource constraints.
- Project Scope – Ensures that the project scope is clearly defined and documented in detail. A well-defined project scope helps avoid delays, unnecessary work, failure to achieve deliverables, cost overruns, or other unintended consequences.
- Project Time – Provides a general framework for the approach which will be taken to create the project schedule and ensures that tasks are completed on time, resources are allocated appropriately, that project performance can be measured.

This section of the Project Plan will include the scheduling tool/format, schedule milestones, and schedule development roles and responsibilities.

- Project Quality – Defines how quality management will be used to ensure that the deliverables for the project meet a formally established standard of acceptance. This section includes quality roles and responsibilities, quality control, quality assurance, and quality monitoring.
- Project Staffing – Includes the project organizational structure and how resources will be procured and managed as well as the key resources needed for the project. (See our response in the table directly below for more detail on our Staffing Plan approach.)
- Project Communications – Defines communication requirements of the project and how information will be distributed to ensure project success (see our response to Section 9.4 for more detail on our Project Communications approach).
- Project Risks/Issues – Defines the approach taken to identify and manage the risks associated with the project including likelihood, impact and mitigation strategies
- Project Procurement – Defines the necessary steps and responsibilities for procurement from the beginning to the end of a project.

---

#### Section 4, Subsection 4.29 – Project Work Plan Objective

Section 4, Subsection 4.29.1 – The Vendor should describe in the response a draft project work plan that includes project phases and milestones required from project initiation through full implementation (i.e. planning, analysis, design, development, testing, deployment, and operations).

---

#### Vendor Response:

Our proposed solution complies.

Our Summary Project Plan for this project is embedded here for your review. Veridos has assumed a project start date of October 1, 2018. Following contract award, the start date will be adjusted to match the actual start date with tasks maintaining duration but shifting accordingly.

While most of the State's the minimum standards have been included with our Summary Project Plan, we will work with the WVDMV to establish a mutually-agreed upon Project Plan.

---

#### Section 4, Subsection 4.30 - Test Plan Objective

Section 4, Subsection 4.30.1 - The Vendor should describe how they will develop, implement, and maintain a test plan, subject to the Agency's approval, in accordance with industry standards to manage testing and defect tracking for providing an efficient error correcting process to be used in system and user acceptance testing ("UAT").

---

#### Vendor Response:

Our proposed solution complies.

The Test Plan, provided by Veridos as a project deliverable, will detail the test phases identified in the Project Plan. Our implementation methodology is to ensure that the integrity of the testing phase remain in place without affecting the implementation date. This is achieved by strong Project Management discipline throughout the lifecycle of the project; utilizing tools such as the Issue Management Process, Escalation Management Process and the Change Management Process to ensure early on that the project remains on plan. As mentioned, strong Project Management is supported by a robust Test Strategy.

We have embedded Sample Test Documentation as an example. These documents are also provided in Exhibit B. Final test documentation will be provided following a collaboration with WVDMV.



Sample Test  
Documents.pdf

---

#### Section 4, Subsection 4.31 - Test Plan

Section 4, Subsection 4.31.1 - The test plan should include all the following:

431.1.1 Unit testing – on-going development testing (Vendor)

431.1.2 Integration testing – all the pieces work together (Vendor and the Agency) 431.1.3 Usability testing – user friendly, intuitive application (Vendor and the Agency) 431.1.4 Functional testing – test scenarios against requirements (Vendor and the Agency) 431.1.5 Performance testing – stress and load (Vendor)

4.31.1.5.1 Vendor to provide mechanism to create load and stress conditions

4.31.1.6 Testing of external interfaces – communication with other applications, databases, etc. (Vendor and the Agency)

4.31.1.7 Continuous regression testing – on-going to determine impact of changes (Vendor and the Agency)

4.31.1.8 Backup and recovery testing – ability to conduct a local recovery and disaster recovery (Vendor and the Agency)

---

#### Vendor Response:

Our proposed solution complies.

The assurance of any successful project is centered on its ability to dedicate a sufficient amount of time to testing, supported by a robust test strategy. As testing is one of the last phases prior to the implementation of a project, the temptation may exist to cut this phase short in order to meet an implementation date. Our implementation methodology is to ensure that the integrity of the testing phase remain in place without affecting the implementation date. This is achieved by strong Project Management discipline throughout the lifecycle of the project; utilizing tools such as the Issue Management Process, Escalation Management Process and the Change Management Process to ensure early on that the project remains on plan. As mentioned, strong Project Management is supported by a robust Test Strategy. Veridos incorporates Alpha Testing throughout the various components of the project. In addition, robust collaborative Beta Tests are performed. These tests are completed with input by the client, and involve full regression testing of all components of the solution.

In addition to the above, testing can be further augmented by a controlled pilot of the proposed solution. This would provide WVDMV an added level of comfort, ensuring that all lessons learned relative to market acceptance issues can be incorporated into the full implementation phase.

All of the following will be addressed in the Test Plan:

- Unit Testing
- Integration Testing
- Usability Testing
- Functional Testing
- Performance Testing
- Testing of External Interfaces
- Continuous Regression Testing
- Backup and Recovery Testing

Please See Section 4.30.1 and Exhibit B for our Sample Test Plan.

**Section 4, Subsection 431.2 - The test plan should include schedule for when software or other changes will be deployed to the test system and testers must receive documentation of the changes.**

**Vendor Response:**

Our proposed solution complies.

Our Project Management Methodology includes monitoring software updates and other changes and using the Change Management Process to ensure communications and protocols are following. Testers and team members will receive release notes and other relevant documentation of these changes in advance of implementation.

Please See Section 4.30.1 and Exhibit B for our Sample Test Plan.

---

**Section 4, Subsection 4.31.3 - The Agency requests a minimum of two (2) weeks' notice to schedule resources for UAT.**

---

**Vendor Response:**

Our proposed solution complies.

The target dates for UAT will be well defined and documented in the Project Plan developed in collaboration between Veridos and WVDMV. This planning will ensure WVDMV has ample time to schedule resources for UAT.

---

**Section 4, Subsection 4.32 - Test Scripts**

---

**Section 4, Subsection 4.32.1 - The Vendor should provide and execute a test script, subject to the Agency approval, prior to the implementation of equipment, configuration changes and/or software to the UAT system. the Agency should conduct testing of new equipment and/or software in UAT before any such changes are installed in production.**

---

**Vendor Response:**

Our proposed solution complies.

Veridos promotes and supports the practice of WVDMV conducting UAT prior to any new equipment and/or software being deployed. Veridos will provide test scripts approved by WVDMV in support of UAT.

---

**Section 4, Subsection 4.32.2 - Full regression testing by the Vendor on the QA system should be completed before any change is deployed to the UAT system.**

---

---

**Vendor Response:**

Our proposed solution complies.

Veridos will maintain a test environment and will conduct full regression testing prior to any change being deployed to the UAT system.

---

#### Section 4, Subsection 4.33 - Documentation for Testing

Section 4, Subsection 4.33.1 - Updated user, and/or administrator manuals should be supplied prior to the testing and acceptance phases of the project.

---

##### Vendor Response:

Our proposed solution complies.

Veridos will update user and/or administrator manuals prior to testing and acceptance of the project to ensure the manuals completely reflect the final solution.

---

#### Section 4, Subsection 4.33.2 - Vendor should supply written test cases for the Agency resources to use during UAT. Vendor Response:

Our proposed solution complies.

Veridos will provide written test cases for WVDMV resources to use during UAT.

---

#### Section 4, Subsection 4.34 - User Acceptance Testing

Section 4, Subsection 4.34.1 - The user acceptance testing (UAT) should be planned and coordinated jointly by the Vendor and the Agency project managers.

---

##### Vendor Response:

Our proposed solution complies.

Veridos will coordinate User Acceptance Testing with WVDMV in joint planning sessions.

Following UAT, we will conduct Production Testing with the WVDMV. This activity takes place after all systems have migrated final code to production and before the systems are released to the pilots. Records produced during this test can be for designated WVDMV personnel or else for fictional test "users." These cards will be used only to validate the test criteria and should be destroyed by WVDMV in a secure manner.

For this Production Test, WVDMV testers will enter the required test through the front end user interface, process records and transmit file to Veridos in the required format. Veridos will process the file, fulfill the packages (Card+Carrier+Inserts), provide required reporting and return files in the agreed format.

Following execution of the testing plan, Veridos will implement our proposed solution on a select group of pilot sites. We will work with the WVDMV to generate card production files for the records and images processed from these pilot sites and successfully issue and mail cards from our central production facility in Twinsburg, Ohio.



Once the pilot program is successful, we have prepared a plan to roll the solution out to all locations, while supporting the WVDMV to immediately include card production data for each site that is installed. This process will ensure a smooth transition – taking each site to central production as soon as local installation is confirmed by our field technicians.

Throughout the transition process and on an ongoing basis, our card production system will be available real-time to WVDMV personnel to monitor and track card production as it occurs. We will also immediately generate reports from the card production data to confirm that DL/ID cards are being properly issued and mailed for each site that is brought on-board.

Veridos will reduce WVDMV risk and will work in a conservative, yet efficient manner to bring all sites on-line with central issuance without issue.

Section 4, Subsection 434.2 - The Vendor should use standard defect tracking tools to track all feedback from testers. Final UAT should end when the system has met the standard of performance for a period of seven (7) consecutive calendar days, as determined by the Agency Project Manager in conjunction with the Agency testers.

**Vendor Response:**

Our proposed solution complies and Veridos agrees that UAT will end when the system has met the standard of performance for a period of seven consecutive calendar days. The standard of performance will be determined by WVDMV.

Section 4, Subsection 434.3 - Prior to final sign-off of user acceptance testing, all stated requirements for functionality should be in place, tested, and working free of bugs or defects, and all system performance testing must be complete and must meet required performance measures.

**Vendor Response:**

Our proposed solution complies and Veridos agrees to these terms for final sign-off of UAT.

**Section 4, Subsection 4.35 - Test Materials**

Section 4, Subsection 435.1 - The Vendor should provide test materials at no additional cost to the Agency. This includes secure paper for testing production of the temporary DL and card materials for testing the end-to-end process through the central issuance facilities.

**Vendor Response:**

Our proposed solution complies.

Veridos will provide test materials including permanent and temporary DL/ID card materials, carriers, and envelopes for testing the end-to-end process through card personalization and mailing.

---

#### Section 4, Subsection 4.36 - Test Systems

---

---

##### Section 4, Subsection 4.36.1 - The Vendor should describe how they will conduct Vendor Quality Assurance Testing. Vendor Response:

---

Our proposed solution complies.

It is a standard operating procedure for Veridos to conduct Quality Assurance Testing. Veridos has a comprehensive Quality Assurance program in place throughout the Production environment. This program incorporates both quality and security balancing procedures at each production step. In addition to the in-process QA review, Veridos has an independent QA team that randomly samples all completed Production output to ensure the highest level of quality is maintained. The total Level of sampling amounts to over 12 million+ cards annually. All production rejects are logged in our Production System (SAP).

- Automatic quality checks are performed by central issuance equipment
- Cards identified as failed are separated and each is manually inspected
- Inspection is based on: cards damaged, poor data, signature and photo quality
- Damaged card status is updated on systems and cards are remade

This entire process is tested as follows:

- Unit Testing
- User Acceptance Testing
- Regression Testing prior to change implementation

Following Quality Assurance Testing, we will conduct Production Testing with WVDMV. This activity takes place after all systems have migrated final code to production and before the systems are released to the pilots. Records produced during this test can be for designated WVDMV personnel or else for fictional test "users." These cards will be used only to validate the test criteria and should be destroyed by WVDMV in a secure manner.

Section 4, Subsection 4.36.2 - The Vendor should describe how they propose to facilitate Agency User Acceptance Testing prior to full system implementation, and during the first two years of the contract period, as well as being available for on-going testing and training for the life of the contract.

**Vendor Response:**

Our proposed solution complies.

The production deployment of the Secura FRS will consist of redundant 'Primary' and 'Disaster Recovery' environments which contain the Secura Datacenter components. These components consist of:

- Secura Application Server
- Cognitec Application Server
- SQL Database Server (Primary and Disaster Recovery mirrored)

An additional 'Test' environment will also be deployed to support User Acceptance Testing and testing of future upgrades. This Test environment will be available for ongoing testing and training for the life of the contract.

**Section 4, Subsection 4.37 - Training Plan Objective**

Section 4, Subsection 4.37.1 - The Vendor should describe how they will develop and implement a training plan that specifies the approach and steps to be taken by the Vendor to ensure that the knowledge, skills, and abilities necessary to operate the proposed system are transferred to the Agency's Train-the-Trainers (approximately 75 employees).

**Vendor Response:**

Our proposed solution complies.

A sample Training Plan is attached and is also provided in Exhibit A. This plan will be updated in collaboration with WVDMMV's team to ensure the Training Plan captures all of WVDMMV's requirements.



WV DMV Sample  
Training Plan.docx

---

#### Section 4, Subsection 4.38 - Training Guide Objective

Section 4, Subsection 4.38.1 - The Vendor should describe how their training guide will be made available to all Agency employees.

---

#### Vendor Response:

Our proposed solution complies.

Please see our attached sample training plan in our response to Section 4.37.1 and in Exhibit A. Once finalized following a collaborative effort with WVDMV, the training plan and related training documentation will be available to all Agency employees.

---

#### Section 4, Subsection 439 - Training Guide

Section 4, Subsection 439.1 - The training guide should include

439.1.1 An introduction to the Digital Driver's License application systems

4.39.1.2 A layman's explanation of the function of each component of the system

4.39.1.3 Systematic operating instructions for system components

4.39.1.4 Procedures for system start-up, daily operation, and end-of-day transactions

4.39.1.5 Guidelines for maintenance, problem solving, troubleshooting, back-up, and recovery

---

#### Vendor Response:

Our proposed solution complies.

All of these items are included in the Sample Training Plan in Section 4.37.1 and Exhibit A. This Training Plan will be finalized in collaboration with WVDMV's team.

---

**Section 4, Subsection 4.40 - User Operations Manuals Objectives**

**Section 4, Subsection 4.40.1 - The Vendor should describe how they will provide documentation for functional specifications and user manuals for all system components.**

---

**Vendor Response:**

Our proposed solution complies.

A Master Functional Specifications document will be provided and maintained during the course of the development and implementation of the program. Changes to the functionality of the solution will be documented and reviewed as they are updated and agreed to by WVDMV and Veridos.

As referenced in Section 4.39, the training will provide documentation (user manuals) and training targeted to different user levels for all system components including but not limited to: operating instructions for all system components, procedures for system start-up, daily operations, end-of-day transactions, and guidelines for maintenance, problem solving, troubleshooting, back-up, and recovery.

This information will also be validated and updated as necessary as a derivative of the Functional Specification.

---

**Section 4, Subsection 4.40.2 - The Vendor should explain how user operations manuals will be made accessible as a reference document.**

---

**Vendor Response:**

Our proposed solution complies.

The Training and User Operations information will be made available in electronic form that is printable for distribution if required. The user manuals can also be made accessible to DMV employees through shareable web programs.

---

#### Section 4, Subsection 4.41 - Technical Documentation Objective

Section 4, Subsection 4.41.1 - Vendor should explain how they will deliver and maintain technical documentation that describes the operation of all system components, including their interfaces to Agency or third-party systems. This documentation should include:

---

4.41.1.1 Complete Data Dictionary with all tables, fields, and values

4.41.1.2 System Architecture Diagrams

---

4.41.1.3 Communication Protocols

4.41.1.4 Listing of all data center equipment with DNS and IP information, operating systems, and software information including versions

---

4.41.1.5 Functional Specifications for the interaction of all components Vendor Response:

Our proposed solution complies.

Veridos will provide documentation in the form of functional specifications and user operation manuals for all system components including:

- Development of detailed Functional Specifications Document
- Development of detailed Deployment Diagrams and Networks
- Solution Documentation - Operator
- Solution Documentation - Admin
- Solution Documentation – IT staff

Veridos will provide and update operational documentation to a level sufficient to operate the support environment at agreed-upon SLAs. Veridos uses best practices for documentation standards, reviews, audit trails and release control. At minimum, the following technical documentation will be provided to the WVDMV in support of this project and to finalize the Implementation Plan. The documentation addresses the operation of all system components including interfaces to the WVDMV systems.

- Capture Manager Solution overview and customization requirements
- Instruction Set for Capture Tower with customer camera
- Documentation for "moving the test environment to production"

- Veridos Detailed Disaster Recovery "of all elements" plan
- Development of detailed Deployment Diagrams and Networks
- Solution Documentation - Technical and Procedural manual
- Capture Manager - Software Development Kit with APIs
- Project Management Plan, inclusive of the following:
  - Project Integration – Veridos typically refers to this section as the Project Management Approach that outlines the roles, responsibilities and authority of project team members, including resource constraints.
  - Project Scope – Ensures that the project scope is clearly defined and documented in detail. A well-defined project scope helps avoid delays, unnecessary work, failure to achieve deliverables, cost overruns, or other unintended consequences.
  - Project Time – Provides a general framework for the approach which will be taken to create the project schedule and ensures that tasks are completed on time, resources are allocated appropriately, that project performance can be measured. This section of the Project Plan will include the scheduling tool/format, schedule milestones, and schedule development roles and responsibilities.
  - Project Quality – Defines how quality management will be used to ensure that the deliverables for the project meet a formally established standard of acceptance. This section includes quality roles and responsibilities, quality control, quality assurance, and quality monitoring.
  - Project Staffing – Includes the project organizational structure and how resources will be procured and managed as well as the key resources needed for the project. (See our response in the table directly below for more detail on our Staffing Plan approach.)
  - Project Communications – Defines communication requirements of the project and how information will be distributed to ensure project success (see our response to

Section 9.4 for more detail on our Project Communications approach).

- Project Risks/Issues – Defines the approach taken to identify and manage the risks associated with the project including likelihood, impact and mitigation strategies
- Project Procurement – Defines the necessary steps and responsibilities for procurement from the beginning to the end of a project.
- Project Action Log – Weekly, includes Issues, Risk list, Dependencies, Change Request list, Contact Sheet
- Project Schedule / Gantt Chart – in MS Project or PDF, updated as required.
- Technical Specifications – Outlining the technical solution for card fulfillment, reporting, return file etc.
- Color Mattes (PDF Proofs) – for design confirmation

#### Section 4, Subsection 4.42 – Updates to Documentation Objective

Section 4, Subsection 4.42.1 – The Vendor should describe how they will supply and or update all training, operations, or troubleshooting manuals when a system is replaced, or software is upgraded creating a significant change to a process.

#### Vendor Response:

Our proposed solution complies.

All project documents and efforts include a version control mechanism; an example is provided below. All of our project managers and team members are familiar with Microsoft SharePoint as it is used by Veridos internally and is also used by several of our customers.

#### Tracking Release History

Document Release History

Version No	Release Date	Purpose	Author
001		Document the Change Management Plan	

#### Section 4, Subsection 4.43 - Implementation Plan Objective

Section 4, Subsection 4.43.1 - The Vendor should detail their implementation plan for every component of the system. The implementation plan should ensure all equipment and system components can be installed and functional prior to the target go live date of the system.

#### Vendor Response:

Our proposed solution complies.

Veridos will provide an Implementation Plan to ensure all equipment and system components can be installed and functional prior to the target go live date for the system.

The purpose of this document is to provide documentation on the preparation and implementation of migration of systems, data, interfaces and operations for WVDMV's new statewide driver license and identification card solution. The document will address all aspects of the implementation, focusing on these three key areas:

1. Integration of the Secura environment in the Agency's Data Center
2. Card personalization and mailing conducted by Veridos' Central Card Production Facility in Twinsburg, Ohio
3. Installation, deployment and training at WVDMV facilities

A successful Transition will bring WVDMV's sites online with an integrated image and signature capture solution with central issuance of all driver licenses and state identification cards in a secure, efficient manner that does not disrupt WVDMV's business operations.

No functionality of the current operations being transitioned will be disabled until the new Contractor provided service is demonstrated to materially conform to the requirements set forth in any related Statements of Work and operationally performs and is conformant to agreed-upon Service Levels, and has been accepted by the State of West Virginia.

The Implementation Plan will support a go live date prior to October 1, 2019.

The State of West Virginia has the right to monitor, test and otherwise participate in the implementation as described in the Implementation Plan. The State of West Virginia, the current Contractor and Veridos will develop a mutually agreed upon responsibility matrix for discrete activities and tasks as part of the transition planning process. The State of West Virginia will provide availability of the Contractor Application support

group to the Contractor according to such agreed-to responsibility matrix in the Implementation Plan.

---

#### Section 4, Subsection 4.44 - On-site Training

Section 4, Subsection 4.44.1 - As part of the Vendor's Training Plan, the Vendor should describe how they will conduct on-site Train-the-Trainer instruction. This should include duration, methods, materials provided by the Vendor, materials required of the Agency and number of trainers conducting the training.

##### Vendor Response:

Our proposed solution complies.

Please refer to the Sample Training Plan in 4.37.1 and Exhibit A which describes the elements of Train-the-Trainer instruction.

---

#### Section 4, Subsection 4.45 - Account Manager for Operations

Section 4, Subsection 4.45.1 - Vendor should provide the Agency one primary person who will be responsible for the long-term management of the contract and service level agreement. Explain the role the account manager will have in the escalation process for issues that cannot get resolved through normal processes and within agreed upon timelines.

##### Vendor Response:

Our proposed solution complies.

Our Account Manager for WVDMV is **Kathleen Synstegaard**. Kathleen has 20 years of experience with both Veridos and Entrust Datacard providing government solutions. Kathleen was the AAMVA Industry Advisory Board Chairperson last year.

Kathleen has been part of the team for 21 years, and has overseen business growth in the driver license, electronic benefit transfer (EBT), and Medicaid markets. Working to ensure that the front end solution is constantly maintained and meets the State's needs. After 19 years with Entrust Datacard, Kathleen is now the primary account manager for Veridos. Kathleen has managed multi-million dollar government and commercial projects for the US Federal Government, 21 state and provincial driver license and healthcare programs, and global national ID, healthcare and driver license programs.

An integral part of our Project Management process is the collection, analysis, and reporting of quality and service related incidents. As part of our continuous improvement initiative, we have implemented an "incident" tracking system that is utilized by all areas of our Operation. An "incident" is anything that impacts a



customer and /or production deliverable regardless of the nature or root cause of the incident, i.e. the issue can be the result of a customer initiated problem, e.g. late deliveries of inserts for card packages or the result of an internal matter to Veridos. Customer correspondence which raises a service and/or quality issue are also logged via the "incident reporting" system.

The Incident report details:

- Description of the problem
- Area describing any immediate action taken. This area is also utilized to request clarification or further information to rectify and/or request assistance in dealing with the incident.
- Customer Resolution
- Veridos Internal Resolution. This involves conducting a review of existing procedures and making any necessary changes as required. This resolution may involve a longer term as it could involve the changing of processes, training, equipment, acceptance, etc. All Incidents are tracked and reported by Department as well as by WVDMV on a regularly scheduled basis.

Our Production Coordination Team continually benchmark our internal operating practices. This benchmarking allows for the free exchange of ideas and opportunities throughout all Operations with the goal of eliminating waste and inefficiency while standardizing best practices through continuous incremental changes. The benefits of this process include:

- Facilitates communication
- Ensures incidents are reviewed against standing procedures
- Highlights opportunities for improvement
- Highlights areas for future investment
- Provides valuable data to Project Management to conduct customer meetings and reviews

As noted above, the QA Reviews and Incident Reporting form the basis for initiating the review process. All QA incidents are reviewed by the QA Department to determine root cause. Once the cause is identified, the standing procedures are reviewed to assess any gaps and implement the necessary changes.

As part of our project management discipline, cross-functional teams are in place to review the changed agenda. The function of an effective change management process is to control the changes to the operating infrastructure through the creation of a standard set of procedures and methods utilized to plan, analyze, approve, test, implement and deploy all change requests to the Production environment. This approach applies to all requests whether internally or externally driven. This structure facilitates the proper approval and sign-off process and ensures the appropriate assignment of resources to implement the request. All changes to the production environment, regardless of size and scope, must be signed-off by the process owners and coordinated by the cross-functional project teams.

Veridos has a vigorous testing discipline supported by a testing environment in both the IT and production functions. This testing often incorporates the coordinated involvement of both G+D and the customer. A sign-off process is in place to accept the changes to the Production environment as well as changes to the customer's reporting. The benefits of this process include:

- Promotes a culture that can readily adapt and accept change.
- Creates effective processes to quickly adapt to changing WVDMV requirements and market opportunities.
- Mitigates risk as change requests are subject to a thorough review process
- Promotes continuous improvement through the elimination of rework
- Improved quality of deliverables and service levels

The escalation contacts for this project are provided below.

Name	Title	Phone	Email
Kathleen Synstegaard	Account Executive	612-618-5124	kathleen.synstegaard@veridos.com
Russell Walsh	Director of Manufacturing	614-940-0990	Russell.walsh@gdmsai.com
Paul Mazzeo	President, Veridos America	703-480-2040	paul.mazzeo@veridos.com

#### SERVICE LEVEL AGREEMENT

##### Section 4, Subsection 4.46 - Replacement of Equipment / Inventory of Spares

Section 4, Subsection 4.46.1 - The Vendor should explain how their proposal will address chronic hardware issues. (Requires a support call and occurs three (3) or more times within a twelve (12) month period).

##### Vendor Response:

Our proposed solution complies.

The hardware we have proposed for this solution has been proven in the field, i.e. the Secure Capture Tower has been deployed for all of our government ID programs in North America and has been in-use for over a decade in some programs. We do not anticipate chronic hardware issues for this program. In the highly unlikely event that chronic hardware issues are incurred, Veridos will take the following steps:

- Work with the manufacturer to correct hardware defects and replace units in the field as needed

- Replace defective hardware with a comparable or better hardware solution with the approval of WVDMV

Section 4, Subsection 4.46.2 - If a repair or maintenance problem is systemic, i.e. occurring system wide, the Vendor should provide a system wide solution, which may include statewide upgrade or replacement of all units.

**Vendor Response:**

Our proposed solution complies.

Section 4, Subsection 4.46.3 - The Vendor should explain how their proposal will address equipment to be used as replacement units, as needed for service calls.

**Vendor Response:**

Our proposed solution complies.

It is always our practice to test all hardware prior to deploying it to a location and will certainly be the case on this project. Additionally, we believe in having a contingency for the contingency. Each of our Field Technicians will always arrive onsite with two tested devices just in case there is a failure with one.

The field services headquarters in Charleston will maintain an adequate supply of spare parts (whole unit spares and individual spare parts as recommended by the equipment manufacturer) as well as what is required by WVDMV as "State" spares. The field services headquarters has ample secured storage space to manage the required inventory. The inventory will be managed with a high degree of rigor using asset tagging, asset description and a well-maintained site asset log.

1. All hardware is asset tagged
2. If the failure is determined to be a hardware issue, the device will be immediately uninstalled and a replacement device will be installed and tested
3. The technicians will track the asset being removed and the asset being installed
4. This information will be included in the field service record
5. The field technician will update the help desk team before leaving the site to inform the help desk of the issue resolution
6. The help desk team will immediately update the ticket and close it
7. The field technician will return the removed asset for repair or replacement

---

#### Section 4, Subsection 4.47 - Service Response Times

Section 4, Subsection 4.47.1 - The Vendor should detail their proposed service response plan for dealing with issues related to CIF, ICW, CIDS, CIS and FRS. This should include a response in the number of working hours expected after notification based on the component and severity of the fault.

##### Vendor Response:

Our proposed solution complies.

An Incident Management Process is used to track and resolve issues that arise within any area of the solution. The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on West Virginia's operations, thus ensuring that the best possible levels of service quality and availability are maintained. Severity 1 issues are handled with top priority and an "all hands on deck" approach. Veridos and Excel Management will work with the WVDMV to determine specific SLAs for each severity level.

---

#### Section 4, Subsection 4.48 - Help Desk Support

Section 4, Subsection 4.48.1 - The Vendor should explain their Help Desk capabilities and responsibilities. This should include hours of operation, response times, remote access requirements, field service technician involvement, and escalation process.

##### Vendor Response:

Our proposed solution complies.

Our help desk systems include; 1) A web portal to submit service requests. 2) An established toll free number. 3) A ticketing system.

- The help desk system will be available from 7:00 AM to 8:00 PM during weekdays and 7:00 AM to 2:00 PM on Saturdays.
- The help desk will be staffed from A service request from WVDMV would be submitted through our web portal. A service request may also be submitted by placing a call to our 800 number or by email though the most efficient option is the use of the web portal.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes
- A service ticket will be created by the help desk team. The ticket and its status will be visible to the WVDMV team through the web portal.



- Our help desk team will immediately contact the site that is reporting the issue immediately and execute the troubleshooting protocol.
- If the issue was not resolved by the troubleshooting protocol then a field technician will be immediately dispatched and will be onsite within the agreed upon SLA.
- All field technicians will have two devices in their possession as well as any other materials that may be needed to service the devices (i.e., cabling, patch cables, etc.).
- The field technician will quickly execute the troubleshooting protocol again. The technician will determine if the failure is due to a hardware or software issue.
  - If the failure is determined to be an Agency issue then the technician will immediately contact WVDMV technical support team to report the issue and continue to troubleshoot the issue in collaboration with the WVDMV technical team.
  - If the failure is determined to be a hardware issue the device will be immediately uninstalled. A replacement device will be installed and tested. The onsite contact will be kept updated throughout the service call. The technician will fill out a form to track the asset being removed and the asset being installed. The site log would also be updated. This information would be included in the field service record.
- The field technician will update the help desk team before leaving the site as to the resolution of the ticket.
- The help desk team will immediately update the ticket and close it.
- The help desk will review and acknowledge receipt of all tickets within 15 minutes. The resolutions will be recorded and reconciled within the web-based help desk system for the consumption of fellow Help Desk Operators and facilitating the WVDMV to generate reports.
- Veridos will provide an incident report via the web-based tracking system to the WVDMV upon completion of a service call detailing the actions taken to resolve the problem and status of the problem.
- The field technician would return the removed asset to the field services headquarters to be repaired or returned to the manufacturer.
- The Veridos team will submit monthly reports to WVDMV related to all service requests received for the month. The report will highlight the following service request data:

**Volume Summary** - Each month a summary of all service requests will be provided by the Contractor that quantifies problem types, resolution types, etc. by equipment type. This information will include a previous twelve months to help identify trends.

**Inventory Report** - Each month a comprehensive inventory is reported that shows the location and status of all Contractor equipment. This report will track all installed equipment, spare pool hardware, and equipment out for repair. Any equipment that is permanently removed from service will be considered "retired" and can no longer be transacted against, but a record should be maintained in an inactive status for historical purposes.

**Performance Report** - This monthly report will list all of the performance data against SLA requirements including; response time, ETA, arrival time, time to repair and close time against WVDMV business hours. This data is generated monthly and published with a twelve-month history for trend analysis.

**Ad Hoc Reports** - Contractor will provide reports to WVDMV on request that will in general be specific to WVDMV needs regarding: problems, call volume analysis and comparison at the site level, site history reporting, operator history reporting etc.

The escalation process for the help desk will be determined in collaboration between WVDMV and Veridos, based upon WVDMV's requirements.

An Incident Management Process is used to track and resolve issues. The primary goal of the Incident Management process is to restore normal service operation as quickly as possible.

A service ticket will be created by the help desk team. The ticket and its status will be visible to the WVDMV's internal support team through our web portal.

Our help desk team will immediately contact the site that is reporting the issue and execute the troubleshooting protocols.

If the issue was not resolved by the troubleshooting protocol then a field technician will be immediately dispatched and will be onsite within the SLA.

If the failure is determined to be a hardware issue the device will be immediately uninstalled. A replacement device will be installed and tested. The onsite contact will be kept updated throughout the service call. The technician will track the asset being removed and the asset being installed. This information would be included in the field service record.

- The field technician will update the help desk team before leaving the site as to the resolution of the ticket.
- The help desk team will immediately update the ticket and close it.

- The field technician will return the removed asset to the field services headquarters to be repaired or returned to the manufacturer.

#### Section 4, Subsection 4.49 – Help Desk Reporting System

Section 4, Subsection 4.49.1 – Vendor should explain their help desk reporting system used to report, log, and track support issues, including the how the Agency will access the system, automatic tracking of issues and notification alerts, and report generation capabilities.

#### Vendor Response:

Our proposed solution complies.

Our help desk systems include; 1) A web portal to submit service requests. 2) An established toll free number. 3) A ticketing system.

- The help desk system will be available from 7:00 am to 9:00 pm during weekdays and on Saturday as needed.
- The help desk will be staffed from A service request from WVDMMV would be submitted through our web portal. A service request may also be submitted by placing a call to our 800 number or by email though the most efficient option is the use of the web portal.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes
- A service ticket will be created by the help desk team. The ticket and its status will be visible to the WVDMMV team through the web portal.
- Our help desk team will immediately contact the site that is reporting the issue immediately and execute the troubleshooting protocol.
- If the issue was not resolved by the troubleshooting protocol then a field technician will be immediately dispatched and will be onsite within the agreed upon SLA.
- All field technicians will have two devices in their possession as well as any other materials that may be needed to service the devices (i.e., cabling, patch cables, etc.).
- The field technician will quickly execute the troubleshooting protocol again. The technician will determine if the failure is due to a hardware or software issue.
  - If the failure is determined to be an Agency issue then the technician will immediately contact WVDMMV technical support team to report the issue and continue to troubleshoot the issue in collaboration with the WVDMMV technical team.

- If the failure is determined to be a hardware issue the device will be immediately uninstalled. A replacement device will be installed and tested. The onsite contact will be kept updated throughout the service call. The technician will fill out a form to track the asset being removed and the asset being installed. The site log would also be updated. This information would be included in the field service record.
- The field technician will update the help desk team before leaving the site as to the resolution of the ticket.
- The help desk team will immediately update the ticket and close it.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes. The resolutions will be recorded and reconciled within the web-based help desk system for the consumption of fellow Help Desk Operators and facilitating the WVDMV to generate reports.
- Veridos will provide an incident report via the web-based tracking system to the WVDMV upon completion of a service call detailing the actions taken to resolve the problem and status of the problem.
- The field technician would return the removed asset to the field services headquarters to be repaired or returned to the manufacturer.
- The Veridos team will submit monthly reports to WVDMV related to all service requests received for the month. The report will highlight the following service request data:

**Volume Summary** - Each month a summary of all service requests will be provided by the Contractor that quantifies problem types, resolution types, etc. by equipment type. This information will include a previous twelve months to help identify trends.

**Inventory Report** - Each month a comprehensive inventory is reported that shows the location and status of all Contractor equipment. This report will track all installed equipment, spare pool hardware, and equipment out for repair. Any equipment that is permanently removed from service will be considered "retired" and can no longer be transacted against, but a record should be maintained in an inactive status for historical purposes.

**Performance Report** – This monthly report will list all of the performance data against SLA requirements including; response time, ETA, arrival time, time to repair and close time against WVDMV business hours. This data is generated monthly and published with a twelve-month history for trend analysis.

**Ad Hoc Reports** - Contractor will provide reports to WVDMV on request that will in general be specific to WVDMV needs regarding: problems, call volume analysis and comparison at the site level, site history reporting, operator history reporting etc.

The escalation process for the help desk will be determined in collaboration between WVDMV and Veridos, based upon WVDMV's requirements.

An Incident Management Process is used to track and resolve issues. The primary goal of the Incident Management process is to restore normal service operation as quickly as possible.

A service ticket will be created by the help desk team. The ticket and its status will be visible to the WVDMV's internal support team through our web portal.

Our help desk team will immediately contact the site that is reporting the issue and execute the troubleshooting protocols.

If the issue was not resolved by the troubleshooting protocol then a field technician will be immediately dispatched and will be onsite within the SLA.

If the failure is determined to be a hardware issue the device will be immediately uninstalled. A replacement device will be installed and tested. The onsite contact will be kept updated throughout the service call. The technician will track the asset being removed and the asset being installed. This information would be included in the field service record.

- The field technician will update the help desk team before leaving the site as to the resolution of the ticket.
- The help desk team will immediately update the ticket and close it.
- The field technician will return the removed asset to the field services headquarters to be repaired or returned to the manufacturer.

**Section 4, Subsection 4.50.1 - The implementation plan should include:**

**4.51.1.1 Listing of the Vendor resources for each implementation task**

**4.51.1.2 Plan for conducting site surveys of all the Agency facilities**

**4.51.1.3 Schedule including delivery and installation of equipment and training**

**4.51.1.4 Plan for migrating data from current image database**

**4.51.1.5 Plan for installation and deployment of all data center equipment and systems**

**4.51.1.6 Plan for installation and deployment of all central issuance facility equipment and production procedures**

**4.51.1.7 The Vendor should provide as a part of their proposal, a sample plan for the implementation and rollout of the solution to all locations, including timeline.**

**Vendor Response:**

Our proposed solution complies.

Veridos will provide an Implementation Plan to ensure all equipment and system components can be installed and functional prior to the target go live date for the system.

The purpose of this document is to provide documentation on the preparation and implementation of migration of systems, data, interfaces and operations for WVDMV's new statewide driver license and identification card solution. The document will address all aspects of the implementation, focusing on these three key areas:

1. Integration of the Secura environment in the Agency's Data Center
2. Card personalization and mailing conducted by Veridos' Central Card Production Facility in Twinsburg, Ohio
3. Installation, deployment and training at WVDMV facilities

A successful Transition will bring WVDMV's sites online with an integrated image and signature capture solution with central issuance of all driver licenses and state



identification cards in a secure, efficient manner that does not disrupt WVDMV's business operations.

No functionality of the current operations being transitioned will be disabled until the new Contractor provided service is demonstrated to materially conform to the requirements set forth in any related Statements of Work and operationally performs and is conformant to agreed-upon Service Levels, and has been accepted by the State of West Virginia.

The Implementation Plan will support a go live date prior to October 1, 2019.

The State of West Virginia has the right to monitor, test and otherwise participate in the implementation as described in the Implementation Plan. The State of West Virginia, the current Contractor and Veridos will develop a mutually agreed upon responsibility matrix for discrete activities and tasks as part of the transition planning process. The State of West Virginia will provide availability of the Contractor Application support group to the Contractor according to such agreed-to responsibility matrix in the Implementation Plan.

Our expert technicians will install the workstations, set up the back end infrastructure to interface with Veridos systems, and conduct full testing, including: unit testing with full QA, integration testing, usability testing, functional testing, performance testing with load and stress condition testing, external and internal interface testing, regression testing, user acceptance testing, and full end-to-end and performance testing.

Once the system is fully tested, the Veridos team will provide a full staged rollout including site assessments, installation and training program to the WVDMV locations. The Veridos installation teams will assess each site, install all workstation software and peripherals, and provide full training, as well as instructional documents and overview fliers, to key personnel for each location, as we transition the sites to the new solution.

---

#### Section 4, Subsection 4.51 - 14 Day Pre-Post Support Plan

Section 4, Subsection 4.51.1 - The Vendor should provide a comprehensive plan for product support that consists of a 7-day period prior to and a 7-day period immediately following implementation.

#### Vendor Response:

Our proposed solution complies.

Veridos understands that the days leading up to and following implementation require an "all hands on deck" approach to ensure everything goes smoothly. Our help desk

personnel are capable of verifying preliminary checks with the WVDMV representative prior to dispatching a technicians as needed.

The help desk will be backed by local technicians situated strategically throughout the State of West Virginia as a fully prepared Mobile Service Response team. Each member of the Response team will be outfitted with a completely equipped response vehicle, stocked with all necessary equipment to ensure a quick response and resolution to any issue that cannot be corrected over the phone.

Each Response team member will be fully trained and certified to meet the service requirements of our solution. In addition to repair supplies, each Response team member will have an inventory of full replacement units to allow for quick resolution of nearly any problem by, when necessary, simply swapping out an affected device.

Veridos acknowledges all of the maintenance and support requirements. Veridos has included our hardware maintenance plan at no additional cost to the State and will remain in place for the full-term of the contract. The critical elements of our support model are in absolute alignment with the requirements and include the following:

- The field team designates one of their senior technicians as the Subject Matter Expert of the respective hardware.
- The subject matter expert, in collaboration with WVDMV, constructs documentation regarding the technical specifications of any hardware. The documentation also includes standard troubleshooting protocol for each device. This documentation will include all technical manuals from the equipment OEM. These will be provided and maintained in written and CD format to assist field technicians, and an electronic copy of the most current documentation provided to WVDMV for central maintenance and reference.
- There will be a minimum of 10 field technicians who will be supporting the DL/ID devices. The field team supporting the hardware will be selected based on the required Service Level Agreement that must be achieved.
- All field technicians that will be supporting the hardware are provided the technical and troubleshooting documentation and receive training from the subject matter expert. The training will be conducted in person with each technician that will be supporting the devices and will be "hands on".
- All equipment and hardware provided as part of Veridos' solution will be of new manufacture. Staging and testing will be conducted by field technicians prior to installation, to ensure all hardware is installed in good working order. Approval will be obtained from WVDMV prior to installation.
- Each field office will always have a supply of all materials required to service these devices in their possession so that they will be able to respond quickly to service requests. The field services headquarters in will maintain and manage the

inventory of devices and supplies that will be distributed and replenished to the field technicians as needed. The spare parts pool will be purchased by Veridos at the outset of the contract to ensure their availability. Veridos has allocated the required inventory stock in our purchasing plan. This inventory will be constantly tracked in a site inventory log.

**Section 4, Subsection 4.51.2 - Support should be available on-site at the agency headquarters in Kanawha City. Support should be available to installation technicians and the Agency staff during installation and configuration of any system component.**

**Vendor Response:**

Our proposed solution complies.

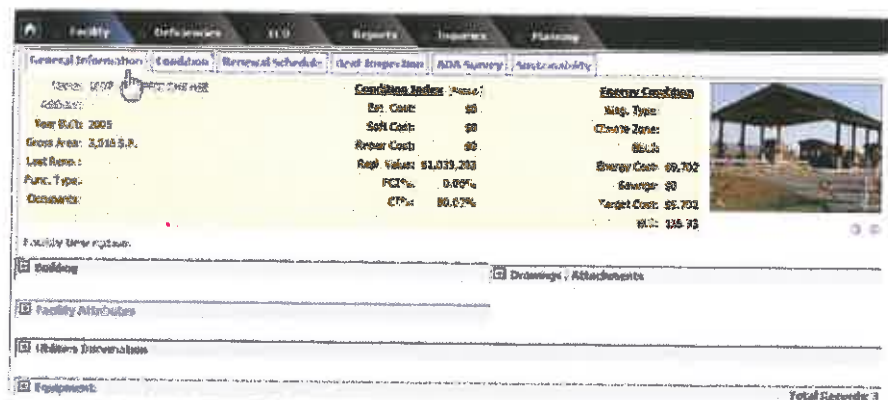
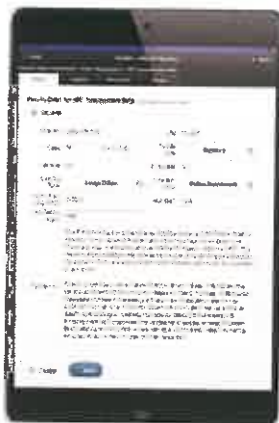
Based upon the requirements outlined in this RFP, Veridos has identified and is planning to provide the following deployment activities.

Veridos will be responsible for complete installation and testing of all of the components of the system. Our expert technicians will install the workstations, set up the back end infrastructure to interface with Veridos systems, and conduct full testing, including: unit testing with full QA, integration testing, usability testing, functional testing, performance testing with load and stress condition testing, external and internal interface testing, regression testing, user acceptance testing, and full end-to-end and performance testing.

Once the system is fully tested, the Veridos team will provide a full staged rollout including site assessments, installation, start-up training program to the WVDMV locations. The Veridos installation teams will assess each site, install all workstation software and peripherals, and provide full training, as well as instructional documents and overview fliers, to key personnel for each WVDMV location, as we transition the sites to the new solution.

To facilitate a quick and smooth transition to the new solution at the WVDMV locations, the Veridos team will perform site assessments prior to the installations taking place. The Veridos team has a long history performing site assessments stemming from our experience with critical infrastructure in federal, state, local, and commercial markets.

Our team has expertise in using assessments extensively for the work throughout the life cycle of the asset, placing a strong emphasis on safety, security, and quality, along with operational readiness and efficiency. Following are screen shots of the application for which we have conducted field assessments using mobile toolkits in the field – some using our mobile toolkits to collect data, photos and, when required, mark-up blueprints and other drawings to identify issues.



The Veridos team will meet with the WVDMV team to collaboratively verify and finalize requirements for the sites prior to the installation of the workstation software and peripherals to ensure the sites are ready for the transition activity. Following completion of requirements gathering, we will present a proposed template in the Transition Plan to ensure uniformly conducted site assessments at every WVDMV location. Compiling current and accurate details relating to each individual location is vital to ensuring efficient installation of the new equipment.

Upon approval of the plan, the Veridos team will begin conducting the site assessments to help the WVDMV personnel be better prepared for the installations of the new system.

Veridos team members will contact WVDMV personnel, as designated by WVDMV, to schedule the planned site visit. We will send notifications to each contact person prior to the date of the visit to ensure that delegated parties identified by WVDMV will be available for the survey.

During this initial contact, we will perform a brief interview requesting information that will help expedite the onsite visit, ensure the most efficient use of time for the WVDMV personnel, and eliminate any disruption or customer inconvenience at the centers.

Information requested during our initial call will include, but may not be limited to, date and time for the visit; confirmation of appropriate contact person and contact information; availability of existing floor, electrical, or other plans; photographs; and any outstanding facility issues. The site survey template will also be provided prior to the visit to help inform and prepare the WVDMV personnel in advance of the scheduled site visit.

During the onsite site survey visit, a Veridos team member will conduct a thorough survey of the location, including taking measurements of workstation areas and confirming the location and dimensions of the area for secure storage. A site survey report will subsequently be completed and delivered to WVDMV for evaluation.

The site survey report will include:

- Facility layout
  - Location of workstation(s)
- Appropriate measurements
  - Workstation area
- Electrical requirements
- Cabling requirements
- Other recommendations or concerns

The Veridos team will work with the WVDMV team to complete the site assessments at all Deputy Registrar locations well in advance of equipment installation activities and will provide the site survey reports for each contact person.

The Veridos team performing equipment installation are fully trained technicians who will have completed comprehensive training and obtained certification from the equipment manufacturer. Information gained from evaluation reports based on the previously completed site visits will be used for efficient installation. During the installation, a detailed checklist, like the example that follows, will be followed by the on-site service technicians:

Driver License Center/Photo License Center Site Acceptance Checklist		
	Task Information	Pass/Fail
1	Site Address:	
2	Region Number:	
3	Date of Inspection:	
4	Inspector Name:	
5	Inspector Title:	
6	Phone No. (Area Code & No.):	
7	Assigned Card Printer (Make & Model)	
8	Serial Number	
9	Signature Pad (Make & Model)	
10	Serial Number	
11	Barcode Scanner (Make & Model)	
12	Serial Number	
13	Image Capture Tower	
14	Serial Number	
15	Secure Client Laptop	
16	Serial Number	
17	Complete Client Workstation Upgrade	
18	Remove existing hardware	
19	Install new PC, Monitor, etc.	
20	Boot up PC and following a successful local login, then let the Windows 7 operating system install itself to the new hardware, downloading and installing all new updates drivers, etc.	
21	Install and configure workstation, network, and login to the workstation once network is checked, and all devices are properly installed via device manager.	
22	Join the workstation to the domain using the provided username and password.	
23	Reboot, then log in with a Secure Client's credentials and verify all required domain accounts is granted for the employees of that office, that we have an established network connection, and that the required hardware is properly installed and functioning.	
24	Complete install and test of Image Capture Station	
25	Uninstall and download vision inspection or Secure Capture Tower software, and capture test.	
26	Setup the operation on this laptop or monitor.	
27	Connect Secure Capture Tower and all parts to be provided (video cables, Secure and standard client work station card, Power and Grounding to Tower).	
28	Connect all Secure Client devices to Power up Secure Capture Tower and follow the Standard Secure Capture Tower setup directions.	
29	Log in to Secure client.	
30	Verify client computer recognizes all devices.	
31	Install all devices the Capture Manager Design Center.	
32	Secure Capture Tower – set alarm, then remove, and mark device location on counter top.	

- Unpack and conduct a visual inspection of the workstation hardware
- Set up the equipment on workstation area
- Install new workstation, peripherals and software

- Boot up workstation and log in, allowing computer to run all necessary drivers and scripts
- Shut down the client workstation, restart, and log in to the workstation to verify device installation
- Join the workstation to the domain using the assigned computer name
- Reboot the workstation and log in with our domain credentials to verify:
  - Domain access for the Team Members of that office
  - Network connection
  - Functionality of required applications, hardware, and peripherals
- Connect the peripherals to a grounded facility power source and conduct "stand-alone" power up test
- Power off the Secure Capture Tower
- Connect all devices to client computer, power up the Secure Capture Tower, and follow the Secure Capture Tower setup
- Log in to the Secura client
- Verify the computer recognizes all devices and test them via the Capture Manager Design Center
- On the Secure Capture Tower, set zoom, flash intensity, and mark tower position on countertop
- Perform an end-to-end test enrollment
- Using Capture Manager Design Center Application, position and make mechanical adjustments to align the Capture Tower via live preview
- Mark final location/position of the Capture Tower base on table and secure Capture Tower
- Launch the Secura application
- Scan test form to locate test record
- Capture image and signature
- Print test temporary DL/ID
- Receive acceptance signoff from WVDMV key personnel and/or designated Team Member(s)

Our local technicians will visit the WVDMV locations frequently during the first 90 days of operations to see how well the transition is taking place. The information gathered during these site visits will be shared with WVDMV and will be used to correct any issues that arise during the first 90-day period.

## Attachment B: Mandatory Specification Checklist

### FACILITY IMAGE & SIGNATURE CAPTURE WORKSTATION (ICW) REQUIREMENTS

Section 4, Subsection 5.1 - Vendor must install digitized image capture workstations at each of the twenty-seven (27) locations as defined in Attachment D. At the time of installation, all equipment must be new and in good working order.

#### Vendor Response:

Our proposed solution complies.

Veridos will be responsible for complete installation and testing of all of the components of the system. Our expert technicians will install the workstations, set up the back end infrastructure to interface with Veridos systems, and conduct full testing, including: unit testing with full QA, integration testing, usability testing, functional testing, performance testing with load and stress condition testing, external and internal interface testing, regression testing, user acceptance testing, and full end-to-end and performance testing.

Once the system is fully tested, the Veridos team will provide a full staged rollout including site assessments, installation and training program to the WVDMV locations. The Veridos installation teams will assess each site, install all workstation software and peripherals, and provide full training. In addition to the workstation PC, Veridos will provide equipment at each of the 27 locations defined in Attachment D. All equipment will be new and in good working order.

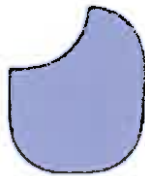
## Secure Image Capture Tower - Specifications



- Base plate: 8.0 in. x 8.0 in. (20.32 cm x 20.32 cm)
- Size - 13.0 in. x 8.0 in. x 32.0 inches in height.
- Weight - 22.0 lbs. (10.0 kg) system
- Power - 120 VAC / 60Hz
- Operating Temp - 60°F to 95°F (15°C to 35°C)
- Operating Humidity - 20% to 80% RH non condensing
- Storage - 5°F to 140°F (-15°C to 60°C)
- Flash Working Range - 3.0 to 12.0 feet (1.8<sup>m</sup> to 4.6<sup>m</sup>)
- Flash Cycles – rated for 250,000 cycles
- Flash, External - 100WS, 120 VAC Flash Recycle time – average of 5 seconds or less for re-take support
- Camera Resolution – 18.0 megapixel or greater digital SLR photo capture
- Camera Zoom – Digital Auto Zoom or Manual Zoom
- Camera Tower Range – Vertical Adjustment - 10 inches
- Camera Tower Range – Rotation – tilt range of 30 degrees - allows for seated or standing subjects

- Camera Tower Security – hardware mountable to a countertop – theft and vandalism resistant
- Camera API Compatibility – Windows XP or 7 via Datacard Secure Camera Tower iCap license
- Connectivity – USB 2.0 - Multiple USB ports in support of computer and peripheral connectivity
- Connectivity – Ease of Connectivity – Single Wire data connection with built in USB hub for peripherals

**Photo Backdrop – A Professional Photo Backdrop System consisting of:**



- Screen Size – 36" Wide x 48" or 48" Wide x 60" Tall when expanded
  - Size to be chosen subject to contract award and SOW
  - Includes clips for mounting to backdrops stands
- Frame Material – Internal Self Expanding Frame
- Storage / Transport Case – Zippered nylon case
- Color – Blue one side, White opposite side
- Operating Temp - 50° F to 120° F
- Support Hardware – Wall / Ceiling Clips – for mounting Backdrop clips to a wall or ceiling

**Signature Tablet - SigGem® 5.7 Color Display or Equivalent**



- Full-color TFT VGA (640x480) LCD Display
- Displays the signature on the signature pad, as well as the computer screen.
- Tempered glass signing surface w. internal high-performance E/M digitizer.

- Rated for 2 million signatures
- Pen Type - Active low-power, rugged E/M pen, battery-less
- Pen Settings - 1024 pressure level option
- Dimensions - 7.2" x 6.6" x 2.1" sloping (180 x 160 x 54 mm)
- Signing area - 4.6" x 3.4" (118mm x 86mm)
- 377 Points per second.
- 410 points per inch (programmable)
- Dual Serial / USB connectivity
- Encryption Capabilities - AES optional, FIPS-197 compliant
- APIs provide for interactive text, graphics, pen-tap hotspots and checkboxes
- Forensic-quality .SIG data capable of examination and authentication.
- FCC, RoHS, and WEEE compliant

**Document Scanner – Kodak Alaris – S2000 Series - ADF Type**



- Shown with and without Optional Passport Scanner
  - Scanning Technology - Camera Based Page Sensing
  - Daily Duty Cycle – 5000 scans per day
  - Pages Per Minute (PPM) - up to 50
  - Optical Resolution 600 dpi
- Output Resolution :
  - 175 / 100 / 150 / 200 / 240 / 250 / 300 / 400 / 500 / 600 / 1200
- Max / Min Document Size:
  - 216 mm x 356 mm (8.5 x 14 in.) / 52 mm x 52 mm (2.08 in. x 2.05 in.)
- Supports shared scanning from multi-workstations
- Handles Real ID breeder docs such as birth certificates, utility bills, etc
- Handles small documents such as ID cards, embossed hard cards, etc
  - Hard card (license) transport in both landscape or portrait
- Power – 120 / 240 Volt – 50 / 60 Hz
- Standby/Sleep mode/Network Standby: <36 Watts

- 1.5" Color Graphic Display
- Pause and resume or Jam resume modes
- Weight: 3.3 kg (7.2 lbs.)
- Depth: 204 mm (8.0 in.), not including input tray and output tray
- Width: 312 mm (12.3 in.)
- Height: 182.5 mm (7.2 in.), not including input tray
- Depth with Input Tray 269 mm (10.6 in.)
- Height with Input Tray 231.6 mm (9.1 in.)
- Paper Thickness and Weight 34-413 g/m2
- Feeder Up to 80 sheets of 80 g/m2
- Connectivity USB 3.0 (cable included)
- File Format Outputs - Single and multi-page:
  - TIFF, JPEG, RTF, BMP, PDF, TXT, PNG, CSV, Word and Excel
- Agency Approvals – Meets all UL, CSA, CE, and FCC requirements

#### **Document Scanner – Passport Reader Accessory**



#### **Passport Scanner Accessory - Kodak Alaris S2000 Series**

- Integrates directly into the primary S2000 Series ADF Scanner
  - No additional power cords or USB power required
- Docks directly beneath the primary scanner for a compact footprint
- Automatically triggers scanning when passport is placed into the scanner
- Able to scan two passport pages at once
- Able to scan both US and International passports of varying thicknesses
- Captures images in 2-3 seconds at 300 dpi settings
- Optical resolutions up to 1200 dpi
- Output resolutions 75, 100, 150, 200, 240, 250, 260, 300, 400, 500, 600 and 1200 dpi
- Supports reading of other small, fragile, or high value documents
- Max doc size 5" x 7.3 in" (27 x 186 mm)

- Height x width x length (2.8 x 12 x 10 in.) (72 x 306 x 255 mm)
- Weight 3.5 lbs. (1.6 kg )

**Paper Printer – HP LaserJet Pro – For Interim ID/DL**



- HP LaserJet Pro M402n – or equivalent - Laser Printer
  - Technology - Monochrome – laser
  - Resolution – HP FastRes 1200 dpi
  - Monthly duty cycle – up to 80,000 pages
  - Recommended volume – up to 4000 / month
  - Paper Trays - Standard – 2 (100 pg. and 250 pg.)
  - Connectivity USB 2.0, and 10,100,1000 Gb Ethernet
  - Printer Toner Cartridge – HP26A or Extended HP26X
  - Dimensions - WxDxH - 15 x 14.06 x 8.5 in
  - Weight - 18.92 lbs.

---

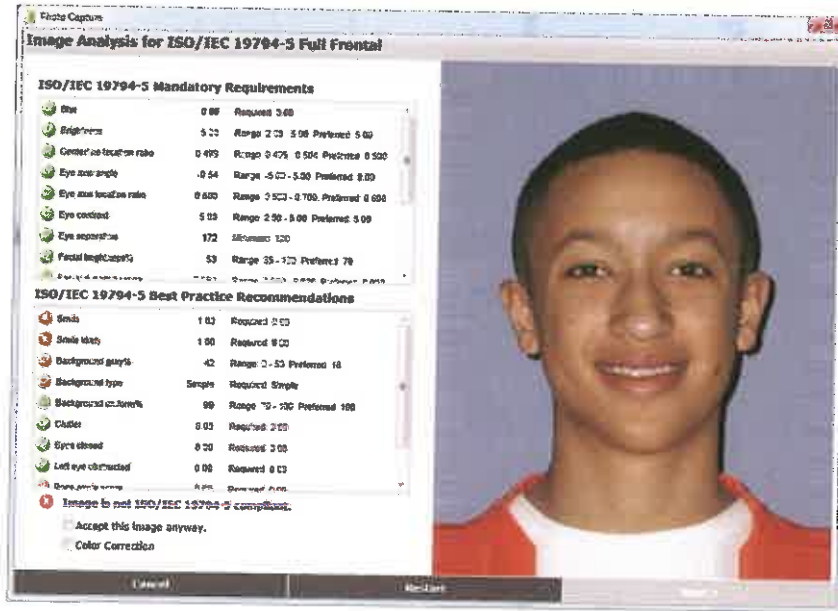
**Section 4, Subsection 5.2 – Functional – ICAO**

**Section 4, Subsection 5.2.1 – Image must meet ISO/IEC 19794-5:2011 Information Technology – Biometric Data Interchange Formats – Part 5: Face Image Data or current specifications.**  
[http://www.iso.org/iso/home/store/catalogue\\_ics/cataloguedetailics.htm?csnumber=50867](http://www.iso.org/iso/home/store/catalogue_ics/cataloguedetailics.htm?csnumber=50867)

**Vendor Response:**

Our proposed solution complies.

Capture Manager software includes an algorithm that provides an automatic cropping routine for cropping and analyzing images against ICAO and ISO/IEC 19794-5 specifications. The results are shown to the operator; if compliance is not obtained with the initial image capture, the operator can then use additional tools to re-crop the image, click 'Restart' to go back to the live preview to take another picture, or accept the image as is. The screenshot below shows the ISO/IEC 19794-5 image checks that are performed by the capture component of our solution.



**Section 4, Subsection 5.2.2 The system must be capable of ICAO image quality checks. Vendor Response:**

Our proposed solution complies.

The solution includes an internal ICAO-compliant quality checking algorithm, performed during the capture process that eliminates records being sent that would not be satisfactory for use in the FRS.

Automatic ICAO photo quality checks are performed on photos captured by the system. Images are rechecked for ICAO compliance if any manual cropping is performed.

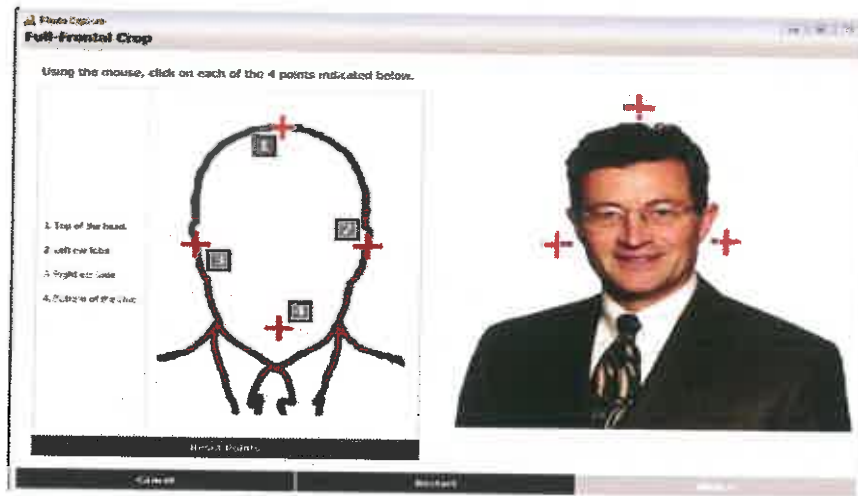
The specific ICAO checks to be performed, and the acceptable threshold levels, are configurable by the System Administrator. This allows the solution to be tailored to WVDMV's needs without interfering with the objective of capturing ICAO-complaint images.

An operator also has the ability to make adjustments to the placement of the head in the window if necessary.

An optional Color Correction step can be provided in the workflow, if desired. This option would provide operators the ability to enhance the image quickly and easily by choosing one of the images in the left hand pane. All the ICAO and photo consistency checks are run on the chosen image to ensure the image meets the required quality specifications.



The system allows for the manual capture and retaking of images. The image checks performed include facial feature identification, image cropping, image placement, and checks for lighting. Users can also manually crop the image, at which time it is checked for ICAO compliance. A supervisory override is available, if required, to allow images of individuals who have unique characteristics that may show up in the background of an ID card photo; for example, a high-backed wheelchair in an accessible station.



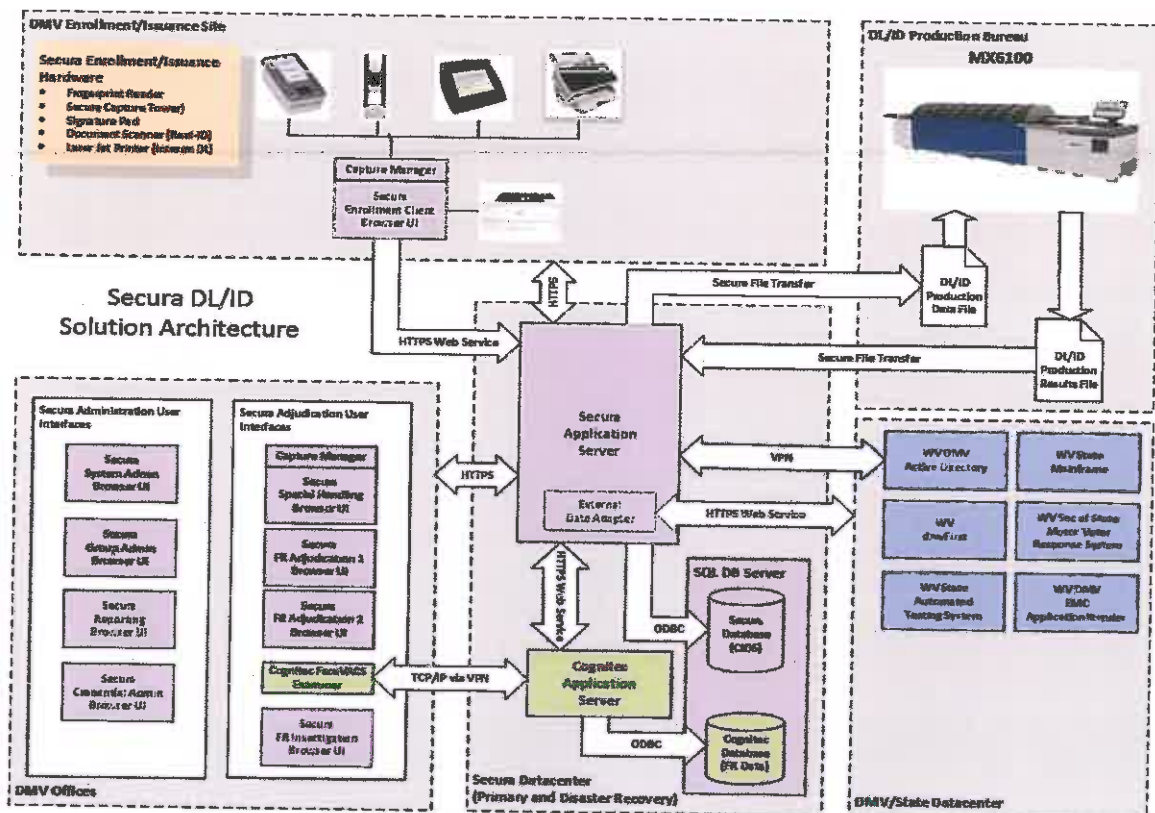
## Section 4, Subsection 5.3 - Functional - Interface with Agency Internal Systems

Section 4, Subsection 5.3.1 - Must interface with the dmVFIRST Web Application, a component of dmVDRIVES, via a web service call. This interface ensures the appropriate fees are collected based on the type of credential issued.

### Vendor Response:

Our proposed solution complies.

Our proposed solution includes a component called Data Adapters. Data Adapters are the mechanisms used to exchange data with other systems and interfaces. Data Adapters support most commonly used data exchange technologies such as but not limited to web services, XML, SOAP, XML, Rest, and can also incorporate proprietary methodologies if necessary. These Data Adapters will be used to support these interfaces as shown in the diagram below.



---

Section 4, Subsection 5.3.2 - Must display voter registration questions on the signature pad and send the returned responses to the West Virginia Secretary of State's Office, to include applicant signature, required per West Virginia Code §3-2-11.

**Vendor Response:**

Our proposed solution complies.

Our proposed signature capture solution will display voter registration questions and capture applicant signature. This captured data will be collected and stored in the database.

As described in our response to Section 5.3.1, Data Adapters will be used to send these returned responses on the voter registration questions along with the applicant signature to the West Virginia Secretary of State's Office.

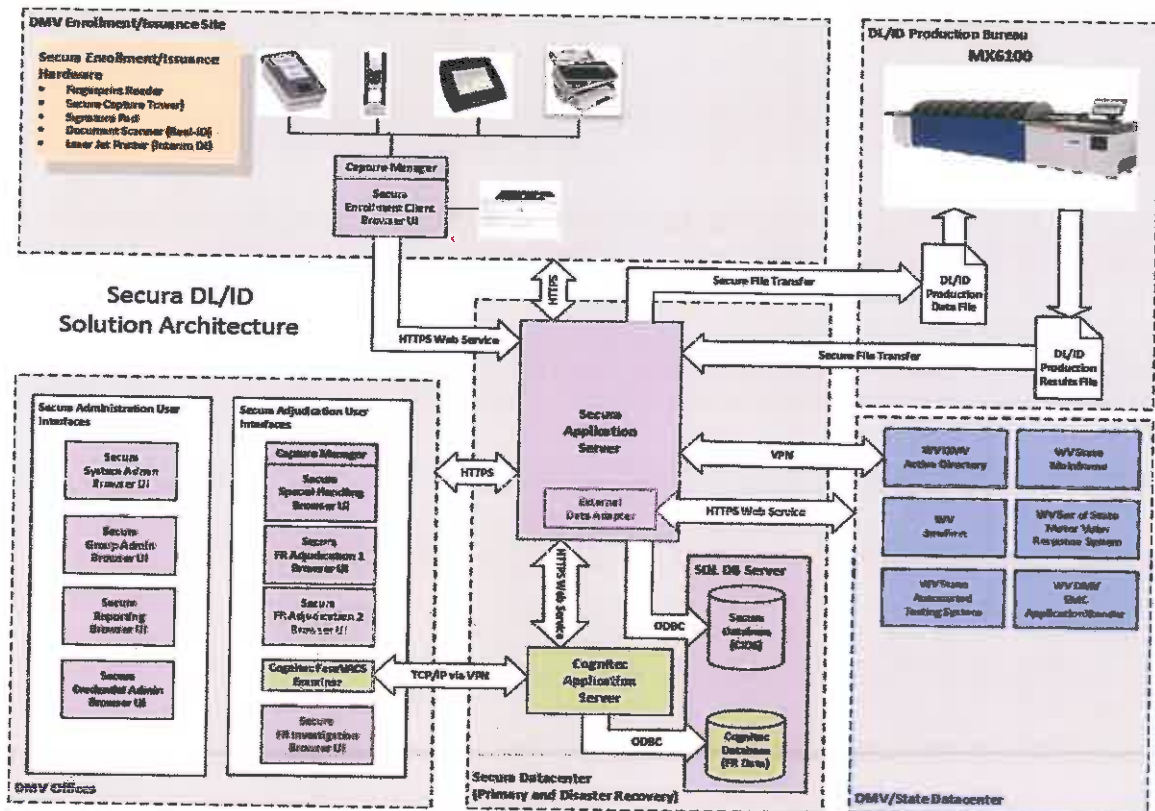
---

Section 4, Subsection 53.3 - Must interface with the State's mainframe system, that serves as the primary driver record, ensuring the applicants status and availability to receive a credential.

**Vendor Response:**

Our proposed solution complies.

Our proposed solution includes a component called Data Adapters. Data Adapters are the mechanisms used to exchange data with other systems and interfaces. Data Adapters support most commonly used data exchange technologies such as but not limited to web services, XML, SOAP, XML, Rest, and can also incorporate proprietary methodologies if necessary. These Data Adapters will be used to support these interfaces as shown in the diagram below.

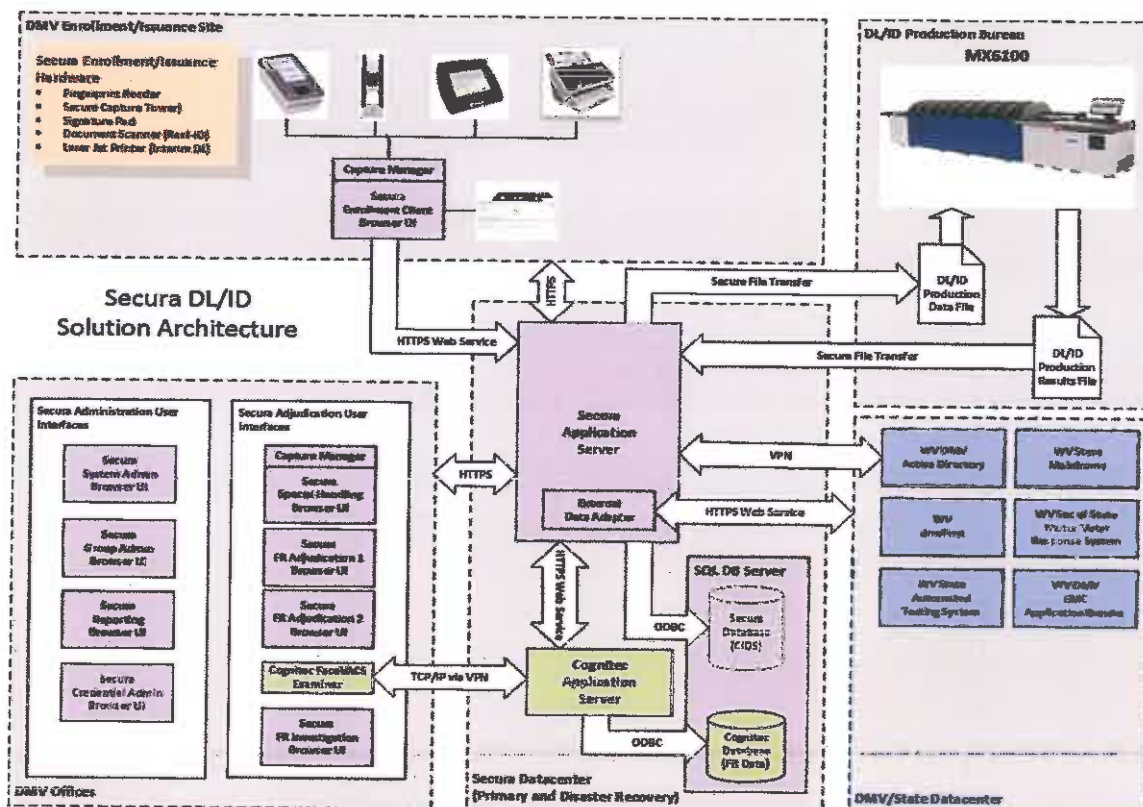


Section 4, Subsection 5.3.4 Must interface with the State's Automated Testing System, passing applicant demographic information.

#### Vendor Response:

Our proposed solution complies.

Our proposed solution includes a component called Data Adapters. Data Adapters are the mechanisms used to exchange data with other systems and interfaces. Data Adapters support most commonly used data exchange technologies such as but not limited to web services, XML, SOAP, XML, Rest, and can also incorporate proprietary methodologies if necessary. These Data Adapters will be used to support these interfaces as shown in the diagram below.

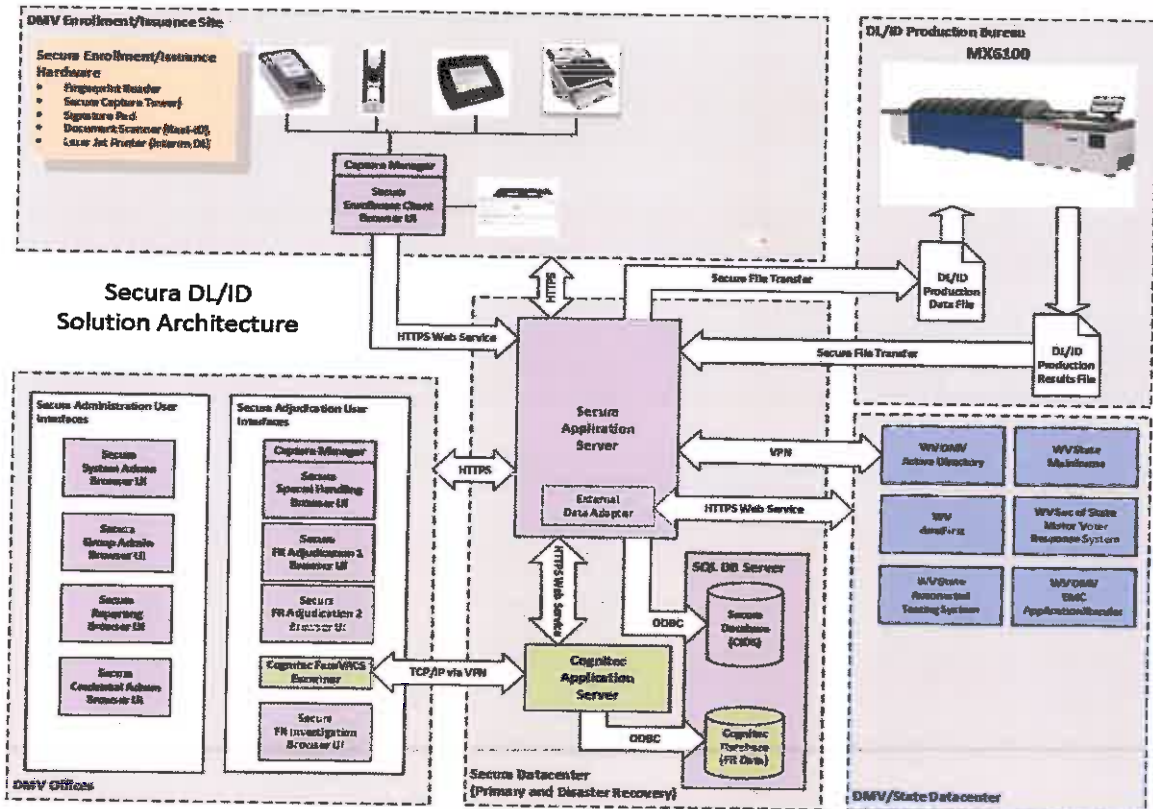


**Section 4, Subsection 5.3.5 - Must interface with West Virginia Interactive passing applicant demographic information related to multiple online solutions such as DL renewals, and employee 11) applications.**

**Vendor Response:**

**Our proposed solution complies.**

Our proposed solution includes a component called Data Adapters. Data Adapters are the mechanisms used to exchange data with other systems and interfaces. Data Adapters support most commonly used data exchange technologies such as but not limited to web services, XML, SOAP, XML, Rest, and can also incorporate proprietary methodologies if necessary. These Data Adapters will be used to support these interfaces as shown in the diagram below.



#### Section 4, Subsection 5.4. - Functional - Communication with Central Image/Demographic System

Section 4, Subsection 5.4.1 - The ICW must be capable of near real-time transfer (not just nightly batch) of demographic data and images to the central image/demographic system.

#### Vendor Response:

Our proposed solution complies.

The proposed system will update the Image repository in near real time, sending data as it is captured and received at the workstations or as communication allows in case of an outage.

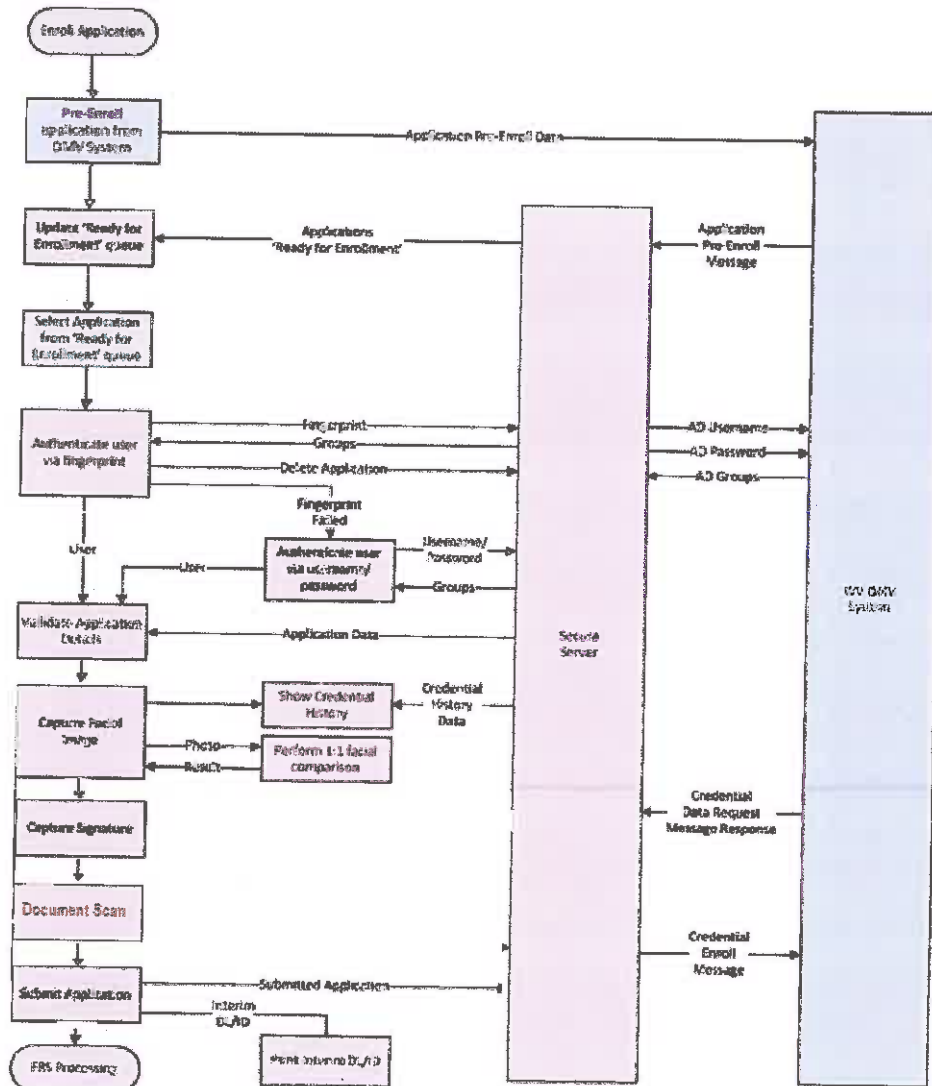
Section 4, Subsection 5.4.2 - All images and data captured must be transferred to the central image/demographic system for storage even if the transaction was cancelled or not completed.

5.4.2.1 If the applicant had to cancel or was not able to complete the transaction, Vendor's solution must provide for a verification match of the applicant's image and data against the central image/demographic system upon the applicant's return to any Agency Office for completion of the licensing process.

**Vendor Response:**

Our proposed solution complies.

The proposed solution will always run a 1:1 check on the newly capture image compared to the last image on file for the applicant. This will be done for all enrollments including transactions that were incomplete and the applicant returns to complete it at a later time. All applicants will be processed through the following process that can be tailored to WV DMV's specific needs if required.



**Section 4, Subsection 5.43 - Images and data for incomplete transactions must be distinguishable from completed issuance records.**

**Vendor Response:**

Our proposed solution complies.

Images stored in the records are flagged if they originate from an incomplete transaction. Incomplete transaction images will be easily distinguishable from images from properly completed transactions.

**Section 4, Subsection 5.5 - Security - Remote Access**

**Section 4, Subsection 5.5.1 - Secure, remote access to Vendor staff for purposes of support will be allowed via the West Virginia Office of Technology Network Access Form (NAF) request process at no cost to the Vendor.**

**[https://technologv.wv.gov/SiteCollectionDocuments/Policies%20Isued%20by%20the%20OCT0/2017/P01021 AccountManage Sept2017.pdf](https://technologv.wv.gov/SiteCollectionDocuments/Policies%20Isued%20by%20the%20OCT0/2017/P01021%20AccountManage%20Sept2017.pdf)**

**Vendor Response:**

Our proposed solution complies. Veridos acknowledges that remote access will be available for the purposes of support following the abovementioned process.

**SYSTEM ADMINISTRATION REQUIREMENTS Section 4, Subsection 5.6. - User Interface**

**Section 4, Subsection 5.6.1 - The solution must include a system administration module with a user interface for managing system settings.**

**Vendor Response:**

Our proposed solution complies.

The proposed solution provides a configuration screen that system administrators with the correct privileges can use to set the thresholds for 1:1, 1:N, search limits, and adjust other settings with as required.

The System Administration module also provides the ability to view and assign the Windows Groups that have been configured for use by the WVDMMV's environment.

System Administration also allows for the managing of workstations, The system has a Workstations list that shows the field office workstations which are connected and registered as Secura workstations. Optionally, a period of time where the workstations are unable to be used can be setup. This is an added layer of security to the application that prevents an authorized employee from attempting to process enrollment requests

outside of normal working hours. The operational schedules can be set globally or per workstation.

There is also the Problem Applications queue which displays a list of credentials which have encountered a problem while being processed by the Secura FRS workflow steps. These problems require resolution of the underlying cause and manual intervention to 'restart' the credential application processing. The Secura FRS system supports configuration of automatic email notification of problem applications in the Secura system

The Scheduled Action Setup screen supports configuring the time schedules for the schedule actions which are defined in the FRS workflows. The currently 'Defined Scheduled Actions' are Enroll Photo and Execute FRS Checks. The options available for each of these is to process the requests as they come in throughout the day (Run all Day), only during a specific window of time during the day, or run overnight during a specific span of time.

The System Administration module also allows the searching and viewing the user audit log data, setting up of notifications for specific events such as an email list to notify individuals when a credential is placed in a Secura specific workflow queue.

---

#### Section 4, Subsection 5.7 - User Account Management

Section 4, Subsection 5.7.1 - Vendor's solution must be compatible with Windows Active Directory protocol to utilize the agencies logon credentials, managed by the Office of Technology, to manage user roles.

#### Vendor Response:

Our proposed solution complies.

The proposed solution leverages the user accounts held within the State's Active Directory environment. User accounts are authenticated by the State's AD environment and then rights are assigned within the proposed application.

The proposed solution uses permission-based access control (PBAC) as part of the system security architecture. PBAC is a method to control which users have access to system resources based on the roles assigned to them. This security feature protects stored data from unauthorized viewing and modifications. PBAC security is transparent to users. This means that after users identities are verified, they are only allowed to view data and execute authorized operations based on their defined roles and permissions. The PBAC method protects data and system security by making sure that users cannot misuse their access rights and privileges.

User accounts with the System Administrator privilege are used to manage other user account permissions. A system Administrator uses the Users and Roles tab of the web client to configure authorized users and define how they access the system. The Roles tab lets you manage permissions assigned to Secura roles.

## Users

Users reside inside the enterprise LDAP and are created within the system. To ensure system integrity, each user is identified based on a User ID/ Password authentication mechanism. A system administrator assigns each user to one or more roles (with all of the corresponding permissions). The roles as-signed to each user determine what activities they are allowed to perform and what information they can access.

## Permissions

Permissions enforce the actions and activities that users are allowed to perform within their assigned roles. A system administrator associates each role with specific permissions for specific tasks; therefore, the roles assigned to each user determine which permissions (authorized actions) they are granted.

---

### Section 4, Subsection 5.8 - System Configuration

Section 4, Subsection 5.8.1 - At a minimum, the Agency must be able to configure the following settings:

5.8.1.1 Thresholds for 1: N and 1:1 match or non-match results

5.8.1.2 Search limit thresholds for all applications

#### Vendor Response:

Our proposed solution complies.

The proposed solution provides a configuration screen that System Administrators with the correct privileges can use to set the thresholds for 1:1, 1:N, search limits, and adjust other settings, including the search limit thresholds, as required.

---

### CENTRAL IMAGE/DEMOGRAPHIC SYSTEM ("CMS") REQUIREMENTS Section 4, Subsection 5.9 - Hardware and Software

Section 4, Subsection 5.9.1 - All software necessary for communication between the central image/demographic system and other Vendor or Agency systems, must be provided by the Vendor.

#### Vendor Response:

Our proposed solution complies.

All software provided is industry best practices, open architecture using TCP/IP, HTTP or HTTPS and other protocols including but not limited to SOAP or REST services, Public Key Infrastructure (PKI), Virtual Private Networks (VPN) and other encryption for protecting data while in movement or at rest. The proposed solution provides a web service interface that other Vendor or other agencies can use to retrieve data from the system as required.

---

**Section 4, Subsection 5.9.2 - All virtual servers necessary for the central image/demographic system shall be provided by and located in the West Virginia Office of Technology data center in Charleston, West Virginia.**

**Vendor Response:**

Our proposed solution complies.

Our proposed solution fully supports use of provided Virtual Servers. Server specifications as to Type of Virtual Machine, Operating Systems, RDBMS and specifications will be coordinated with West Virginia Office of Technology.

---

**Section 4, Subsection 5.9.3 - All data stores necessary for the central image/demographic system shall be provided by the Agency and located in the West Virginia Office of Technology data center in Charleston, West Virginia**

**Vendor Response:**

Our proposed solution complies.

Our proposed solution fully supports storage of all data by the West Virginia Office of Technology Data Center.

---

**Section 4, Subsection 5.10 - Data Storage**

**Section 4, Subsection 5.10.1 - Vendor's solution must meet all policy requirements regarding the collection, storage, usage, classification, transmission, backup, and retention of data as defined by the Office of Technology Policy number P01001, P01006, and P01013.**

**<http://www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx>**

**Vendor Response:**

Our proposed solution complies.

The solution supports the use of best practices industry standard protocols and systems for protection of data. These include HTTPS and the underlying certificates and technology related to Public Key Encryption, Virtual Private Networks (VPN) and other encryption for protecting data both in movement and at rest. Backup of the various servers and databases is fully supported and would be coordinated with the West Virginia Office of Technology.

Section 4, Subsection 5.10.2 - The central image/demographic system must store the facial image files, signature image files, demographic data, and card issuance data for every transaction through the life of the contract. This must include specific card data that will be returned from the central issuance facility.

**Vendor Response:**

Our proposed solution complies.

The proposed solution will store all the required data as defined by the WVDMV.

Section 4, Subsection 5.10.3 - Facial image and signature files must be stored in JPEG 2000 for image compression, or standard that is an open (consensus) format, without proprietary wrappers, to ensure States can effectively use the image captures of other States as necessary.

<https://www.gpo.gov/fdsys/uku/FR-2008-01-29/htnal/08-140.htin>

**Vendor Response:**

Our proposed solution complies.

The image capture solution provides the flexibility to store images in a number of formats, including JPG2000 format, the solution will store the images in a format agreed upon during the design phase of the project which meets the listed specifications, is not a proprietary format, and is compliant with ICAO standards (ISO/IEC FCD 19794-5).

Section 4, subsection 5.10.4- The system must log and store audit data for all types of system and data access including details of specific tasks performed and records accessed.

**Vendor Response:**

Our proposed solution complies.

The Secura platform supports the provision of detailed transaction audit files. The enrollment transaction becomes a subset of the complete enrollment and issuance audit/log.

Secura retains the user audit log for all types of system and data access.

Standard system summary reports can include (but are not limited to):

- Enrollment Summary - Service Center
- Enrollment Summary - Date Range



- Enrollment Summary - Monthly
- Enrollment Summary - Quarterly
- Enrollment Summary - Yearly
- Investigation Summary - Date Range
- Investigation Summary - Monthly
- Investigation Summary - Quarterly
- Investigation Summary - Yearly
- N Lead Summary - Date Range
- N Lead Summary - Monthly
- N Lead Summary - Quarterly
- N Lead Summary - Yearly
- R Lead Summary - Date Range
- R Lead Summary - Monthly
- R Lead Summary - Quarterly
- R Lead Summary - Yearly
- Special Handling Summary

Credential and user audit event activities are logged. Standard system audit reports can include (but not limited to):

- Audit Report - Credential
- Audit Report - Customer
- Audit Report - User

---

#### Section 4, Subsection 5.11 - Ownership of Data

Section 4, Subsection 5.11.1 - Vendor must sign and agree to Attachment F - WV Division of Motor Vehicles Contract Privacy Policy.

##### Vendor Response:

Our proposed solution complies. Veridos has signed and agrees to Attachment F - WV Division of Motor Vehicles Contract Privacy Policy.

---

Section 4, Subsection 5.11.2 - Vendor must sign and agree to Attachment H - PII Acknowledgement.

##### Vendor Response:

Our proposed solution complies. Veridos has signed and agrees to Attachment H - PII Acknowledgement.

---

#### Section 4, Subsection 5.12. - Access to Data

Section 4, Subsection 5.12.1 - Access to the central image/demographic system will be restricted to individuals whose duties require such access and are authorized by the Agency.

##### Vendor Response:

Our proposed solution complies.

The proposed solution will use current security measures including but not limited to database encryption, AES256, and login roles and groups to ensure that the images and data are only accessible to those who are authorized to view it by the Agency.

The proposed solution leverages the user accounts held within the State's Active Directory environment. User accounts are authenticated by the State's AD environment and then rights are assigned within the proposed application.

The proposed solution uses permission-based access control (PBAC) as part of the system security architecture. PBAC is a method to control which users have access to system resources based on the roles assigned to them. This security feature protects stored data from unauthorized viewing and modifications. PBAC security is transparent to users. This means that after users' identities are verified, they are only allowed to view data and execute authorized operations based on their defined roles and permissions. The PBAC method protects data and system security by making sure that users cannot misuse their access rights and privileges.

User accounts with the System Administrator privilege are used to manage other user account permissions. A system Administrator uses the Users and Roles tab of the web client to configure authorized users and define how they access the system. The Roles tab lets you manage permissions assigned to Secura roles.

### Users

Users reside inside the enterprise LDAP and are created within the system. To ensure system integrity, each user is identified based on a User ID/ Password authentication mechanism. A system administrator assigns each user to one or more roles (with all of the corresponding permissions). The roles assigned to each user determine what activities they are allowed to perform and what information they can access.

### Permissions

Permissions enforce the actions and activities that users are allowed to perform within their assigned roles. A system administrator associates each role with specific permissions for specific tasks; therefore, the roles assigned to each user determine which permissions (authorized actions) they are granted.

---

Section 4, Subsection 5.12.2 - Secure, remote access for Vendor staff for purposes of support will be allowed via the West Virginia Office of Technology Network Access Form (NAP) request process at no cost to the Vendor.

### Vendor Response:

Our proposed solution complies. Veridos understands and agrees to this requirement and will secure remote support access per the West Virginia Office of Technology NAP request process.

---

### Section 4, Subsection 5.13 - System Performance

Section 4, Subsection 5.13.1 - The total time required from the time the image file transmit request is received by the central image/demographic system until the image file is being transmitted from the central image/demographic system shall not exceed one (1) second during the life of the contract. Total time for retrieval excludes the transmission time across any communications network.

### Vendor Response:

Our proposed solution complies.

Our proposed system is designed for high volume and speed of issuance and will be scaled appropriately to meet the WVDMMV's requirements.

---

**Section 4, Subsection 5.14 - Software Optimization**

Section 4, Subsection 5.14.1 - The Vendor is responsible for any optimization to the software that is required to maintain these response times no matter how many retrieval requests are received.

**Vendor Response:**

Our proposed solution complies.

Our proposed solution will be optimized to meet the required response times regardless of the number of retrieval requests received.

---

**Section 4, Subsection 5.15 - Image Migration and Volume**

Section 4, Subsection 5.15.1 - Vendor's solution must provide for the migration of credential images and index information from the current Gemalto ID system to the new central image/demographic system (CIDS). Migration must result in a minimum of 98 percent usage of the current credential images. There are approximately 3 million JPG images that average 10kbs in size each.

**Vendor Response:**

Our proposed solution complies.

Before undertaking any migration project, a clear understanding of the environment to be migrated to and from is a necessity. Without a sufficient understanding of both source and target system, transferring data into a more sophisticated application will amplify the negative impact of any incorrect or irrelevant data, perpetuate any hidden legacy problems, and increase exposure to risk.

Veridos understands the importance of WVDMMV's business needing to run 24 hours a day, 7 days a week even during this migration phase. We have successfully migrated data in other large programs by adopting the incremental approach to migrating data. Rather than aim to complete the whole event at once requiring downtime, trickle migration involves running the old and new systems in parallel and migrating the data in phases. This results in no interruption to work and no system downtime.

Veridos has specially designed tools that allows us to successfully migrate the data into the new FRS systems in a well-defined process. The tool ensures that the images are successfully enrolled in the FRS, 1:N, and 1:R searches are done as required, and the results of those actions being a record enrolled and also placed into an appropriate queue as required.

The queues are either the special handling queue where images that were not successfully enrolled can have operator intervention such as re-cropping the image, manually annotating the eyes, or other corrective actions that are necessary for the specific failure. Records may also be automatically placed in the adjudication queues if there are hits on any of the, 1:N, or 1:R checks. Otherwise records that are successfully enrolled and had no hits will remain in the FRS battery to be used as probe images as required by the contact.

Migration of existing customer images into the facial comparison system will be conducted using the following steps.

### Data Migration Process

The data migration process involves repeating a set of batch import tasks over a period of several weeks. The optimal size of each batch import will be determined through empirical testing (initial estimate would be 300 to 500k records).

The tasks involved in accomplishing each batch import will include:

- 1) Export of the credential data from the source database:
  - a. The format of the exported data is a comma separated file (one line for each credential containing the above fields in the order shown) and the set of referenced photo files
  - b. Assign in the export database and export file an 'Issuance ID' for each credential record which will be used as a key reference between the FRS databases
  - c. Transfer from the source Datacenter to the WVDMV Datacenter
- 2) Creation of the FRS import files:
  - a. The Secura Import Manager utility will be used to read in the data file exported in the previous steps and create the FRS batch files
- 3) Execute the FRS batch import commands which will:
  - a. Read the records from the FRS batch import file
  - b. At a scheduled interval, the FRS workflow engine will process new entries
  - c. Create and store in the FRS database facial comparison templates for each photo referenced in the imported records
- 4) Manually enroll failed records:
  - a. For those records that failed to enroll during the FRS batch enrollment process, use the Database Enrollment application to manually specify the eye locations to be used in creating the facial comparison template
- 5) Validate the result of the batch import:
  - a. Use supplied database queries to reconcile the number of records in the source import file to the number of records imported to FRS
  - b. Send the validate report via email to jurisdiction



- c. Once the batch import results have been validated, the import data files will be deleted

Note: Steps 2-5 above will generate log files which will be monitored for errors. Any errors that occur will be addressed and the import resumed.

### **Data Migration Plan**

The following sections outline the data migration activities and milestones for each FRS deployment.

#### **Development 1**

- No data migration activities are required for the Development 1 deployment

#### **System Integration Testing (SIT)**

- The import of 500,000 to 1 million records will be required to:
  - Support integration and testing of the FRS functionality
  - Determine the optimal export package size
  - Estimate the time to import an export package
- **Milestone:** Establish the Export Package size and expected time to import

#### **User Acceptance Testing (UAT)**

- The import of at least 2 to 3 million records will be required to:
  - Support user acceptance testing of the FRS functionality
  - Determine the time to import an export package to support production migration scheduling
  - Determine the data required to be included in the Import Validation Report
- **Milestone:** Create the Production Migration schedule based on the export package size and time to import
- **Milestone:** Define the contents of the Import Validation Report

#### **Production Records prior to installation**

- The import of all existing customer records per the Production Migration schedule
- **Milestone:** All customer records migrated to the FRS

### **Data Migration During Transition**

The daily import and enrollment of records which have been processed through the existing system during the transition period between the new and the old FRS solutions. This process is used to ensure the new FRS has the maintains the entire dataset once the data migration process has started until the go live date and decommissioning of the existing solution occurs.

#### **Process:**

- A import file is extracted each evening from the existing system and imported into the new FRS each morning
- The import file records go through the same processing as if submitted from FRS Enrollment
- All leads from existing system's probes are adjudicated in the new FRS
- For fraud that is found in new FRS but not in old solution, a report is generated that is used to notify the bureau to suspend production on those specific records.

Given this plan and our FRS's ability to work successfully with low quality images, Veridos will be able to import the required images successfully into WVDMV's new system.

---

**SECURE CENTRAL ISSUANCE FACILITY REQUIREMENTS. Section 4,  
Subsection 5.16 - Credential Issuance**

Section 4, Subsection 5.16.1 - Vendor must meet the requirements of the REAL ID Act of 2005 (<http://www.dhs.gov/xlibrary/assets/real-id-act-text.pcii>), including any relevant security mandates, including those pertaining to personnel, with supporting documentation provided, as required.

**Vendor Response:**

Our proposed solution complies. Our central issuance facility and project personnel meet the requirements of the REAL ID Act of 2005. Veridos will provide supporting documentation as required.

---

**Section 4, Subsection 5.17 - Communication with the Agency's  
Data Center - Transfer of Data**

Section 4, Subsection 5.17.1 - The secure central issuance facility must communicate with the Office of Technology data center via a VPN tunnel, which hosts the Agency's mainframe, central image/demographic system, and dmVFIRST solutions.

**Vendor Response:**

Our proposed solution complies.

S-FTP transmission is used to ensure that client is communicated via encrypted channel (VPN) from the WVDMV Server to Veridos Server. Files transmitted via Secure Channel are encrypted using PGP (or any other file encryption method required). This ensures that the file is always secure to arrival upon the server. Veridos' systems are set to detect files arriving on the server and to immediately move it into Veridos' internal encrypted networks. Once the file is securely stored in the Veridos network, with all the logical and physical security described above, the file is decrypted using PGP shared pair keys, and balanced for integrity at Veridos.

---

**Section 4, Subsection 5.17.2 - The transfer of information must  
be over secure channels and all data in motion must be  
encrypted, for instance using SMB 3 security enhancements.****Vendor Response:**

Our proposed solution complies.

Ohio data transmission will be sent via a VPN tunnel and encrypted according to specific security requirements (i.e. PGP file level encryption complimented with the use of SFTP file transmission).

Upon transmission, WVDMV files will be pulled onto Veridos' secure internal network. Files are then logically subdivided. Order files are decrypted by Veridos' DPS (Data Processing System) and the required data uploaded to the identified environment (Production, Test etc.).

All secure and sensitive data is subjected to hashing (SHA-256) and encryption (AES-256). Once data is transmitted to Veridos all data is stored in secure areas only and classified as "Veridos Strictly Company Confidential. Veridos' security standards and procedures comply with ISO 27001 , PCI Card Production Physical and Logical Security Requirements and Visa, Mastercard, AMEX and Discover security regulations.

Please also refer to our response to Section 5.17.1.

---

#### Section 4, Subsection 5.18 - Card Production Data Files

Section 4, Subsection 5.18.1 - The Agency will send the standard card production data file once daily. Vendor Response:

Our proposed solution complies.

Veridos' Data Processing System (DPS) is capable of receiving and processing West Virginia's files daily, as well as receiving expedited files separately, or as a single transmission. The special handling requests are indicated by the submitting party through selection of 'Priority' DL/ID, triggering expedited card production.

---

Section 4, Subsection 5.18.2 - The Vendors solution must be capable of receiving a card production data file seven (7) days a week.

Vendor Response:

Our proposed solution complies.

Our DPS will receive and acknowledge card production files seven days a week.

---

#### Section 4, Subsection 5.19 - Management of Central Issuance Facilities

Section 4, Subsection 5.19.1 - The Vendor shall be responsible for the complete management of the central issuance facility.

Vendor Response:

Our proposed solution complies.

Veridos' high-security facility in Twinsburg, Ohio is owned by Veridos' parent firm Giesecke & Devrient. Veridos and G+D are the only tenants. Our facility is staffed and will be operated by our personnel. At no time will staffing be contracted to any outside parties.

---

**Section 4, Subsection 5.19.2 - All hardware and software necessary for the operation of the secure central issuance facilities will be the responsibility of the Vendor.**

**Vendor Response:**

Our proposed solution complies.

Our high-security central issuance facility in Twinsburg, Ohio has 170 employees and a current capacity of approximately 144 million cards / annually (and has produced that number in the past). We use high-quality Datacard MX6100 Card Personalization Systems to personalize and mail the cards and currently have more than enough capacity to manage WVDMV's card production.

---

**Section 4, Subsection 5.19.3 - All staffing and operational needs will be the responsibility of the Vendor. Vendor Response:**

Our proposed solution complies.

Our high-security central issuance facility in Twinsburg, Ohio has 170 employees and a current capacity of approximately 144 million cards / annually (and has produced that number in the past). We use high-quality Datacard MX6100 Card Personalization Systems to personalize and mail the cards and currently have more than enough capacity to manage WVDMV's card production.

---

**Section 4, Subsection 5.19.4 - Security of the central issuance facilities will be the responsibility of the Vendor and must meet the security requirements of the REAL ID Act and any Department of Homeland Security published implementation rules.**

**Vendor Response:**

Our proposed solution complies.

Our high-security, Real ID-compliant card production facility in Twinsburg complies with the very strict PCI Card Production, Physical and Logical Security Requirements and is audited annually. Twinsburg is also certified by Visa, Mastercard and Discover. It is to the benefit of WVDMV that this high-volume site offers one of the most diverse product lines in the industry as Twinsburg must maintain certification for all of our business units, from financial through to government solutions.

**Physical Security of Veridos Facilities**

Our site access standard governs who is authorized to access the site and how. Our standard provides guidelines for resident employees, visiting employees from other sites, as well as contractors/suppliers and other visitors. Everyone who enters a Veridos production facility must be in possession of a Veridos or G+D issued identification electronic chip card. All visitors are signed in by the hosting employee and escorted in

the site at all times. All visitors are required to sign a site access confidentiality agreement prior to entering Veridos production facilities. Escalating authorities are required and prompted automatically as the level of access increases. Our access request database allows for access to restricted and/or critical areas via direct authorization by the area owners only.

Our security concept encompasses issues pertaining to physical security of our production, personalization and distribution facilities and buildings, production processes, data processing, personnel and all aspects of order processing and production.

In the area of external security (security on company premises and in company buildings), it shall be ensured that:

- Personnel access our sites at controlled access points utilizing an electronic chip card, single-entry full-height turnstile doors or man-trap. All entrances and exits to and from company premises and to the production, storage and office by employees are only possible upon unprompted production of the company chip ID card, or by the access control system and personnel locks.
- All visitors and non-company workers may enter the premises only following written registration and submission of an identification document and visitor form and escorted by a company staff member. Entry and exit times are recorded in the control documents and the last contact person visited confirms the exit time by his/her signature at the end of the visit.
- Facility is provided for immediate alarming of the police by a modern computer-based alarm system or from numerous emergency call stations positioned on company premises.

Movement of product and inventory/supplies is via shipping/receiving points only with our receipt and dispatch being a designated restricted area. Raw materials used in card manufacture, including printing plates, raw plastic sheets, laminating plates, elemental security features, etc. are considered secure materials and are subject to secure shipping and inventory control measures through the entire production process, including shipping of final card products, destruction of scrap material and returns of defective raw materials to the supplier. Internal inventory control procedures include dual control or the "four eyes principle" and secure storage as detailed in the card security section.

While on premises, all card bodies are subject to secure storage as well as a rigorous tracking and inventory management program that ensures materials, card bodies and other components are safe from theft and kept separate from non-Ohio card bodies. A docket is generated for each different card type every time a file is received from Ohio. The only way that cards and collateral can be obtained and released from both the vault and warehouse is with the authorized docket which clearly states the material numbers required to fulfill the file.

Package searches may be conducted on any material or persons leaving the facility. Random searches of persons and their belongings are executed when anyone be it



visitors, contractors, vendors and employees leave the production facilities. The employee exit doors of the building are manned 24x7 by security guard personnel.

Digital video recording is in use at our sites 7 days a week 24 hours a day 365 days per year. Video cameras record and archive activity throughout both corporate and production facilities, including, but not limited to the exterior site perimeter and at access points. Images are retained for a minimum 90 days on the digital video recorder itself. Signs are affixed throughout the site announcing the presence of video through all areas of all facilities. Security breaches are immediately reported to site management and then to corporate security.

Any unusual activity is investigated. Access cards are retrieved from terminated employees before they leave the premises.

#### **Guard Duties**

There are two posts which the guards occupy when onsite, the employee entrance/exit and the Security Control Room. Access to the security control room is restricted to authorized personnel only.

Guards do not have access to any office or production areas within the facility. They also do not have access to any of the following: personnel records, master accountability audit logs, card access system server, cardholder information, card products or stock and card stock or cardholder information waste. Detailed Post Orders for the guards have been developed and duties include:

- Monitoring of the Closed Circuit Television (CCTV) systems
- Access control procedures including visitor registration and system monitoring
- CCTV procedures such as system use and daily image comparison checklists
- Monitoring the burglar alarm system
- Reporting procedure and escalation calls
- Reporting daily shift reports and incident reports
- Conducting random searches
- Response preparedness for emergencies, evacuations (fire, bomb threats, civil disturbances, ransom demands, hostages and kidnapping)

#### **External Construction**

External constructions such as the electrical room, generator, ventilation and HVAC system ducts and roof hatches that lead into the facility have been designed so that the facility is protected against unauthorized access. Metal security bars have been installed in the ventilation and HVAC ducts leading from the outside. The roof hatch, electrical room and generator all have alarm contacts installed that are monitored by the on duty guard.

#### **Exterior Entrances and Exits**

All exterior doors, excluding emergency exit doors are connected to the access control system and are contact monitored and also have the appropriate interlocking or

mantrap configuration. Exterior doors are also monitored by Closed Circuit Television (CCTV) surveillance and are also equipped without automatic closing devices.

**External Walls, Doors and Windows**

Motion sensors, glass break sensors and door contacts have been strategically located throughout the building and are monitored by the on duty guard and monitoring station.

**Emergency Exits**

Emergency exit doors are permitted to be used in the event of an emergency or during a fire drill.

There are signs on each emergency exit door indicating that the door is an emergency exit and that an alarm will sound if the door is opened. Emergency exits are fitted with local audible alarms and are armed and monitored 24x7x365. The alarm is activated locally and is received by the guard that is on duty.

Emergency exit doors are tested every other month and the results are maintained for 24 months.

**Exterior Lighting**

Adequate lighting has been installed around the perimeter of the building. Exterior lights are checked monthly and the logs are maintained for a minimum of 24 months

**Roof Access**

Roof hatches that access our building are alarm contact monitored and locked down at all times. Ventilation and HVAC system ducts that penetrate the building are protected with metal security bars.

**Exterior CCTV**

Closed Circuit Television (CCTV) cameras are installed and focused on all exterior doors of the building. All of these images are monitored within the Security Control Room.

**Signage**

There are no signs on the exterior of the building that indicate or imply that cards are made or personalized at this facility.

**Reception - Internal Structure and Processes**

Access is permitted through electronically controlled doors. The front door leads into a secure vestibule area and the vestibule leads into a visitor waiting area where it is interlocked with the door in the vestibule area. Walls of entire lobby area are floor to deck concrete block re-enforced. A two-way intercom system is used to communicate with visitors through bullet resistant proof glass. There is a duress button, glass break sensors and motion sensors in the reception area that are monitored by security guards 7 days a week 24 hours a day 365 days per year.

**Employee Entrance**

The Employee Entrance is the access point that must be used by all employees to enter and exit the building. Staff must use their access cards to enter and exit the building through a person by person turnstile door with anti-passback in effect. There are also door held open and forced open alarms have been implemented on man doors with a duress button installed and the area under Closed Circuit Television (CCTV) surveillance.

Due to the sensitive nature of our business, Veridos has the right to randomly search all employees' and visitors' possessions and will ensure that it is performed in a fair and reasonable manner. These searches must be conducted without preference or discrimination with random searches. These random searches do not indicate a suspicion of theft; rather searches are a routine part of business that serves to deter any potential theft. Searches are performed upon exit of the facility at the Employee Entrance and all results of the search are logged.

---

**Section 4, Subsection 5.20 - Standard Processing Time.**

**Section 4, Subsection 5.20.1 - Cards must be mailed via US Postal Service, from the production facility no later than two (2) regular business days following the printing of the credential.**

**Vendor Response:**

Our proposed solution complies.

This SLA is in accordance with our normal business practice.

All DL / ID cards for the State of West Virginia will be manufactured, personalized and shipped from our Twinsburg location. This means that there is **no need to transport card bodies or secure production materials** to put them at risk for loss or theft.

---

**Section 4, Subsection 5.20.2 - Vendor must have monitoring in place to ensure card production is completed within two business days after the appropriate fraud hold period.**

**Vendor Response:**

Our proposed solution complies.

This SLA is in accordance with our normal business practice. Our systems automatically monitor files and records that are placed on hold and ensure that they processed when holds are released.



customer initiated problem. Any WVDMV correspondence which raises a service and/or quality issue is also logged via the incident reporting system.

---

**Section 4, Subsection 5.22 - Card Mailing**

**Section 4, Subsection 5.22.1 - The Vendor shall be responsible for all USPS fees associated with postage and shipping.**

**Vendor Response:**

Our proposed solution complies.

---

**Section 4, Subsection 5.22.2 - The Vendor shall mail all 'FOR FEDERAL' credentials using USPS paid online 'Signature Confirmation'**

**Vendor Response:**

Our proposed solution complies.

---

**Section 4, Subsection 5.22.3 - All NOT FOR FEDERAL' credentials shall be mailed via USPS, using a return address specified by the Agency, unless the two-day production time is exceeded as defined in para.5.20.3.**

**Vendor Response:**

Our proposed solution complies.

---

**Section 4, Subsection 5.22.4 - All envelopes shall be marked with "Return Receipt Requested" to prevent forwarding.**

**Vendor Response:**

Our proposed solution complies.

---

**Section 4, Subsection 5.22.5 - If a third-party Vendor is to be used for mail sorting, their processing time must be included in the maximum two (2) business days and the Vendor must be disclosed as a subcontractor.**

**Vendor Response:**

Our proposed solution complies.

We use Midwest Direct located in Cleveland, Ohio for mail sorting services.



---

#### Section 4, Subsection 5.23 - Card Volume

Section 4, Subsection 5.23.1 - The central issuance system must be capable of meeting yearly production needs of approximately 500,000 cards.

**Vendor Response:**

Our proposed solution complies.

Our high-security central issuance facility in Twinsburg, Ohio has 170 employees and a current capacity of approximately 144 million cards / annually (and has produced that number in the past). We use high-quality Datacard MX6100 Card Personalization Systems to personalize and mail the cards and currently have more than enough capacity to manage WVDMV's card production.

---

Section 4, Subsection 5.23.2 - Sufficient capacity must be provided to accommodate system outages including repairs and preventative maintenance.

**Vendor Response:**

Our proposed solution complies.

Our card production facility has several MX6100 Card Personalization Systems that provide sufficient capacity to accommodate system outages for repairs and preventative maintenance.

---

#### Section 4, Subsection 5.24 - Billing

Section 4, Subsection 5.24.1 - All cards printed and mailed from the central issuance facilities will be billed only after successful processing and transfer to the USPS.

**Vendor Response:**

Our proposed solution complies.

Our production facility generates monthly production reports indicating the number of cards successfully printed and mailed. This report will be used to generate monthly invoices for WVDMV.

Section 4, Subsection 5.24.2 - Sufficient detail must be provided to allow the Agency to reconcile card counts between the invoice, the credential issuance system, and internal Agency systems.

**Vendor Response:**

Our proposed solution complies.

Our monthly invoice to WVDMV will include the detailed report that reflects successful cards printed and mailed. This report can be used by WVDMV to reconcile with the internal systems.

Section 4, Subsection 5.24.3 - The Agency will only be responsible for paying the cost per card for cards issued to an applicant. The Agency will not pay for cards rejected due to material or printing process defects, or for cards used for system testing.

**Vendor Response:**

Our proposed solution complies.

Veridos will only invoice WVDMV for cards that are successfully issued to an applicant.

**CARD DESIGN AND SECURITY FEATURES REQUIREMENTS**

Section 4, Subsection 5.25 - Data on Secure Temporary Driver's License and ID's

Section 4, Subsection 5.25.1 - The secure temporary DL or ID will include the same data that will be printed on the permanent, standard term card, including facial image and signature.

**Vendor Response:**

Our proposed solution complies.

The temporary DLID will include the same data as the permanent credential including the facial and signature images. The exact layout of the temporary DLID will be determined during the planning stages of the project collaboratively with Veridos and the WVDMV.

**Section 4, Subsection 5.25 .2- Must include correct expiration date of temporary credential. Vendor Response:**

Our proposed solution complies.

The temporary DL/ID will include the correct expiration date that will be automatically calculated by the enrollment solution. The exact layout of the temporary DL/ID will be determined during the planning stages of the project.

**Section 4, Subsection 5.25.3 - Must state on face that it is a temporary credential. Vendor Response:**

Our proposed solution complies.

The temporary credential will state that it is the temporary credential. The exact layout of the temporary DL/ID will be determined during the planning stages of the project.

**Section 4, Subsection 5.25.4- Must include statement, "Valid for operation of motor vehicle only". Vendor Response:**

Our proposed solution complies.

The temporary credential will state "Valid for operation of motor vehicle only". The exact layout of the temporary DL/ID will be determined during the planning stages of the project.

**Section 4, Subsection 5.25.5 - Must have a fraud-warning marker on the temporary credential, for any application that is marked for potential fraud, i.e. not meeting the facial 1:1 match.**

**Vendor Response:**

Our proposed solution complies.

The temporary credential will have a marking(s) to show if any automated checks were not completed successfully. For example, if the 1:1 check does not meeting the preset threshold, the system would automatically print a specific marking on the temporary DL/ID. The exact layout of the temporary DL/ID will be determined during the planning stages of the project.

---

**Section 4, Subsection 5.26 - Card Types**

Section 4, Subsection 5.26.1 - Vendor's solution must produce the card types defined in Attachment G – Current Card Types, as issued by the Agency.

**Vendor Response:**

Our proposed solution complies.

---

**Section 4, Subsection 5.27 - Card Design.**

Section 4, Subsection 5.27.1 - Card design shall be based on 2016 AAMVA DL/ID Card Design Standard (<http://www.aamva.org/2016CardDesignStandard/>).

**Vendor Response:**

Our proposed solution complies.

Veridos has prepared a total Real ID-compliant solution for WVDMV. The total solution package being offered to West Virginia is designed to prevent tampering and counterfeiting. Our cards feature advanced security and production measures designed to assist law enforcement use the cards during field operations while simultaneously providing attractive, long lasting cards to the citizens of West Virginia.

The proposed Driver's License is constructed of Polyester Enhanced Polycarbonate (PEC) that has been extensively tested and qualified by Veridos and third party laboratories. The card body is constructed of multiple layers, which include transparent and opaque materials which are a Veridos trade-secret and are not commercially available. Once assembled, the materials are laminated together under specific heat and pressure (without any adhesive or thermoplastics) to form a consistent card body which **cannot be delayered** as is possible using other substrates.

**Card Overview**

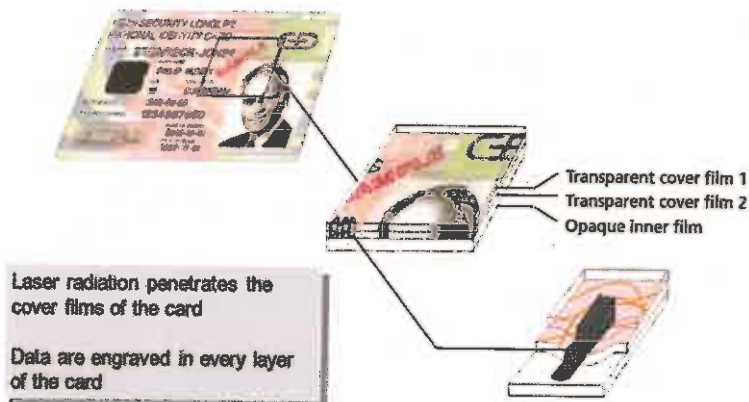
<b>Material:</b>	Polyester Enhanced Polycarbonate (PEC)
<b>Service Life:</b>	8 years of usage
<b>Dimensions:</b>	85.60 mm x 53.98 mm x 0.76 mm (nominal)
<b>ISO/IEC Spec:</b>	7810:2003 (Card Body)
<b>Color Photo:</b>	Thermal dye diffusion printing
<b>Data Elements:</b>	Laser Engraving

**Benefits of Polyester Enhanced Polycarbonate (PEC)**

- Durable PEC card body
- Color photo using thermal dye diffusion printing (D2T2)
- Laser engraving for secure data application
- Offers superior value at cost effective price
- Offers outstanding durability
- Similar technology to what is used in passports and National ID card programs
- Environmentally friendly material
- Protection against photo substitution
- Protection against counterfeits including types A1, A2, B1, and B2




Laser engraving means that all textual data is engraved 'into' the card body, where it cannot be altered. Laser engraving produces visual effects or images on cards that are permanent and highly secure. Multi-layer cards are laser engraved by passing a laser beam through the top clear layer of a card and focusing on a transparent laser receptive layer. It is here where the pigments react and form a black image as the layers react with each other. This process is often referred to as carbonizing. Additional energy is created with additional engraving time to create darker images and with sufficient energy; a tactile or raised image.



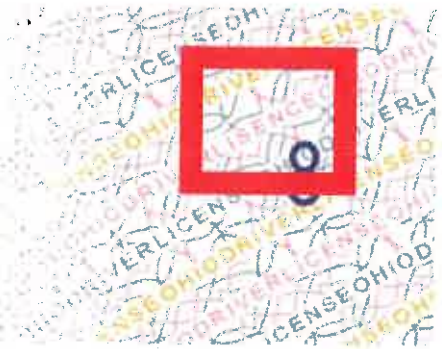
Cards will be laser engraved on both sides using an internal turning device, and multiple lasers can be used in sequence to laser engrave several cards at once to increase card throughput. Laser image quality is controlled by the internal software of the Datacard MX6100 card issuance systems. Card setups can control the type of laser engraving, the resolution (which can exceed 500 dpi), and the length of time the laser beam engraves a given area or pixel. Highly sensitive and accurate optical sensors control registration. Precise optics and mirrors ensure the accurate placement of laser engraved images.









All cards will be personalized, affixed to carrier and mailed using Datacard MX6100 card personalization and mailing equipment. The MX6100 will laser engrave all personal data. The MX6100 is modular in design and can easily be expanded to accommodate technological advances in card production.



### Proposed Security Features




Microprinting / Nanoprinting	<p><b>Security Feature: Level 2</b></p> <p>Miniature lettering which is discernible under magnification. Incorporated into fine line backgrounds or placed to appear as bold lines. Continues to decrease in size as technology improves. Cannot be scanned or reproduced on commercially available printers.</p> <p>Microprint lettering has been embedded in numerous areas of our proposed card design for added security.</p>	 
Redundant Data	<p><b>Security Feature: Level 1,2</b></p> <p>The application of redundant data provides another obstacle in attempts to alter or compromise a card. The date of birth for example can be applied in multiple locations, one using tactile format. Changing either of these elements is impossible without damage to the card structure. These cards can also provide redundant data in the form of a ghost image applied to the front and back of the card, and a secondary signature to the front.</p>	
Rainbow Printing	<p><b>Security Feature: Level 1</b></p> <p>A printed feature demonstrating a controlled, subtle color shift in a linear, continuous fashion.</p> <p>In the second example, notice how</p>	

	the Microprinting shifts in color in parallel with the rear graphic.	
Color Shifting Inks	<p><b>Security Feature: Level 1 (Optional)</b></p> <p>Special security inks containing microscopic pieces of metallic substances and arranged in such a manner as to change color when tilted to view. Very common in currency, travel and identity documents.</p>	
Undisclosed Third Level	<p><b>Security Feature: Level 3</b></p> <p>The third level security feature has been applied within the card design. These elements are for forensic analysis only, and will be discussed upon request. All such forensic features are unique to each jurisdiction, and thus due to the strictly confidential nature of the feature it can only be discussed in confidential meetings.</p>	
Deliberate Error	<p><b>Security Feature: Level 2</b></p> <p>Veridos' experience has taught us that designing the card as a total solution provides us with flexibility to meet future security and legislative needs. Since our cards are made of overlapping security features, individual features can be added, removed or reconfigured based on advances in technology and changes in standards, all without leaving any gaps in the solution or causing undue extra cost.</p>	
Security Background	<p><b>Security Feature: Level 1,2</b></p> <p>The designs for these cards have been created specifically for WV.</p>	

	and incorporate a secure background consisting of a fine, structured guilloche pattern. These patterns change in color across the card area, creating a rainbow effect. These two features alone are virtually impossible to imitate. With the combination of all the blended security features, attempts to alter or change the document could be detected with minimal difficulty.	
Ultraviolet Text in Substrate	<p><b>Security Feature: Level 2</b></p> <p>This feature is incorporated within the design on both sides of the card and is only visible under an ultraviolet (black light) source. These will fluoresce when exposed to the correct light source. Part of the blended security features within the microprint on the background will also fluoresce when exposed to the correct light source.</p>	
Laser Engraving / Etching	<p><b>Security Feature: Level 1</b></p> <p>A method of personalizing cards with photographs and variable personal data using focused laser energy. It also generates level 1 security by using extra laser energy to disturb the page surface, thus creating tactility.</p>	

Tactile Data	<p><b>Security Feature: Level 1,2</b></p> <p>A proposed option for WV included in our base card as well as Option 2, is our clear laser feature. Clear laser combines both laser marking and secure indent to create an individually personalized clear security feature that is all but impossible to alter or and counterfeit. Overlap of this feature with the primary photo, with further prevent fraudulent attempts at image substitution. Our clear laser feature can also contain a pattern, design or outline that can be customized to WV for a level 2 security feature.</p>	 
Overlapping Data	<p><b>Security Feature: Level 1,2</b></p> <p>Overlapping of data fields adds increased difficulty to counterfeit attempts. This is accomplished during the data application process, with the primary signature overlapping the primary photo on the Driver's License and Identification card. Overlapping data has been found to be an effective deterrent against attempts at photo substitution style fraud.</p>	
PersoCurve / Laser Shadow	<p><b>Security Feature: Level 1,2 (Optional)</b></p> <p>PersoCurve combines unique variable large fonts, microprint, and biographical data, such as a name, document number etc. using laser engraving. The shape can be designed and customized in many different forms. For example</p>	

	<p>to wrap around in a spiral manner or a wave shape.</p> <p>This variable text image is created automatically during the job run without requiring pre-conversion of stored images because it provides more flexibility and efficiencies to the process of using unique images, without having to extract from a pre-converted file in a database.</p> <p>LaserShadow uses a dithered laser engraving technology to create large backgrounds of variable text or images that overlap other personalized data fields.</p>	
<p>Security Background Overlapping the Portrait Image Area</p>	<p><b>Security Feature: Level 1,2</b></p> <p>To provide for optimum visibility of the photograph, there is little or no printing in the relevant areas of the card. The harmonious phasing out of the image into the background print and overlapping the portrait edges makes it difficult to alter or counterfeit. Veridos has intentionally designed the background design to overlap the defined photo area.</p>	

Pre-Printed Serial Number on Card Backs – Document Control Number (DCN)	<p><b>Security Feature: Level 1,2</b></p> <p>Veridos assigns each DL/ID card a DCN on the card back. The DCN is laser engraved and consists of a unique alphanumeric value consisting of two alpha characters and seven numeric characters.</p> <p>A database of these DCNs is recorded and provided to WVDMV prior to storage in the secure vault. Cards are then transported to the secure vault and fully inventoried. The secure vault has its own CCTV system and is always operated under dual custody. WVDMV will have access to the 'Vault DCN Report' which is a standard report generated by Veridos' Online Portal.</p>	
Machine Readable Technology (MRT) (rear)	1D-barcode; Code-39, Verifies the authenticity of the document, the data or the person by the use of a reader and comparison of the stored data to other information.	
Machine Readable Technology (MRT) (rear)	2D-barcode; PDF-417, Verifies the authenticity of the document, the data or the person by the use of a reader and comparison of the stored data to other information.	

Section 4, Subsection 5.27.2 - Card design must comply with West Virginia Code §Chapter 17B Motor Vehicle Driver's License (<http://www.legis.state.wv.us/wvcode/Code.cfm?char=17b&art=1>)

**Vendor Response:**

Our proposed solution complies.

Section 4, Subsection 5.28 - Card Materials and Security Features

Section 4, Subsection 5.28.1 - Card materials must be serialized during manufacturing. Vendor Response:

Our proposed solution complies.

During the Manufacturing process, a Document Control Number (DCN) is laser engraved on each card which are then transported to our secure vault and fully inventoried. A database of DCNs is sent to the WVDMV prior to storage in our secure vault which has its own surveillance cameras and is always operated under dual custody.



While on premises, all card bodies are subject to secure storage as well as a rigorous tracking and inventory management program that ensures materials, card bodies, and other components are safe from theft. All material use and machine use is fully tracked and monitored as described below to ensure there is no unauthorized use of the facility.

Internal inventory control procedures include dual control ("four eyes principle") and secure storage as detailed in the card security section. Veridos will manage card inventory and raw materials including:

- Maintaining the proper inventory level in a secure facility consistent with distributor or operator needs.
- Tracking of all raw materials and undistributed cards until they leave the Veridos facility.
- Maintaining a separate inventory for disaster recovery purposes in a Veridos secure card production facility within the United States.

Since Veridos manufactures and produces the card blanks within the Card Production Center, no transport of card blanks outside the facility is required. This facilitates increased security and decreases transport access risks and costs.

Raw materials that are used in card manufacturing – printing plates, raw materials, laminating plates, elemental security features, etc. – are considered secure materials. All secure materials are subject to secure shipping and inventory control measures through the entire production process. This process includes shipping of final card products, destruction of scrap material, and returns of defective raw materials to the supplier.

Veridos provides information for the inventory and accounting system for each raw material, card type and category until the cards leave the secure facility. During the period of time that the cards are in Veridos' possession, we will have full responsibility for security, including providing inventory and accounting information.

**Section 4, Subsection 5.28.2 - Specific card layout and design will be selected during the planning phase after contract award.**

**Vendor Response:**

Our proposed solution complies.

The proposed card design for West Virginia will be carefully drafted to incorporate the best security features from a multi-disciplinary design team experienced in secure government documents. Not only will these cards be highly resistant to tampering and counterfeit but will include layered validation options for private citizens, law enforcement and forensic investigation.

Veridos is an active partner to industry associations such as AAMVA and ISO. Through our participation in industry events we are able to offer our clients the most current industry trends as well as pro-actively counter emerging threats.

**In the words of Manitoba:**

"G&D [Veridos] has provided expert guidance on the basis of its extensive experience in smart card design and production, and has been instrumental in working with our various stakeholders to deliver outstanding project services, while continuing to be helpful and supportive throughout all."



Section 4, subsection 5.28.3 - The credential must comply with 2016 AAMVA DL/ID Card Design Standard -Annex B Physical Security requirements listed (<http://www.aamva.org/2016CardDesignStandard/>).

**Vendor Response:**

Our proposed solution complies.

Section 4, Subsection 5.29 - Card Design Changes

Section 4, Subsection 5.29.1 - Any changes to the card design will be handled by Change Request, approved by the agency based on an hourly rate as defined in Attachment C Cost Sheet.

**Vendor Response:**

Our proposed solution complies.

Our commitment to the ongoing security of the WVDMV program is reflected in our everyday partnership. The WVDMV will have a dedicated Relationship Manager who is available at any time to discuss individual concerns. The Relationship Manager also reports directly to the Account Executive who will routinely discuss recommendations for additional design changes to combat evolving threats.

Veridos takes pride in being at the forefront of innovative technology to be one step ahead of fraudulent attempts to replicate Driver's Licenses and national forms of identification. Our R&D department is focused on developing new security features and card enhancements that allow the card to be refreshed over a long-term contract. We work closely with law enforcement and our customers to hold bi-annual meetings to review the cards and explore ways to enhance or introduce new security features. In addition, our internal graphics department is current on all standards to ensure that correct specifications are being adhered to before the card goes to print. To facilitate these efforts we have allowed for the design of the card to be flexible in the sense that new security features can be incorporated without transforming the entire image. All cards manufactured and produced adhere to AAMVA standards and requirements; this applies to card body features and also to personalized features such as barcode, etc.

---

Section 4, Subsection 5.29.2 - Vendor must implement card format changes within 30 days of Change Request approval.

**Vendor Response:**

Our proposed solution complies.

---

Section 4, Subsection 5.30 - Consumables for Secure Temporary DL

Section 4, Subsection 5.30.1 Secure paper stock to produce secure temporary DL will be provided to the Agency by the Vendor.

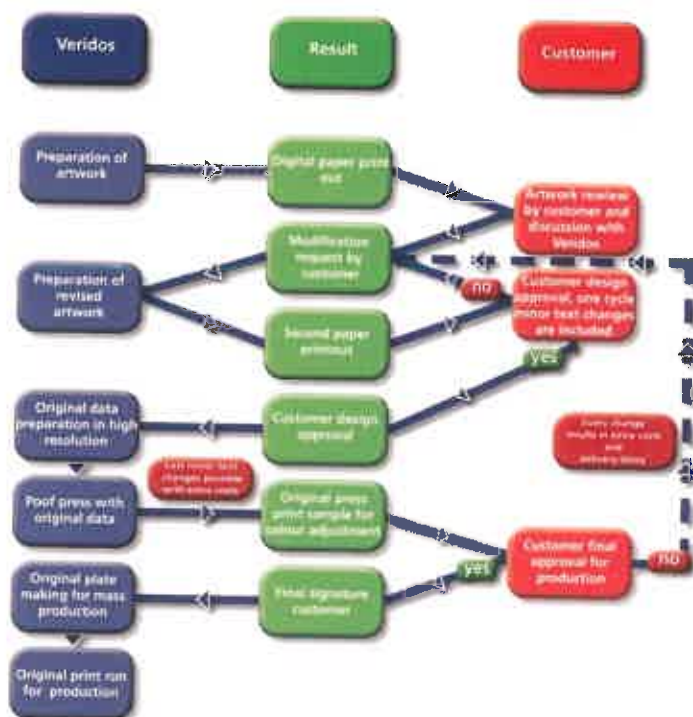
**Vendor Response:**

Our proposed solution complies.











The design of the Temporary DL/ID will be generated according to WVDMV specifications. The design, creation, origination and approval process is illustrated below and the respective steps can be deduced from it. The following steps will be part of the approval process:

- 3) Approval of design artwork (graphical)
- 4) Approval of origination

This process is outlined below.



The proposed paper includes the following features:

Element	Description	Verification level
	<b>High-security paper</b> <ul style="list-style-type: none"> <li>The paper of the Interim Driver License is composed of paper with 100% cellulose.</li> <li>The paper does not contain optical brighteners (dull, non-fluorescent).</li> <li>This paper is restricted to high-security applications and the material is not available to the public on the open market.</li> <li>The paper allows for high-resolution inkjet personalization.</li> </ul>	<div>1 </div> <div>1 </div> <div>2 </div>
	<b>Protection against chemical erasure</b> <ul style="list-style-type: none"> <li>The paper contains a chemical agent which reacts strongly on contact with acids, alkalis, bleaching agents and organic solvents, producing a visible stain. These chemicals are frequently used by counterfeiters in an attempt to remove information from the Interim Driver License.</li> </ul>	2 
	<b>UV security fibers</b> <ul style="list-style-type: none"> <li>Invisible fibers in the paper, which become visible in bright colors in blue, red and green when the paper is exposed to ultraviolet light. This feature is not available for ordinary office paper.</li> </ul>	2 
	<b>Visible security fibers</b> <ul style="list-style-type: none"> <li>Visible fibers, which are easily recognizable by the human eye, are integrated with the paper.</li> </ul>	1 

---

## COVERT SYSTEM REQUIREMENTS

Section 4, Subsection 5.31 - The Agency requires system functionality to support the issuance of covert credentials. For security reasons, details of the desired functionality will not be provided as part of the Request for Proposal. The Agency believes that Vendors understand the needs for this type of program and will be able to address those needs appropriately during the planning and design phase of the project. Vendor must not include details of their covert systems in their response but must acknowledge that this is a required functionality that must be provided.

### Vendor Response:

Our proposed solution complies. Veridos is very familiar with these types of credentials and acknowledges that this is a required functionality that will be provided with our solution.

---

## MAINTENANCE AND SUPPORT.

Section 4, Subsection 5.32 - This is a critical system and shall be operational and fully supported 7:00 a.m. to 8:00 p.m. EST Monday through Friday, and 7:00 a.m. to 2:00 p.m. EST on Saturday.

Section 4, Subsection 533 - The Vendor's solution must be compatible with the networking and operating environment established by the Office of Technology at the time of award, currently consisting of:

533.1 Internet Explorer version: 11

5.33.2 Java version: 7

5.33.3 .NET Framework version: 4.1

### Vendor Response:

Our proposed solution complies and is compatible with these networking and operating environments.

- Internet Explorer 11 – Yes
- Java Verison 7 – Yes
- .NET Framework version 4.1 - Yes

Section 4, Subsection 5.34 - Changes to this environment will be addressed by Change Order as this environment could change as new security vulnerabilities are identified and addressed in future updates.

**Vendor Response:**

Our proposed solution complies.

Section 4, Subsection 5.35 - The Vendor's solution must maintain full functionality and operations with any Office of Technology published security update within 30 days of scheduled release.

**Vendor Response:**

Our proposed solution complies.

The Veridos solution complies and maintains compatibility with future Windows updates, operating system security patches and Web browsers.

**PROJECT MANAGEMENT RESPONSIBILITIES Section 4, Subsection 5.36 - Project Work Plan**

Section 4, Subsection 5.36.1 - The project work plan will be as detailed as possible with the understanding that it will be revised during the planning and initiation phase of the project.

**Vendor Response:**

Our proposed solution complies.

Our Sample Project Work Plan is provided in Exhibit C.

Section 4, Subsection 5.36.2 - The project work plan will be a living document that must be kept up to date with tasks completed, modified, or added through the life of the project.

**Vendor Response:**

Our proposed solution complies.

The Project Work Plan will be updated as needed throughout the life of the project and will be kept up-to-date with tasks completed, modified or added.

Section 4, Subsection 5.36.3 - The project work plan will be used as a measurement of progress. Vendor Response:

Our proposed solution complies. This requirement is in accordance with our Project Management disciplines.

Section 4, Subsection 5.37 - Performance Testing

Section 4, Subsection 5.37.1 - Performance testing shall end when the system has met the standard of performance for a period of seven (7) consecutive calendar days. The standard of performance shall mean the system operates in conformance with the Vendor's technical and functional specifications, in conformance with this contract, and in conformance to the mutually agreed test criteria.

Vendor Response:

Our proposed solution complies.

Section 4, Subsection 537.2 - If the System fails during a seven (7) day period, the Vendor will re-start performance testing. The testing shall continue daily until the standard of performance is met, without downtime, for a total of seven (7) calendar days.

Vendor Response:

Our proposed solution complies.

Section 4, Subsection 537.3 - The Vendor is to provide the mechanism to create load and stress conditions. Metrics and results of the load and stress testing must be provided to the Agency for review and approval.

Vendor Response:

Our proposed solution complies.

Veridos conducts stress tests as a normal test procedure to ensure that the system can handle peak production volumes. The stress testing plans will be included in our Test Plans for review and approval by WVDMMV.

#### Section 4, Subsection 5.38 - Change Control Plan

Section 4, Subsection 5.38.1 - The Vendor shall develop, implement, and maintain a Change Control Plan, subject to the Agency approval, in accordance with industry standards that sets forth the procedures for controlling changes to project scope, cost, schedule, and quality requirements. The Change Control Plan shall include the procedures and entities involved with requesting, evaluating and approving changes to the project deliverables.

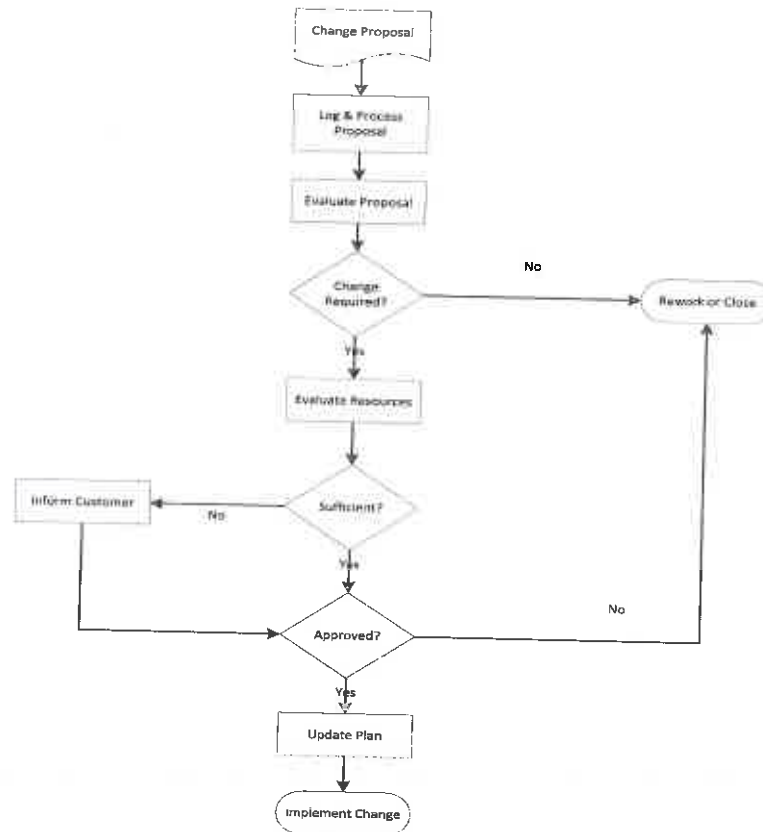
#### Vendor Response:

Our proposed solution complies.

Change Management is a process that provides a mechanism to identify and handle change in a project. Change that will occur can affect the scope, nature of the deliverables. In order to maintain the balance between requirements and the schedule, the project manager will establish a Change Management Process. This process allows for change during the project's life cycle, but will always place change in the context of the latest documented agreement (project plan) between WVDMV and Veridos.

Veridos maintains a change management process to manage the scope of the project and to reduce the risk to timelines. A Change Request process will apply to changes of Project scope, Project Requirements, and/or the timing of Project deliverables as requested by WVDMV or by Veridos. Change request can easily be initiated by sending a written request to Veridos in the form of a Project Change Request form. The Veridos Project Manager will be responsible for the receipt, tracking, communication of impacts and coordination of the customer initiated change requests.

The Change Management Process consists of a series of steps that allows changes to be identified, evaluated and tracked through closure. A typical Change Control Process is illustrated in the following Figure. The Lead Project Manager shall implement a Change Management Process according to the particular needs of this project. Based on previous experience in managing projects of similar size and scope, it is envisioned that change requests will be submitted to the Steering Committee for review and approval. Should the Change Request involve a significant change to the Project Charter, the Change Request will be escalated to the Executive Sponsor for review and approval.



### Decision Requests

For issues of lesser scope than full project changes, a Project Decision Request form can be completed to request approval to: 1) clarify project parameters or deviations from the original scope, 2) when the possible choices are within the bounds of the requirements, or 3) to outline options that may eventually lead to a Change Request where selection of a particular option will have an impact on the agreed upon basis of the project.

### Change Management on Similar Projects

Veridos has utilized our Change Management process for projects of similar size and complexity to update customers' security and technologies to keep on the cutting edge and ensure they meet all jurisdictional standards and regulations as they evolve.

Section 4, Subsection 538.2 - All changes must be documented. Approval must be obtained prior to any work on changes. Documented changes must have official sign-off by both the Agency and Vendor project managers and must include the reason for the change.

Vendor Response:

Our proposed solution complies.

Section 4, Subsection 5.39 - Change Orders

Section 4, Subsection 539.1 - Care must be taken when evaluating the requirements and preparing the cost proposal. Change orders are rarely approved. If a scope change does occur impacting the cost or timeline of the project, the Agency Project Manager and the Agency Purchasing Office must be notified in writing immediately upon discovery and BEFORE any work takes place.

Vendor Response:

Our proposed solution complies.

Section 4, Subsection 539.2 - Change orders submitted for work that has already been completed will NOT be considered. Written approval must be obtained prior to any work that is considered outside the original scope.

Vendor Response:

Our proposed solution complies.

Section 4, Subsection 5.40 - Upgrades, Patches, Fixes, or Other System Updates

Section 4, Subsection 5.40.1 - Ongoing changes to the Vendor's systems or hardware must be documented, tested, and approved by the Agency. Any changes during the life of the contract fall under the testing criteria listed above in paragraph 4.30 thru 4.33.

Vendor Response:

Our proposed solution complies.

All changes to the production environment, regardless of size and scope, must be signed-off by the process owners and coordinated by the cross-functional project teams. Veridos has a vigorous testing discipline supported by a testing environment in both the IT and production functions. This testing often incorporates the coordinated involvement of both Veridos and the customer. A sign-off process is in place to accept the changes to the Production environment as well as changes to the customer's reporting.

**Section 4, Subsection 5.40.2 - Implementation or release of Vendor changes to any of the Vendor's software or hardware must be scheduled and approved by the Agency.**

**Vendor Response:**

Our proposed solution complies.

**Section 4, Subsection 5.40.3 - In the event of a problem with the upgrade, patch, fix, or other system updates, the Vendor shall have a plan to immediately restore the previous version or release to keep facilities in production.**

**Vendor Response:**

Our proposed solution complies.

With all software updates, Veridos includes a back-out/roll-back plan to restore the previous version or release to keep facilities in production.

---

**Section 4, Subsection 5.41 - Right to Reproduce and Distribute**

Section 4, Subsection 5.40.1 - All training material and documentation of this system will become the property of the Agency, which includes the right to reproduce documentation for distribution to system users and managers. All training material and documentation is subject to the Agency approval prior to use.

**Vendor Response:**

Our proposed solution complies.

---

**Section 4, Subsection 5.42 - Training Plan**

Section 4, Subsection 5.42.1 - Training dates for Train-the-Trainer will be determined as part of the implementation plan. The Vendor will be responsible for delivering the training to all employees designated as Train-the-Trainers.

**Vendor Response:**

Our proposed solution complies.

The Training Plan associated with the new DL / ID issuance solution will be uniquely created for WVDMMV by Veridos. The plan will be all-encompassing and train users on each of the systems and hardware elements provided by Veridos. By tailoring the schedules, methods and curriculum specifically to the needs of the WVDMMV in-house trainers, this in-depth training program will reduce risk and provide a smooth transition to the new system.

---

**Section 4, Subsection 5.42.2 - The training plan will be subject to the Agency's approval. Vendor Response:**

Our proposed solution complies.

A sample Training Plan is attached in our response to Section 4.37.1 and Exhibit A. This plan will be updated and approved in collaboration with WVDMMV's team to ensure the Training Plan captures all of WVDMMV's requirements.

---

#### Section 4, Subsection 5.43 - Training Costs

Section 4, Subsection 5.43.1 - The cost of all training and training materials must be included in cost of the card. The Agency will not be responsible for vendor related travel expenses associated with installation or training at facilities.

##### Vendor Response:

Our proposed solution complies. Our price includes all required training and training materials and also includes travel expenses associated with installation and training at WVDMV facilities.

---

#### Section 4, Subsection 5.44 - Implementation Plan

Section 4, Subsection 5.44.1 - The Vendor must fully implement the system and all components at all facilities in the State of West Virginia by October 1, 2019.

##### Vendor Response:

Our proposed solution complies.

Our proposed work plan identifies the major tasks required to meet this date. Veridos has extensive experience implementing similar systems in less than one year. Please see Exhibit C for our Sample Project Work Plan.

---

#### Section 4, Subsection 5.45

##### - Data Migration

Section 4, Subsection 5.45.1 - The Vendor must provide a detailed plan for migrating the data from the current MIDS image database into the new central image/demographic system database.

##### Vendor Response:

Our proposed solution complies.

Before undertaking any migration project, a clear understanding of the environment to be migrated to and from is a necessity. Without a sufficient understanding of both source and target system, transferring data into a more sophisticated application will amplify the negative impact of any incorrect or irrelevant data, perpetuate any hidden legacy problems, and increase exposure to risk.

Veridos understands the importance of WVDMV's business needing to run 24 hours a day, 7 days a week even during this migration phase. We have successfully migrated data in other large programs by adopting the incremental approach to migrating data. Rather than aim to complete the whole event at once requiring downtime, trickle migration involves running the old and new systems in parallel and migrating the data in phases. This results in no interruption to work and no system downtime.

Veridos has specially designed tools that allows us to successfully migrate the data into the new FRS systems in a well-defined process. The tool ensures that the images are successfully enrolled in the FRS, 1:N, and 1:R searches are done as required, and the results of those actions being a record enrolled and also placed into an appropriate queue as required.

The queues are either the special handling queue where images that were not successfully enrolled can have operator intervention such as re-cropping the image, manually annotating the eyes, or other corrective actions that are necessary for the specific failure. Records may also be automatically placed in the adjudication queues if there are hits on any of the, 1:N, or 1:R checks. Otherwise records that are successfully enrolled and had no hits will remain in the FRS battery to be used as probe images as required by the contact.

Migration of existing customer images into the facial comparison system will be conducted using the following steps.

#### Data Migration Process

The data migration process involves repeating a set of batch import tasks over a period of several weeks. The optimal size of each batch import will be determined through empirical testing (initial estimate would be 300 to 500k records).

The tasks involved in accomplishing each batch import will include:

- 6) Export of the credential data from the source database:
  - a. The format of the exported data is a comma separated file (one line for each credential containing the above fields in the order shown) and the set of referenced photo files
  - b. Assign in the export database and export file an 'Issuance ID' for each credential record which will be used as a key reference between the FRS databases
  - c. Transfer from the source Datacenter to the WVDMV Datacenter
- 7) Creation of the FRS import files:
  - a. The Secura Import Manager utility will be used to read in the data file exported in the previous steps and create the FRS batch files
- 8) Execute the FRS batch import commands which will:
  - a. Read the records from the FRS batch import file



- b. At a scheduled interval, the FRS workflow engine will process new entries
  - c. Create and store in the FRS database facial comparison templates for each photo referenced in the imported records
- 9) Manually enroll failed records:
  - a. For those records will failed to enroll during the FRS batch enrollment process, use the Database Enrollment application to manually specify the eye locations to be used in creating the facial comparison template
- 10) Validate the result of the batch import:
  - a. Use supplied database queries to reconcile the number of records in the source import file to the number of records imported to FRS
  - b. Send the validate report via email to jurisdiction
  - c. Once the batch import results have been validated, the import data files will be deleted

Note: Steps 2-5 above will generate log files which will be monitored for errors. Any errors that occur will be addressed and the import resumed.

### **Data Migration Plan**

The following sections outline the data migration activities and milestones for each FRS deployment (refer to the latest version of the document).

#### **Development 1**

- No data migration activities are required for the Development 1 deployment

#### **System Integration Testing (SIT)**

- The import of 500,000 to 1 million records will be required to:
  - Support integration and testing of the FRS functionality
  - Determine the optimal export package size
  - Estimate the time to import an export package
- **Milestone:** Establish the Export Package size and expected time to import

#### **User Acceptance Testing (UAT)**

- The import of at least 2 to 3 million records will be required to:
  - Support user acceptance testing of the FRS functionality
  - Determine the time to import an export package to support production migration scheduling

- Determine the data required to be included in the Import Validation Report
- **Milestone:** Create the Production Migration schedule based on the export package size and time to import
- **Milestone:** Define the contents of the Import Validation Report

#### **Production Records prior to installation**

- The import of all existing customer records per the Production Migration schedule
- **Milestone:** All customer records migrated to the FRS

#### **Data Migration During Transition**

The daily import and enrollment of records which have been processed through the existing system during the transition period between the new and the old FRS solutions. This process is used to ensure the new FRS has the maintains the entire dataset once the data migration process has started until the go live date and decommissioning of the existing solution occurs.

#### **Process:**

- A import file is extracted each evening from the existing system and imported into the new FRS each morning
- The import file records go through the same processing as if submitted from FRS Enrollment
- All leads from existing system's probes are adjudicated in the new FRS
- For fraud that is found in new FRS but not in old solution, a report is generated that is used to notify the bureau to suspend production on those specific records.

Given this plan and our FRS's ability to work successfully with low quality images, Veridos will be able to import the required images successfully into WVDMMV's new system.

---

## SERVICE LEVEL AGREEMENT

### Section 4, Subsection 5.46 - Preventive and Remedial Maintenance

Section 4, Subsection 5.46.1 - The Vendor shall provide all remedial and preventative maintenance for all system components (hardware and software) including provision of all parts and labor during the term of the contract.

#### Vendor Response:

Our proposed solution complies.

---

Section 4, Subsection 5.46.2 - On-site remedial and preventative maintenance for facility equipment shall be available during facility working hours, generally between 7:00am and 8:00pm, Eastern Time, Monday through Friday, and 7:00am and 2:00pm, Eastern Time on Saturday.

#### Vendor Response:

Our proposed solution complies.

Our help desk systems include; 1) A web portal to submit service requests. 2) An established toll free number. 3) A ticketing system.

- The help desk system will be available from 7:00 AM to 8:00 PM during weekdays and 7:00 AM to 2:00 PM on Saturdays.
- The help desk will be staffed from A service request from WVDMV would be submitted through our web portal. A service request may also be submitted by placing a call to our 800 number or by email though the most efficient option is the use of the web portal.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes
- A service ticket will be created by the help desk team. The ticket and its status will be visible to the WVDMV team through the web portal.
- Our help desk team will immediately contact the site that is reporting the issue immediately and execute the troubleshooting protocol.
- If the issue was not resolved by the troubleshooting protocol then a field technician will be immediately dispatched and will be onsite within the agreed upon SLA.

- All field technicians will have two devices in their possession as well as any other materials that may be needed to service the devices (i.e., cabling, patch cables, etc.).
- The field technician will quickly execute the troubleshooting protocol again. The technician will determine if the failure is due to a hardware or software issue.
  - If the failure is determined to be an Agency issue then the technician will immediately contact WVDMV technical support team to report the issue and continue to troubleshoot the issue in collaboration with the WVDMV technical team.
  - If the failure is determined to be a hardware issue the device will be immediately uninstalled. A replacement device will be installed and tested. The onsite contact will be kept updated throughout the service call. The technician will fill out a form to track the asset being removed and the asset being installed. The site log would also be updated. This information would be included in the field service record.
- The field technician will update the help desk team before leaving the site as to the resolution of the ticket.
- The help desk team will immediately update the ticket and close it.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes. The resolutions will be recorded and reconciled within the web-based help desk system for the consumption of fellow Help Desk Operators and facilitating the WVDMV to generate reports.
- Veridos will provide an incident report via the web-based tracking system to the WVDMV upon completion of a service call detailing the actions taken to resolve the problem and status of the problem.
- The field technician would return the removed asset to the field services headquarters to be repaired or returned to the manufacturer.

Section 4, Subsection 5.46.3 - Preventative maintenance for the central image/demographic system and / or facial recognition system components must be completed during pre-arranged maintenance windows, generally on weekends, outside of normal business hours.

**Vendor Response:**

Our proposed solution complies.

Section 4, Subsection 5.46.4 - No costs related to maintenance of hardware and software, including travel time and expenses, shall be billable to the Agency. These costs must be included in the cost per card.

**Vendor Response:**

Our proposed solution complies.

Our pricing includes travel time and expenses related to maintenance of the hardware and software.

**Section 4, Subsection 5.47 - Service Response Times**

Section 4, Subsection 5.47.1 - Chronic or repeat issues - the Vendor will immediately dispatch a system expert to the site of the local image server or facial recognition system if a problem remains undiagnosed and/or unresolved after twenty-four (24) hours, and if the problem affects facility operations or other issuance or retrieval operations or prevents or impedes proper database storage and back up processes, even if it does not result in down time.

**Vendor Response:**

Our proposed solution complies.

Section 4, Subsection 5.47.2 - If reported problems are not resolved within the required response times, the Vendor shall be deemed in default of these standards of performance. In such an instance, the Vendor and the Agency will determine if it is necessary to provide an alternative solution that allows operations to continue.

**Vendor Response:**

Our proposed solution complies.

Our proposed solution has been proven to be very reliable for our existing customers so we anticipate that all problems will be resolved within the required response times.

Section 4, Subsection 5.47.3 - Support issues, tickets, or calls must not be closed without confirmation from the Agency that the issue has been resolved.

**Vendor Response:**

Our proposed solution complies.

Our help desk systems include; 1) A web portal to submit service requests. 2) An established toll free number. 3) A ticketing system. Tickets are opened for every issue and call received and are closed without confirmation from WVDVM that the issue has been resolved.

- The help desk system will be available from 7:00 AM to 8:00 PM during weekdays and 7:00 AM to 2:00 PM on Saturdays.
- The help desk will be staffed from A service request from WVDMV would be submitted through our web portal. A service request may also be submitted by placing a call to our 800 number or by email though the most efficient option is the use of the web portal.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes
- A service ticket will be created by the help desk team. The ticket and its status will be visible to the WVDMV team through the web portal.
- Our help desk team will immediately contact the site that is reporting the issue immediately and execute the troubleshooting protocol.
- If the issue was not resolved by the troubleshooting protocol then a field technician will be immediately dispatched and will be onsite within the agreed upon SLA.

- All field technicians will have two devices in their possession as well as any other materials that may be needed to service the devices (i.e., cabling, patch cables, etc.).
- The field technician will quickly execute the troubleshooting protocol again. The technician will determine if the failure is due to a hardware or software issue.
  - If the failure is determined to be an Agency issue then the technician will immediately contact WVDMV technical support team to report the issue and continue to troubleshoot the issue in collaboration with the WVDMV technical team.
  - If the failure is determined to be a hardware issue the device will be immediately uninstalled. A replacement device will be installed and tested. The onsite contact will be kept updated throughout the service call. The technician will fill out a form to track the asset being removed and the asset being installed. The site log would also be updated. This information would be included in the field service record.
- The field technician will update the help desk team before leaving the site as to the resolution of the ticket.
- The help desk team will immediately update the ticket and close it.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes. The resolutions will be recorded and reconciled within the web-based help desk system for the consumption of fellow Help Desk Operators and facilitating the WVDMV to generate reports.
- Veridos will provide an incident report via the web-based tracking system to the WVDMV upon completion of a service call detailing the actions taken to resolve the problem and status of the problem.
- The field technician would return the removed asset to the field services headquarters to be repaired or returned to the manufacturer.
- The Veridos team will submit monthly reports to WVDMV related to all service requests received for the month. The report will highlight the following service request data:

**Volume Summary** - Each month a summary of all service requests will be provided by the Contractor that quantifies problem types, resolution types, etc. by equipment type. This information will include a previous twelve months to help identify trends.

**Inventory Report** - Each month a comprehensive inventory is reported that shows the location and status of all Contractor equipment. This report will track all installed equipment, spare pool hardware, and equipment out for repair. Any equipment that is permanently removed from service will be considered

"retired" and can no longer be transacted against, but a record should be maintained in an inactive status for historical purposes.

**Performance Report** – This monthly report will list all of the performance data against SLA requirements including; response time, ETA, arrival time, time to repair and close time against WVDMV business hours. This data is generated monthly and published with a twelve-month history for trend analysis.

**Ad Hoc Reports** - Contractor will provide reports to WVDMV on request that will in general be specific to WVDMV needs regarding: problems, call volume analysis and comparison at the site level, site history reporting, operator history reporting etc.

The escalation process for the help desk will be determined in collaboration between WVDMV and Veridos, based upon WVDMV's requirements.

An Incident Management Process is used to track and resolve issues. The primary goal of the Incident Management process is to restore normal service operation as quickly as possible.

A service ticket will be created by the help desk team. The ticket and its status will be visible to the WVDMV's internal support team through our web portal.

Our help desk team will immediately contact the site that is reporting the issue and execute the troubleshooting protocols.

If the issue was not resolved by the troubleshooting protocol then a field technician will be immediately dispatched and will be onsite within the SLA.

If the failure is determined to be a hardware issue the device will be immediately uninstalled. A replacement device will be installed and tested. The onsite contact will be kept updated throughout the service call. The technician will track the asset being removed and the asset being installed. This information would be included in the field service record.

- The field technician will update the help desk team before leaving the site as to the resolution of the ticket.
- The help desk team will immediately update the ticket and close it.
- The field technician will return the removed asset to the field services headquarters to be repaired or returned to the manufacturer.

**Section 4, Subsection 5.48 - System Availability**

**Section 4, Subsection 5.48.1 - All image capture workstations must be available during regular Agency business hours, and during extended hours for special events as needed.**

**Vendor Response:**

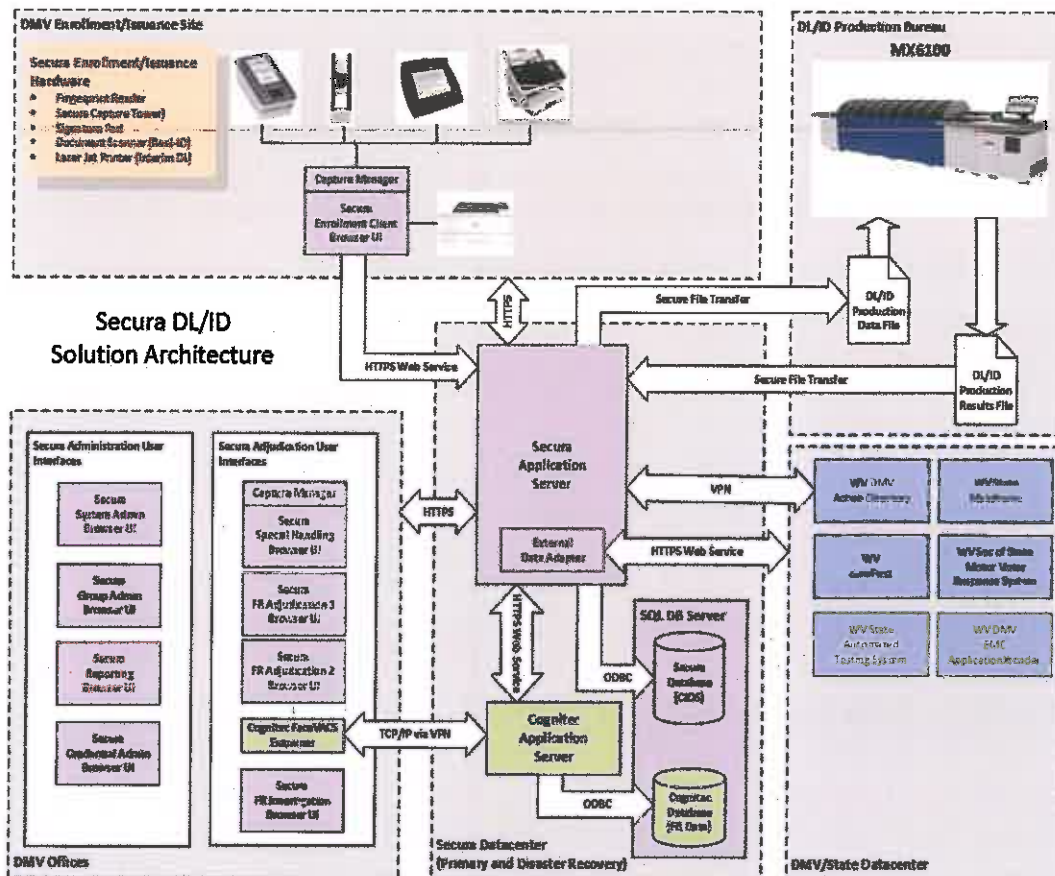
Our proposed solution complies.

The image capture workstations will be available 24/7 depending upon the Agency's network and data center availability.

**Section 4, Subsection 5.48.2 - All servers used as part of the Vendor solution must be configured for automatic failover to minimize system downtime.**

**Vendor Response:**

Our proposed solution complies.



---

The production deployment of the Secura FRS will consist of redundant 'Primary' and 'Disaster Recovery' environments which contain the Secura Datacenter components. These components consist of:

- Secura Application Server
- Cognitec Application Server
- SQL Database Server (Primary and Disaster Recovery mirrored)

An additional 'Test' environment will also be deployed to support User Acceptance Testing and testing of future upgrades.

Section 4, Subsection 5.48.3 - Monthly maintenance windows for servers will be established, and the Vendor must provide notification of their intent to utilize the maintenance window no less than 1 week in advance.

Vendor Response:

Our proposed solution complies.

Section 4, Subsection 5.48.4 - Downtime is defined as any time that any portion of the ICW or FRS systems are unavailable for normal business operations, and when the Agency approved work around is not available.

Vendor Response:

Our proposed solution complies.

Section 4, Subsection 5.48.5 - Downtime will start from the time the Agency first notifies the Vendor's designated representative or Help Desk of the inoperative condition until it is returned to working order.

Vendor Response:

Our proposed solution complies.

Section 4, Subsection 5.49 - Help Desk Support

Section 4, Subsection 5.49.1 - During the entire term of the contract, the Vendor will provide the Agency with a toll-free Help Desk number and email address to contact the Vendor for technical support. At a minimum, the Help Desk Hours must be:

5.49.1.1 7:00am to 8:00pm, Eastern Time Monday through Friday

5.49.1.2 7:00am to 2:00pm, Eastern Time Saturdays

5.49.1.3 Extended hours as needed for special events such as the West Virginia State Fair. Vendor Response:

Our proposed solution complies.

Our help desk systems include; 1) A web portal to submit service requests. 2) An established toll free number. 3) A ticketing system. Tickets are opened for every issue and call received and are closed without confirmation from WVDVM that the issue has been resolved.

- The help desk system will be available from 7:00 AM to 8:00 PM during weekdays and 7:00 AM to 2:00 PM on Saturdays.
- The help desk will be staffed from A service request from WVDMV would be submitted through our web portal. A service request may also be submitted by placing a call to our 800 number or by email though the most efficient option is the use of the web portal.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes
- A service ticket will be created by the help desk team. The ticket and its status will be visible to the WVDMV team through the web portal.
- Our help desk team will immediately contact the site that is reporting the issue immediately and execute the troubleshooting protocol.
- If the issue was not resolved by the troubleshooting protocol then a field technician will be immediately dispatched and will be onsite within the agreed upon SLA.
- All field technicians will have two devices in their possession as well as any other materials that may be needed to service the devices (i.e., cabling, patch cables, etc.).
- The field technician will quickly execute the troubleshooting protocol again. The technician will determine if the failure is due to a hardware or software issue.
  - If the failure is determined to be an Agency issue then the technician will immediately contact WVDMV technical support team to report the issue and continue to troubleshoot the issue in collaboration with the WVDMV technical team.
  - If the failure is determined to be a hardware issue the device will be immediately uninstalled. A replacement device will be installed and tested. The onsite contact will be kept updated throughout the service call. The technician will fill out a form to track the asset being removed and the asset being installed. The site log would also be updated. This information would be included in the field service record.
- The field technician will update the help desk team before leaving the site as to the resolution of the ticket.
- The help desk team will immediately update the ticket and close it.
- The help desk will review and acknowledge receipt of all tickets within 15-minutes. The resolutions will be recorded and reconciled within the web-based help desk system for the consumption of fellow Help Desk Operators and facilitating the WVDMV to generate reports.

- Veridos will provide an incident report via the web-based tracking system to the WVDMV upon completion of a service call detailing the actions taken to resolve the problem and status of the problem.
- The field technician would return the removed asset to the field services headquarters to be repaired or returned to the manufacturer.

---

#### Section 4, Subsection 5.50 - Field Service Support

Section 4, Subsection 5.50.1 - The Agency must be provided with a list of all field service technicians, and the technicians must have a means of identifying themselves to the Agency staff when they arrive at the Agency location.

#### Vendor Response:

Our proposed solution complies.

A contact list for our field technicians will be provided to WVDMV, and our field technicians will wear ID badges when on-site at WVDMV locations.

---

Section 4, Subsection 5.50.1 - As part of the support agreement, Field service technicians will be required to set up and remove equipment for any special events, such as the West Virginia State Fair and other public demonstrations as determined by the State Governor or the Agency Commissioner.

**Vendor Response:**

Our proposed solution complies.

---

**INFORMATION TECHNOLOGY REQUIREMENTS Section 4, Subsection 5.51  
- Communications**

Section 4, Subsection 5.50.1 - The Agency will be responsible for data communication between the facilities and the Agency data center. Communication between the Agency data center and the central production facilities will be the responsibility of the Vendor.

**Vendor Response:**

Our proposed solution complies.

---

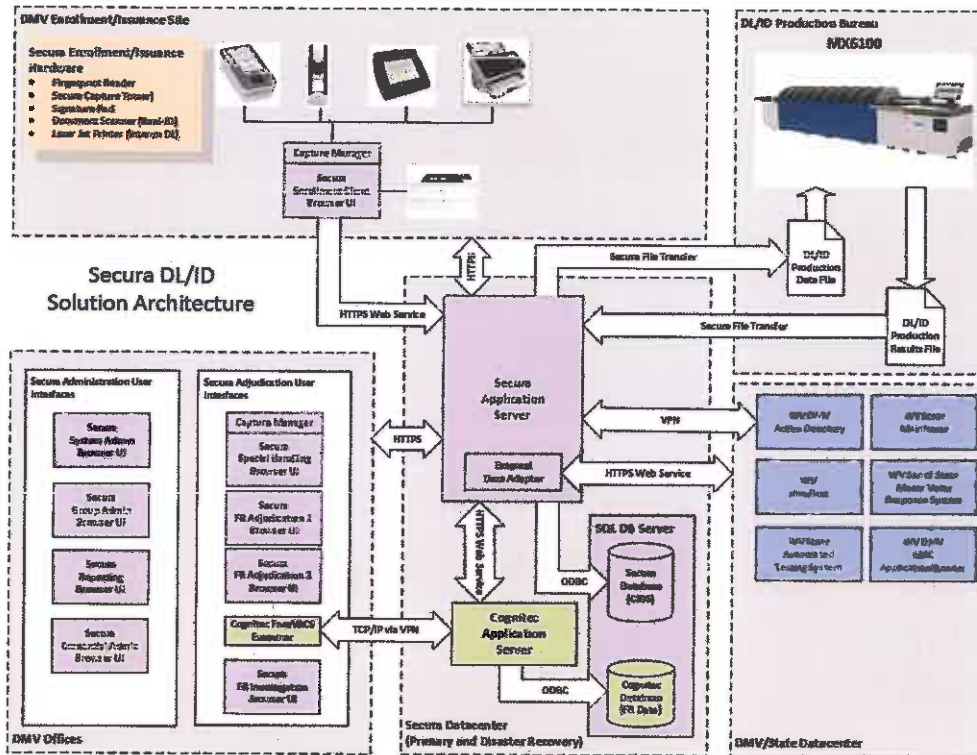
**Section 4, Subsection 5.52 - Data Storage**

Section 4, Subsection 5.52.1 - All documents scanned or collected in the application or production of a credential will be stored at the State's data center to comply with the State of West Virginia statutory requirements, administrative rules, and records retention requirements.

**Vendor Response:**

Our proposed solution complies.

As documented in the solution overview diagram below, all data associated with our proposed solution will be stored at the State's data center in compliance with the State's requirements.



Section 4, Subsection 5.52.2 - The data associated with this system is the property of the Agency and is not available for resale or distribution.

#### Vendor Response:

Our proposed solution complies.

Section 4, Subsection 5.52.2 - Data sent to the central production facility servers for card printing must be deleted no more than thirty (30) days after receipt of the print request.

#### Vendor Response:

Our proposed solution complies.

Our Card Production Services stores information in encrypted and masked formats at all times. In cases where the WVDMV requires Veridos to hold this limited or original information on any other basis, Veridos provides flexibility to ensure data availability in encrypted formats. Once data is deleted, Veridos maintains audit reports to confirm the deletion of such information. In order to ensure proper data retention and destruction

through the life of the contract, our solution is built to meet all AAMVA and North American standards for data retention and destruction practices.

---

#### Section 4, Subsection 5.53 - Software Updates

Section 4, Subsection 5.53.1 - Major software enhancements shall be charged on an hourly basis as defined by Attachment C - Cost Sheet. These enhancements could include, but shall not be limited to, State Legislative and Federal Rule or Compliance changes.

**Vendor Response:**

Our proposed solution complies.

---

Section 4, Subsection 5.53.2 - The Vendor must develop and provide a formal back-out plan for all updates in the event of failure.

**Vendor Response:**

Our proposed solution complies.

With all software updates, Veridos includes a back-out/roll-back plan to restore the previous version or release to keep facilities in production.

---

#### Section 4, Subsection 5.54 - Change to Production System

Section 4, Subsection 5.54.1 - At no time, shall anyone on the Vendor's staff make changes to the Agency production systems without coordination with the Agency, full system testing by both the Vendor and the Agency, and strict adherence to the change management process.

**Vendor Response:**

Our proposed solution complies.

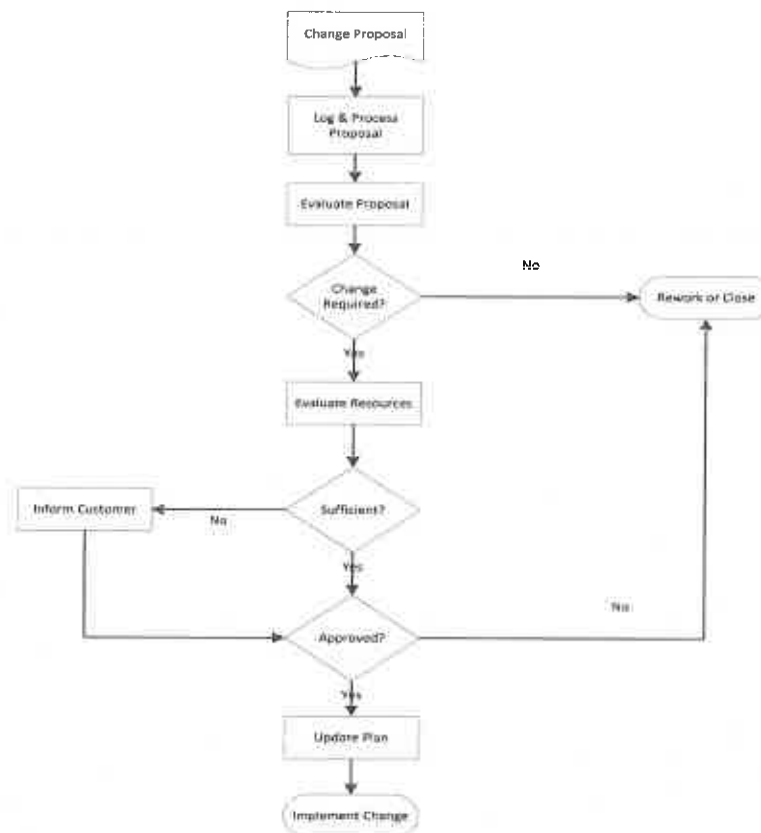
Change Management is a process that provides a mechanism to identify and handle change in a project. Change that will occur can affect the scope, nature of the deliverables. In order to maintain the balance between requirements and the schedule, the project manager will establish a Change Management Process. This process allows for change during the project's life cycle, but will always place change in the context of the latest documented agreement (project plan) between WDMV and Veridos.

Veridos maintains a change management process to manage the scope of the project and to reduce the risk to timelines. A Change Request process will apply to changes of



Project scope, Project Requirements, and/or the timing of Project deliverables as requested by WVDMV or by Veridos. Change request can easily be initiated by sending a written request to Veridos in the form of a Project Change Request form. The Veridos Project Manager will be responsible for the receipt, tracking, communication of impacts and coordination of the customer initiated change requests.

The Change Management Process consists of a series of steps that allows changes to be identified, evaluated and tracked through closure. A typical Change Control Process is illustrated in the following Figure. The Lead Project Manager shall implement a Change Management Process according to the particular needs of this project. Based on previous experience in managing projects of similar size and scope, it is envisioned that change requests will be submitted to the Steering Committee for review and approval. Should the Change Request involve a significant change to the Project Charter, the Change Request will be escalated to the Executive Sponsor for review and approval.



### Decision Requests

For issues of lesser scope than full project changes, a Project Decision Request form can be completed to request approval to: 1) clarify project parameters or deviations

from the original scope, 2) when the possible choices are within the bounds of the requirements, or 3) to outline options that may eventually lead to a Change Request where selection of a particular option will have an impact on the agreed upon basis of the project.

#### Change Management on Similar Projects

Veridos has utilized our Change Management process for projects of similar size and complexity to update customers' security and technologies to keep on the cutting edge and ensure they meet all jurisdictional standards and regulations as they evolve.

---

#### Section 4, Subsection 5.55 - 14 Day Pre-Post Support Plan

Section 4, Subsection 5.55.1 - The successful completion of the 14-day pre-post support period as determined by the Agency shall result in System Acceptance, leading to the issuance of the first Change Order.

#### Vendor Response:

Our proposed solution complies.

---

#### Section 4, Subsection 5.56 - End of Contract

Section 4, Subsection 5.56.1 - At the end of the contract, or sooner, if the contract is terminated, the Vendor must transfer all image files and data to the Agency or third-party database and delete all relevant data from their hosted servers with written approval from the Agency

#### Vendor Response:

It is our understanding that all data will reside on servers provided by the Agency and that Veridos will not be hosting servers for this program.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Veridos America, Inc.

(Company)

Paul Mazzeo, President



(Representative Name, Title)

905.946.2809

(Contact Phone/Fax Number)

June 28, 2018

(Date)

## Attachment F: WV DMV Contract Privacy Policy

**REQUEST FOR PROPOSAL**

111

WVDMV Driver's License and Credential Issuance System  
(dmvLICENSE) CRFP DMV1800000001**Attachment F:****WV Division of Motor Vehicles Contract Privacy Policy**

1. That the Agency is the record owner of and maintains electronic Driver Licensing and Motor Vehicle Information, including Personal Information and Sensitive Personal Information as defined in the federal Driver Privacy Protection Act ("DPPA") and the Uniform Motor Vehicles Records Disclosure Act (§17A-2A-1 et seq.) ("UMVRDA");
2. That pursuant to §17A-2A-7(a)(1), the Driver Licensing and Vehicle Information is available for release from the Agency to a governmental agency including any entity acting on behalf of a governmental agency in carrying out its function;
3. That the Agency will permit to the Vendor computer inquiry access to the Mainframe System, if necessary, using unique employees accounts, except those records which the AGENCY has been directed not to disclose pursuant to West Virginia Code or federal law as amended, by the person about whom the record is kept;
4. That the Vendor will use the information obtained hereunder only for the purpose set forth in their Statement of Work and made a part hereof, in compliance with federal and state privacy laws and the Privacy Program attached to and made part of this Agreement;
5. The Vendor agrees to reimburse the AGENCY, its agents, officers and employees for all claims, loss, damage, injury and liability asserted against the AGENCY, and any of their agents, officers and employees resulting from the negligent, criminal or willful wrongful use or misuse of the information provided to the Vendor on the part of the Vendor, its agents, officers, employees, contractors or a third party;
6. The Vendor assumes full responsibility for the care, custody, control, disclosure and use of the information provided to it by the AGENCY pursuant to this Agreement. The Vendor agrees to ensure that the disclosure of information received from the AGENCY complies with this Agreement. The Vendor assumes full responsibility for its disclosure of information pursuant to all Federal and State laws governing the disclosure and protection of such information, including but not limited to, the Federal Fair Credit Reporting Act (Law 91058), Driver's Privacy Protection Act, (Public Law 103-322 at 18 U.S.C. 123), the amendment to the Driver Privacy Protection Act, (Section 350 of Public Law 106-69), the West Virginia Uniform Motor Vehicle Records Disclosure Act, hereinafter the WVURDA (W. Va. Code 17A-2A-1 et seq.), the Privacy Act of 1974, Computer Security Act 1987, the Federal Information Security Management Act of 2002 (FISMA P.L. 107-347, December 17, 2002), the FIPS Publication 199, Standards for Security

Revised 6/8/2012

**REQUEST FOR PROPOSAL**

112

**WVDMV Driver's License and Credential Issuance System  
(dmvLICENSE) CRFP DMV1800000001**

Categorization of Federal Information and Information Systems, FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000, NIST SP 800-44 Version 2, Guidelines on Securing Public Web Servers, and NISP SP 800-14 Generally Accepted Principles and Practices for Security Information Technology Systems and W. Va. Code §17C-5A-3, all as amended:

7. That the Vendor shall immediately notify the AGENCY upon its discovery that the Vehicle or Driver owner address information provided to it has been released, used or disclosed in violation of this Agreement, in violation of any federal law, in violation of West Virginia law or upon the filing of any claim or complaint for misuse or release of the AGENCY's Vehicle Licensing Information made against the Vendor or against the AGENCY. Immediate notification for any privacy breach means that the Vendor will notify the AGENCY by calling 304.926.0708, by calling the West Virginia Office of Technology at 304.558.9966 or 877.558.9966 and by notifying the AGENCY in writing within 24 hours if it discovers that personal information provided under this Agreement has been used, disclosed or are being used in violation of the Agreement, or state or federal laws. Immediate notification for any privacy breach of Social Security Numbers, if applicable, means that the agency will notify the Social Security Administration within one hour of the breach by calling the SSA's National Network Service Center toll free at 877-697-4889;
8. The Vendor will provide the name, title and telephone number of its designated Security Administrator, as well as a photo copy of the Administrator's state issued driver's license or non-driver identification, to AGENCY before any records are accessed. The Security Administrator will be the employee of the Vendor who is responsible for access and use of any AGENCY records. The Security Administrator will be the employee of the Vendor who is responsible for requesting log-on identification numbers from the AGENCY and to whom the AGENCY may provide log-on identification numbers. The Security Administrator is responsible for the security of all log-on identification numbers assigned to the Vendor and will ensure that the assigned log-on identification numbers and passwords are not exchanged or shared with any other person(s) or entities. Additionally, the Security Administrator is responsible for ensuring that every Vendor employee with access to the records completes a Confidentiality Agreement and returns it to the AGENCY prior to use of the AGENCY records. All Confidentiality Agreements are made a part of this Agreement. If the Security Administrator or any employee of the Vendor leaves the employ of the Vendor or changes job duties and no longer requires access to AGENCY records as part of their official job assignments, the Security Administrator will immediately notify the AGENCY. The access log-on code for the employee will be cancelled. Prior to issuing a log-on number for a new employee, the Security Administrator will submit a signed Confidentiality Agreement from that employee which will become an addendum to this

**REQUEST FOR PROPOSAL**

113

**WVDMV Driver's License and Credential Issuance System  
(dmvLICENSE) CRFP DMV1800000001**

Agreement. Nothing in this Agreement authorizes the Vendor to have more than seven hundred and twenty-nine (729) log-on access numbers at a time. Within 30 days of separation or transfer, the Security Administrator will notify the AGENCY of any authorized user who no longer needs access to our records and may make a request to authorize a new log-on access number on a one for one basis;

9. The Vendor may not use any information provided hereunder for any purpose not listed in this Agreement without prior written approval of the AGENCY;
10. The Vendor agrees that it will not use any information contained in or derived from the records accessed from AGENCY for the purposes of marketing, surveys or solicitation;
11. The Vendor is specifically prohibited from releasing, selling, assigning or otherwise transferring information from AGENCY records to any unauthorized person, firm, association, corporation or government agency without permission in writing from the AGENCY;
12. The Vendor agrees to immediately notify the AGENCY of any claim asserted against the Vendor because of any use of the information provided pursuant to this Agreement. The Vendor agrees that AGENCY shall retain all ownership rights to the information provided pursuant to this Agreement or derived therefrom. The Vendor will enter personal information that it will verify with the AGENCY records. The Vendor agrees that it shall only use, store or combine data as authorized under state and federal law. The Vendor will only release information to the minimum necessary extent to execute its duties under state and federal law and in accordance with this Agreement. Provided, nothing in this Agreement prevents the Vendor from creating a database of personal information obtained from other sources;
13. The Vendor will take all reasonable precautions to protect against unauthorized access or release of AGENCY data records, confidential records or confidential information in its custody;
14. The Vendor agrees that any breach of this Agreement or unlawful use, sale or release of AGENCY records in any form by the Vendor or any of its clients will result in the immediate termination of this Agreement without prior notice to the Vendor. The Vendor agrees to reimburse to AGENCY all reasonable costs and attorney fees by the Vendor of its unlawful sale, release or use of any of AGENCY records;
15. This Agreement shall remain in full force and effect unless canceled by either party upon thirty (30) days written notice or anytime with the mutual consent of both parties. This Agreement shall terminate immediately upon discovery that any information provided to Vendor by the AGENCY has been used or disclosed in violation of this Agreement, State or Federal law. This Agreement shall terminate immediately if changes in West Virginia or Federal law prohibit the AGENCY

**REQUEST FOR PROPOSAL**

114

**WVDMV Driver's License and Credential Issuance System  
(dmvLICENSE) CRFP DMV1800000001**

from releasing the information accessed by this Agreement;

16. The Vendor and its employees, agents, contractors, subcontractors, assigns and heirs who will have access to the provided AGENCY records agree to read the Privacy Program. All personnel who will have access to the AGENCY's records must sign a Confidentiality Agreement prior to access of AGENCY records. Vendor employees who will have access to the Agency's records must submit a copy of their government-issued photo ID or driver's license with photograph. Failure to comply with this provision will affect deadlines required by the Vendor to access AGENCY records. The Vendor agrees that failure to submit Confidentiality Agreements from all Vendor employees who will access AGENCY's records constitutes a breach of the Agreement and the Vendor agrees that the AGENCY may terminate the Agreement without consequence to AGENCY on that basis;
17. The Vendor hereby agrees that it will only access Personally Identifiable Information, hereinafter PII, as required to perform its duties under the Agreement. The Vendor understands that it is required to secure the PII that it accesses as part of this Agreement and to ensure that it is not accessed by unauthorized individuals, or released to any other persons, companies or entities. The Vendor agrees that it will not allow its employees to share account access information or passwords;
18. The Vendor agrees that it will not release or allow access to AGENCY records to any person or company outside the United States of America;
19. This document, together with the Vendor's Statement of Work, the completed Vendor Employees' Confidentiality Agreements with photo IDs and the List of Vendor employees who will have a unique access account assigned to that individual will constitute the entire Agreement between the parties;
20. This Agreement is not assignable by the Vendor;
21. Venue of any lawsuit filed by any party arising in whole or in part out of this Agreement shall be in the Circuit Court of Kanawha County; and

**REQUEST FOR PROPOSAL**

115

**WVDMV Driver's License and Credential Issuance System  
(dmvLICENSE) CRFP DMV1800000001**

22. This Agreement may only be revised or amended in writing by mutual consent of both parties or with 30 days' prior written notice by either of the parties.

Vendor: Veridos America, Inc.

Authorized Signature: Kathleen Synotigaard, Director

Date: June 28, 2018

## Attachment H: PII Acknowledgement

118

### Attachment H

#### PII Acknowledgement

The Vendor understands that this Agreement requires access to Personally Identifiable Information or PII found within the WVDMV's records. Personally Identifiable Information includes any information that can identify a person, including, but not limited to the name, address, social security number, driver's license number, date of birth, photograph, computerized image, telephone number, medical information or disability information of any person or organization found in DMV records.

The Vendor understands that any PII obtained from the WVDMV's records is subject to the federal Driver Privacy Protection Act and the West Virginia Uniform Records Disclosure Act, hereinafter WVURDA found at West Virginia Code §17A-2A-1, et seq. A copy of the WVURDA is attached and made a part of this Agreement.

The Vendor and its' employees, agents, contractors, subcontractors, assigns and heirs agree to read the WVURDA, and all personnel who will have access to the WVDMV's records must sign a Confidentiality Agreement prior to access to PII found within the WVDMV's records. Failure to comply with this provision may affect deadlines required by the Vendor. The Vendor agrees that failure to submit Confidentiality Agreements from all Vendor users of the WVDMV's records constitutes a breach of the Agreement and the WVDMV may terminate the Agreement without consequence to WVDMV on that basis. To complete the Confidentiality Agreement, the Division's Privacy Program must be reviewed by each user. Copies of the Division's Privacy Policy and the Confidentiality Agreement are attached and are made part of this Agreement.

The Vendor hereby agrees that it will only access PII as required to perform its duties under the Agreement. The Vendor understands that it is required to secure the PII that it accesses as part of this Agreement and to ensure that it is not accessed by unauthorized individuals or released to any other persons, companies or entities.

The Vendor agrees to keep all personal and non personal information accessed from testing applicants and WVDMV confidential and protected from intentional and unintentional disclosure;

The Vendor acknowledges that authorized access or transactions provides no right to possession or ownership by the Vendor to the WVDMV's data records or to the records of the testing applicants at any time;

The Vendor shall not access or retain any data submitted by testing applicants or by the WVDMV for any reason other than the information that it is required to retain under this Agreement in its transaction logs;

119

The Vendor will ensure that it does not aggregate information or create any databases to information which it has access, including WVDMV's data and data submitted by testing applicants for the purposes of building comprehensive data records or for any other purpose;

The Vendor will take all reasonable precautions to protect against unauthorized access or release of WVDMV data records, confidential records or confidential information in its custody;

The Vendor will follow the notification requirement if it discovers that information or services provided under this Agreement have been disclosed or are being used in violation of the federal Driver Privacy Protection Act, the West Virginia Records Disclosure Act, the federal Privacy Act of 1974 or any other state or federal laws. The Vendor shall also immediately notify the WVDMV within 24 hours by telephone at 304.558.2723 and by facsimile machine at 304.558.1987 as well as the West Virginia Office of Technology at 304.558.9956 or 877.558.9966 if it discovers that personal information provided under this Agreement have been disclosed or are being used in violation of the Agreement, or state or federal laws;

AGREED:

Kathleen Symstegaard  
Printed Name  
Kathleen Symstegaard  
Signature

Director  
Title  
6/28/18  
Date

## Addendum Acknowledgement Form

### ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: DMV1800000001

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

<input checked="" type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input checked="" type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input checked="" type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input type="checkbox"/> Addendum No. 5	<input type="checkbox"/> Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Veridos America, Inc.  
Company  
Kathleen S. Smitigaard  
Authorized Signature  
6/28/18  
Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

## **Exhibit A: Sample Training Plan**

**VERIDOS**

**IDENTITY SOLUTIONS**

by Giesecke & Devrient  
and Bundesdruckerei

### **STATE of West Virginia (WV) SAMPLE TRAINING PLAN**

## 1. Introduction

### 1.1 Purpose

The purpose of the Training Plan (TP) is to establish

- i) the strategy for training to support the implementation and End User adoption of the Facial Recognition Identity Management Solution
- ii) the approach to be used to equip the Brokers and Service Centre Representatives (SCR), collectively referred to as Operators, and the following group, collectively referred to as Administrators, (Identity Verification Clerks, Facial Recognition Analysts, IV & DI Mgmt, Insurance & Licensing Mgmt, Investigators, Identity Case Administrators, and System Administrators) with the training and knowledge required to perform effectively and efficiently in their assigned roles.
- iii) the methodology that will be employed by EDC to develop and deliver training which meets and/or exceeds the specific needs of each trainee population on the Customer Facial Recognition Identity Management Project.

The TP also serves to guide the management of training, throughout the entire project lifecycle, and ensure that all training needs are addressed through continuous surveillance of the training activities and continuous evaluation of training needs.

### 1.2 Scope

The TP encompasses a number of elements, which are tailored to the specific requirements and needs of the various user groups, organizations, process owners and stakeholders. The TP identifies the major types of training, which will be performed to support operations of the Facial Recognition Identity Management Solution being delivered to Customer. The TP defines the support activities, schedules, curriculum, methods, tools and equipment and facilities required for training. This TP is based on training requirements, Industry and Best Practices related to training.

### 1.3 Assumptions

The following assumptions have been used in producing this document:

1. The following Customer User groups have been identified for training:
  - A. Brokers and Service Centre Representatives – require training in CaptureManager software usage.
  - B. Customer Trainers who will train urban Service Centre Representatives (SCR) on Capture Tower (as required).
  - C. Customer Secura Administrators – This group is subdivided into seven sub-groups with different training needs within the Secura system:
    - Identity Verification Clerks
    - Facial Recognition Analysts
    - IV and DI Management
    - Insurance and Licensing Management
    - Investigators

- » Identity Case Administrators
  - » System Administrators
  - D. New-hire and replacement personnel
2. Each designated Customer training location/site will provide adequate facilities, equipment and support personnel for training to meet requirements and specifications set forth in the TR.
3. Trainees will have the necessary pre-requisite knowledge and skills that serve as a starting point for courses offered as a part of this effort. See Appendix A for Course Descriptions, which include pre-requisite competencies.
4. Trainees will be given adequate time to attend class sessions and schedules will also be altered to reflect a period of reduced work activity as Trainees learn how to put the new training into practice during their daily activities.
5. Trainees' Managers will receive ample notification to schedule staff for training and this will be covered in the training Communications Plan.

## 2. Training Needs Analysis

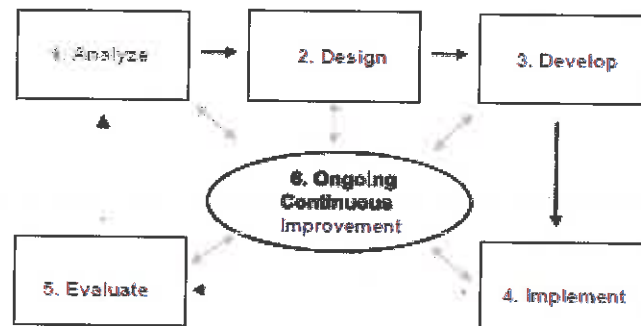
- A GAP analysis of "As Is" and "To Be" states has been undertaken by EDC training staff in the form of discussions between EDC and Customer. This has aided in identifying changes in the Business Processes and Customer/End user and system/application related interactions.
- Training requirements, identified by the needs analysis, are by user groupings in order to address different training needs of each user group.
- Skills and knowledge required for each user grouping to support the new work activities have been identified. These requirements will be matched to the existing personnel skill sets to determine the training needs for each user group.
- Training for Revised Office Procedures – Identification of the training needs has been undertaken to determine the extent of procedural changes that will occur as a result of implementation of the new Facial Recognition Identity Management Solution.

### 3. Training Strategies and Approach

The timing of training for the migration to the new Facial Recognition Identity Management Solution and applications is a critical success factor in ensuring smooth, efficient and seamless delivery of customer service. If done too far in advance of the implementation and migration off the legacy Facial Recognition Identity Management Solution, the effects of "cold storage" breed delays, performance, quality and service issues. If done too late in the process, the migration effort could incur delays, the extent of which, depending on magnitude and its inter-relationship to other variables, can also cause significant costs to be incurred. Our training strategy ensures that audience segments get the appropriate information at the right time, and that messages and information are included that promote and support the desired future state and vision. Once the strategy has been formed, the courses are developed based on specific desired trainee functions and system functionality.

Veridos' approach to training utilizes the Instructional Systems Design (ISD) methodology, which incorporates generally accepted guidelines and practices for developing training programs.

This methodology is divided into six distinct tasks. The six tasks are portrayed in the graphic and described in detail below.



Instructional Systems Design Model

1. **Analysis** - assessing needs, determining the causes of the needs, establishing requirements for outcomes
2. **Design** - identifying the necessary content, establishing objectives and tests, examining the users
3. **Development** - planning the instructional strategies, creating the instruction
4. **Implementation** - operating the education or training program
5. **Evaluation** - determining effectiveness, revising until mastery is achieved
6. **Ongoing Continuous Improvement** - improvement through cycle repetition

## Training Plan Goals

The goal of the TP is to provide a broad framework with which to document the planned structure, task and activities for project related training. Specific goals of the TP are:

- To ensure that each training population's learning needs are fully recognized and addressed
- To ensure that Customer success metrics are incorporated into the training strategy design and curriculum design processes so that progress may be measured quantitatively and reported accurately to relevant stakeholders. Success metrics will be determined based on successful completion of the training for brokers and SCRs and IV&DI's ability to use the software as expected by the end of the ILT training sessions. Veridos will report back to Customer on success metrics related to IV&DI. These will be in the form of student evaluation scores and instructor training summary statement.
- To incorporate lessons learned proactively from previous training efforts and relevant Best Practices. This will help foster end user acceptance and a training friendly environment where end users feel comfortable asking questions to clarify material.
- To document the planned project-related training activities for each Customer training population (brokers/SCRs, Administrators, and Trainers)
- To have a knowledgeable and well trained end user population that is aware of the business reasons and goals for embarking on this project. This population will use the new Capture Manager, Capture Tower and Facial Recognition Identity Management Solution platform effectively and efficiently to support their roles and contribute to the achievement of improved outcomes and enhanced customer service through use of the new Facial Recognition Identity Management Solution platform.

## Implementation Phase:

Training Delivery methods/techniques to be employed during the implementation phase are as follows:

- eLesson provided to brokers and Service Centre Representatives on Capture Manager and photo selection. Content will be provided to the Customer and included in the current LMS delivery system.
- Instructor-Led Training – interactive, hands-on, task-based training conducted on live or simulated workstations. Topics and skills covered in training are derived directly from the results of the needs analysis
  - Train-the-Trainer Training – conducted for the group identified as trainers for the Capture Tower users (operators), as required
  - Secura Administrator Training – conducted for Secura Administrators and FRS Adjudicators, IT, and System Administrators (see 1.3 Assumptions and Appendices A and B).



### Sustainment:

The approach for handing over various ongoing responsibilities for training to the long term business owners encompasses the following:

- E-Learning Online Self-Study – for post-implementation operator training and new users of Capture Manager and/or Capture Tower.
- E-Learning Online Self-Study – EDC to provide e-copy of training presentation materials for Customer to use for the purpose of post implementation training

## 4. Course Development

Courseware is developed to be compliant with the following content development standards.

- The Instructional Systems Design (ISD) methodology, which incorporates generally accepted guidelines and practices for developing training programs.
- Standard Content Objects Reusable Model (SCORM). The E-Learning Online Self-Study training course for operator sustainment training will be created to be SCORM compliant and able to be incorporated into Customer's Learning Management System, if required.

### 4.1 Course Descriptions

Course descriptions are provided for each course and include the following:

- Objectives
- Pre-requisites
- Target audiences
- Description
- Topics
- Duration
- Reference Appendix A for each course's syllabus



## 4.2 Deliverables

### 4.2.1 Train-the-Trainer Operator/User Training (Capture Tower) deliverables include:

- Course Description
- Course Schedule
- Instructor Guide, which includes:
  - Learning Objectives
  - Lessons to support the Learning Objectives
  - Practical exercises
  - Certification requirements (if necessary)
- Training Lab Manual, which includes the objectives, lessons, and exercises

### 4.2.2 Secura Administrator Training deliverables for each affected group based on training needs include:

- Course Description
- Course Schedule
- Instructor Guide, which includes:
  - Learning Objectives
  - Lessons to support the Learning Objectives
  - Practical exercises
- Training Lab Manual, which includes the objectives, lessons, and exercises

### 4.2.3 E-Learning Online Self-Study deliverables include:

- Course Descriptions
- Training Course e-files (will be loaded into Customer LMS system and distributed using usual format and process. For brokers and SCRs, it will be necessary to include existing workflow processes and seamlessly integrate the addition of Capture Manager and/or Capture Tower pieces into the whole.

## 4.3 Quality Assurance

**Quality Criteria** – Accuracy of information and processes presented in training courses is a primary concern when creating new courses. Training is developed and delivered with strict adherence to the following quality criteria:

- Courses are developed to be compliant with course development standards that have been created and maintained by the technical training team

- Course content is reflective of most current released versions hardware, software, and firmware
- For appropriate audiences, ie. Train the Trainer (Capture Tower) and Secura Administrators training is delivered on simulated workstations that are fitted with the most current hardware, software, and firmware versions. Test data for training will be provided by EDC and will meet all requirements set out by the Customer for use (production data will not be used).
- Training manuals and handouts are reviewed internally and by the end-user, if required, to ensure that contents are complete, compliant with customer requirements, and accurate
- Training courses are tested internally and, if required, delivered as pilot courses to the end-user to ensure compliance with customer requirements
- E-Learning courses are created with SCORM compliant development tools, resulting in deliverables that are compatible with Customer's LMS systems

## 5. Course Delivery

### 5.1 Resource Requirements

**Operator Training (TTT) – for Capture Tower** - The successful delivery of this training will depend upon the availability of the following resources:

- **Instructor** – Senior Instructor at Entrust Datacard
- **Student Trainers** – Names to be identified by Customer. As the content of this course is focused on the photo capture subset of the workstation processes, the students must be previously trained or concurrently training on the complete Customer Insurance workstation solution for driver licensing.
- **A functional workstation**, complete with all software and peripheral hardware components (Capture Tower equipment and camera) must be available for use during this Capture Tower training. A preferred maximum student/workstation ratio is 3:1.
- **Tools** – Any tools identified as required to conduct this training must be available at the time and location of the training. A complete set of identified tools must be available for each workstation setup in the training facility.
- **Training facility** – A suitable location to conduct this training must be identified. Facility requirements are specified in the next section (5.2).

**Secura Administrator Training (Secura, FRS)** – The successful delivery of this training will depend upon the availability of the following resources:

- **Instructor** – Senior Instructor at Entrust Datacard
- **Students** – Names to be identified by Customer. As the content of this course is focused on the administration of the Secura software and the Facial Recognition Software, the students must be previously trained or concurrently training on the complete Customer Driver's License solution.
- **Suitably loaded simulators** (laptops with appropriate versions of Secura software and FRS as well as VVI images) must be available for use during this training. Student/workstation ratio is 1:1. These laptops will be provided by EDC.
- **Training facility** – A suitable location to conduct this training must be identified. Facility requirements are specified in the next section (5.2).



## 5.2 Locations and Facilities

**Operator Training (TTT)** – training of Capture Tower. Delivery of this training will require a facility that meets the following requirements:

- Location of this training to be provided by Customer.
- Classroom, conference room, or other space large enough to accommodate # of students. Driver's License workstations (including PC, Monitor, Camera, backdrops, etc.).
- Training room must be fitted with projection equipment, writing board(s), and marking pens.
- Training room must include tables and chairs to accommodate all students, instructor, and workstations.
- Training room must have suitable power outlets or power strips to accommodate all workstation equipment.

**Secura Administrator Training (Secura, FRS)** – Delivery of this training will require a facility that meets the following requirements:

- Location of this training to be provided by Customer.
- Classroom, conference room, or other space large enough to accommodate four students at a time. Veridos to supply preloaded laptops with necessary software, data and other materials.
- Training room must be fitted with projection equipment, writing board(s), and marking pens.
- Training room must include tables and chairs to accommodate all students, instructor, and any required equipment.
- Training room must have suitable power outlets or power strips to accommodate all equipment.

### 5.3 Administration

For each course delivered:

- Classroom setup should occur at least one business day prior to the class start to ensure that all requirements are met and equipment is fully functional.
- EDC will reproduce all required training materials (lab manuals, handouts, etc.) and ship or carry these materials to the training site to be available by, or before, the start of training.
- EDC will enroll students into the EDC LMS for ECD record keeping purposes. Enrollment data (student names, course names, dates, and completion status) will be shared with Customer.
- Instructors will capture the names of each student in each class and submit statements of attendance and completion to the EDC Training Administrator for attendance and completion reporting. This information will also be communicated to Customer Training Admin Staff as a simple spreadsheet of names/course/dates/completion.
- Training courses will not include certification testing, but each student will be expected to demonstrate completion and competency for all defined training course objectives by successful completion of all training and demonstration of proper use of the system once operational.
- Customer will reserve the training facilities to be dedicated to the training courses for on the dates and times as agreed.
- Security issues – Security clearances and site access requirements must be defined and administered by Customer prior to the training date(s). Students and instructor must have access to buildings and training rooms for the duration of the training course events.

## 5.4 Quality Assurance

To ensure that the instructor-led training courses meet or exceed the expectations of Customer, the following activities can be administered as needed:

- Training course materials can be reviewed in advance of commencement of the training to ensure that the course content is complete and accurate. If this is required, it must be conducted 3+ weeks prior to the training in order to allow time for corrections or additions to the course content
- A course evaluation survey will be conducted by the EDC trainer at the end of each course. The evaluation measures instructor effectiveness, course content, course administration, facility suitability, overall rating for the course, and ample opportunity for comments
- Student skills are not measured or tested. Instructors will observe performance, expect participation, and expect completion of all course objectives. Post-training interviews with management to discuss individual performance criteria can be arranged if required
- The e-Learning course content will be incorporated into the Customer training model. Measurement of training effectiveness will be at the discretion of Customer training staff

## 6. Course Schedules

Training schedules will include the following information:

- Course identification (Name and Course ID#, if any) of each course to be delivered
- Planned training dates
- Start/stop times for each course
- Pre-training setup dates/times
- Post-training debrief/reporting with Customer management, if required
- Names of students for each class delivered
- Names of instructor(s) for each class delivered
- Location of each class delivered

## 7. Contact Information

The following provides a sample list of the points of organizational contact (POCs) that may be needed by the TP users for informational and troubleshooting purposes.

Type of Contact	Contact Name	Organization	Telephone	Email
Project Management				
Project Management				
Program Management				
Technical Training Supervisor				
Knowledge Management				
Knowledge Management				

## 8. Appendices

### Appendix A Course Descriptions

#### Capture Manager Training for Brokers and Service Centre Representatives

##### Course Description:

This course will provide the students with detailed instruction on how to use Capture Manager to capture and choose suitable ICAO compliant photos for enrolment using the IWS workstation containing Capture Manager software.

##### Course Benefits:

- Enrolment time and errors will be minimized as enrolment personnel have greater knowledge of workstation features.
- Employee morale and retention will increase as they feel you are making an investment in their career development.
- Fewer customer photo retakes will be needed improving customer service levels.

#### Capture Tower Training

##### Course Description:

This training course will provide students with the fundamental skills necessary to install and setup the Capture Tower. The course will also provide the students with instructional materials to be used as post-training reference material.

##### Course Benefits:

- Enrolment time and errors will be minimized as enrolment personnel have greater knowledge of workstation features.
- Employee morale and retention will increase as they feel you are making an investment in their career development.
- Fewer customer photo retakes will be needed improving customer service levels.

Intended Audience	Designated Customer training staff who are responsible for installing and maintaining the Image Capture Tower
Course Length	1 hour
Delivery Location	Facility location to be specified by Customer
Prerequisites	Experience with current Insurance Work Station Driver's License Enrolment workflows
Recommended Skill Set	Must have a general understanding of personal computers and Microsoft Windows 7 workstation operations
Class Size	NA
Major Topics/Activities	Installation Setup Cleaning
Certification	None

## Secura Administration / FRS Training

DATACARD® SECURA™  
ADMINISTRATION / FRS TRAINING

**Achieve maximum efficiency and uptime through administrator training.**

Whether you are creating new setups regularly or occasionally modifying existing setups, having well trained and certified administrators will lead to greater efficiency and less frustrations in your credential enrollment operation.

## Course Description:

This training course will provide students with the fundamental skills necessary to perform administrative activities on the Datacard® Secura™ Credential Lifecycle Management software.

## Course Benefits:

- Administrators will feel more confident and comfortable creating setups for the Secura software.
- Enrollment efficiency may increase as your administrators understand how to use available features of the Secura software.
- As administrators better understand how the Secura software functions, they assume a stronger ownership in the quality of their work.
- Employee morale and retention will increase as they feel you are making an investment in their career development.

Intended Audience	Identity Verification Clients, Facial Recognition Analysts, IV & DL Mgmt, Insurance & Licensing Mgmt, Investigators, Identity Case Administrators, and System Administrators
Course Length	2 days - only those requiring working on specific tasks will be present for those tasks during the 2 days.
Delivery Location	Facility location to be specified by Customer
Prerequisites	Experience with current Driver's License Enrollment Workstation workbooks
Recommended Skill Set	All participants should have a general understanding of personal computers and Microsoft Windows / Workstation operations.
Class Size	The maximum class size is 16 students.
Major Topics/Activities	<ul style="list-style-type: none"> <li>• The training includes the following modules/topics: <ul style="list-style-type: none"> <li>• Secura Administration Level One (Lead Selection and Adjustment) / Identity Verification Client</li> <li>• Special Handling / Facial Recognition Analyst</li> <li>• Secura Adjustment Level Two / Facial Recognition Analyst</li> <li>• Records Modules / Facial Recognition Analyst, IV &amp; DL Mgmt, Insurance &amp; Licensing Mgmt</li> <li>• Exceptions Report / Facial Recognition Analyst</li> <li>• Transaction Summary Report / IV &amp; DL Mgmt, Insurance &amp; Licensing Mgmt</li> <li>• User Activity Report / IV &amp; DL Mgmt, Insurance &amp; Licensing Mgmt</li> <li>• Transaction Detail Report / IV &amp; DL Mgmt, Insurance &amp; Licensing Mgmt</li> <li>• Capture Manager Photo Correction / Facial Recognition Analyst</li> <li>• Cognifit FaceLink3G Manual Enrollment / Facial Recognition Analyst</li> <li>• Photo Submission (Application) / Facial Recognition Analyst</li> <li>• Search Module / Investigator, Identity Case Administrator, Facial Recognition Analyst</li> <li>• Lead Review / Investigator, Identity Case Administrator</li> <li>• Clearing Further Investigation / Investigator, Identity Case Administrator</li> <li>• Secura Users and Roles / System Administrator</li> <li>• System Administration / System Administrator</li> <li>• Capture Manager Licensing / System Administrator</li> <li>• License Manager Licensing / System Administrator</li> </ul> </li> </ul>
Certification	None

## E-Learning Online Self-Study Training

**IMAGE CAPTURE SELF-STUDY  
OPERATOR TRAINING***Achieve maximum enrolment efficiency through operator training.**Whether you are experiencing frequent turnover of personnel or adding additional enrolment locations having well trained and certified enrolment personnel will lead to greater efficiency in your credential enrolment process.***Course Description:***This training course will provide students with the fundamental skills necessary to perform image capture operational tasks on the Image Capture workstations.***Course Benefits:**

- Enrolment time and errors will be minimized as enrolment personnel have greater knowledge of workstation features.
- Employee morale and retention will increase as they feel you are making an investment in their career development.

Intended Audience	Brown and SOCs who will operate the Capture Towers and Image Capture Workstations.
Course Length	Self-paced self study
Delivery Location	Online
Prerequisite	None
Recommended Skill Set	Must have a general understanding of personal computers and Microsoft Windows 7 operations...
Class Size	N/A
Major Topics/Activities	Image Capture Capture Errors ICAO Compliance Errors Camera environment set up
Certification	None

## Appendix B Training Audience Groups and Content Deliverables

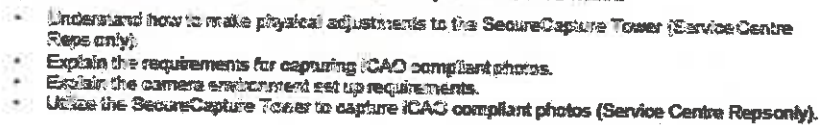
### Training Groups

Source: EDC & MPI Training Docs



Extract Original  
2015 Nov 13

As the roles relate to EDC training, Insurance Brokers and Service Centre Representatives will utilize the SecureCapture Tower (Service Centre Reps only) and Capture Manager software application to capture ICAO compliant identity photos.



Recommended EDC Secura Training for Insurance Broker and Service Centre Representatives

**EDC Capture Manager Training Course Developed for Customer**

**Lesson – The Secure Capture Tower (only for six pilot service centres)**

Student Learning Outcomes:

- Describe the purpose of the SecureCapture Tower
- Operate the SecureCapture Tower and photo capture equipment
- Troubleshoot SecureCapture Tower issues

**Lesson – ISO/IEC Image Capture Requirements and Best Practice Recommendations**

Student Learning Outcomes:

- Note: This is a foundational knowledge-based activity with no tasks, skills, or exercises
- Identify the ISO/IEC 19794-5 Standard image capture requirements and best practices
- Utilizing the ISO/IEC 19794 Standard, identify ISO/IEC compliant and noncompliant images

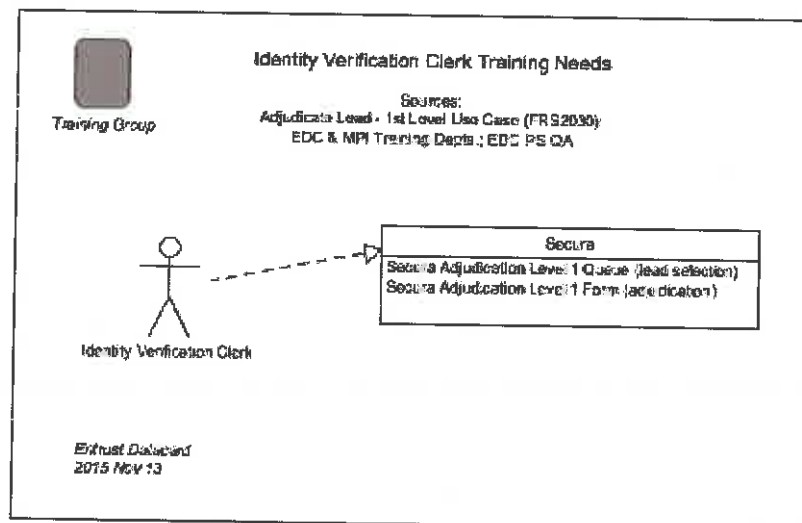
**Lesson – Utilize the Customer Customized Capture Manager Application to Capture Images**

Student Learning Outcomes:

- Capture portrait and signature images utilizing the Capture Manager application.
- Determine if the captured images are ISO/IEC 19794-5 Standard compliant.
- Identify issues causing noncompliance of captured images and take necessary actions to achieve image compliance.
- Identify adjustments that may be required to the camera environment set up to achieve image compliance.

**Role: Identity Verification Clerk****Role of Identity Verification Clerks**

Adjudication leads are generated due to mismatches between customer photos and customer numbers. When an identity is rejected in the Special Handling process it is the role of the Identity Verification Clerks to examine and approve the photo of record for a customer's identity or escalate the lead for further adjudication by a trained facial recognition analyst. Adjudication Level 1 utilizes a two-person-verification agreement process.

**The Identity Verification Clerk must:**

- Understand the lead generation process.
- Be proficient in utilizing the Secura application, Adjudication Level user interface tools for the purpose of acceptance of identities and determining lead escalations.
- Understand the Adjudication Level 1 form and form utilities.

## Recommended EDC Secura Training for Identity Verification Clerks

### EDC Secura Training Course Developed for Customer

#### Lesson – Overview of the Secura System

##### Student Learning Outcomes:

- Describe how Secura identification software is used.
- Identify the unique Secura workflows.
- Describe how Secura manages credentials.
- Describe the Secura enrollment and data capture process.

#### Lesson – Principles of Facial Recognition

##### Student Learning Outcomes:

- Define how in digital photography, pixels are represented by gray scale values.
- Describe how pixel gray scale values can be utilized to identify facial features.
- Describe how separate facial images can be matched electronically.
- Define FIR.
- Differentiate 1:N, 1:R and 1:1 image comparison.

#### Lesson – The Home Tab Operations

##### Student Learning Outcomes:

- Sign in and sign out of the Secura application.
- Identify the individual Secura Main Menu tabs.
- Perform Application searches utilizing the Application Status search utilities.
- Identify the application enrollee information.
- Perform information sorting.

#### Lesson – Special Handling Operations

##### Student Learning Outcomes:

- Describe why enrollments are moved to the Special Handling queue.
- Identify the two outcomes of Special Handling.
- Perform searches utilizing the Special Handling search utilities.
- Utilize the Special Handling form and form functions to vet applications.
- Utilize the Special Handling form Correct Photo utility to perform corrections to non ICAD compliant photos.

#### Lesson – Adjudication Level 1 Operations

##### Student Learning Outcomes:

- Describe why an adjudication lead is created.
- Define the role of the Adjudication Level 1 clerk.
- Describe why leads appear in the Adjudication Level 1 queue.
- Define Reason Code.
- Identify the Adjudication Level 1 form and form utilities.
- Utilize the Adjudication Level 1 form utilities to approve or escalate a lead.

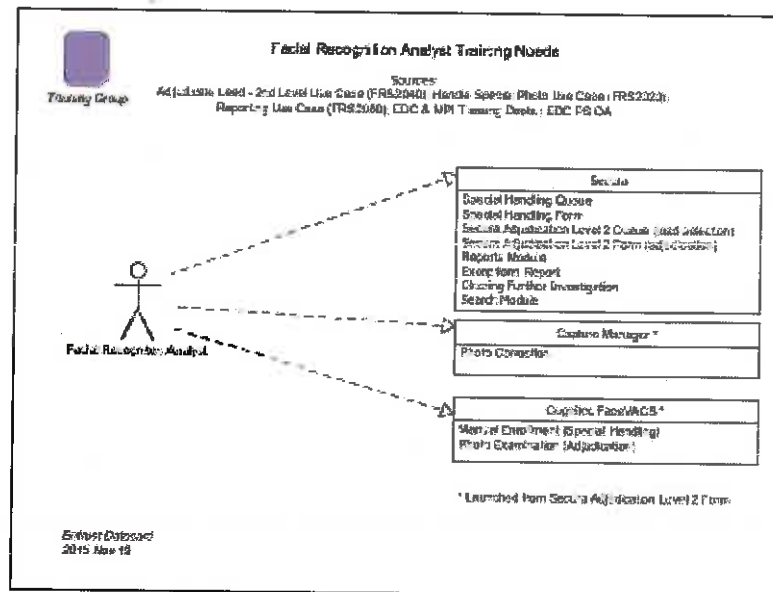
### Training Methods

The EDC, Secura application training for Identity Verification Clerks utilizes:

- Presentation of information related to the Capture Manager and Secura application processes and graphical user interfaces.
- Instructor-led hands-on practice utilizing the Capture Manager and Secura application processes and graphical user interfaces.
- Student proof of learning exercises to determine student understanding.

**Role: Facial Recognition Analysts****Role of Facial Recognition Analysts**

When one or both Identity Verification Clerks escalate a lead, it is the responsibility of the facial recognition analyst to examine and approve the photo of record for a customer's identity or escalate the lead for further investigation.



The Facial Recognition Analyst must:

- Understand the lead generation process.
- Determine if photos that have failed compliance failed because of poor photo quality due to equipment or photographer workmanship or because of an attribute of the photo subject that prevents ICAO compliance (patch, facial art, etc.).
- Determine if photos require retakes or if the photo may be corrected.
- Utilize the Capture Manager tools to correct photos.
- Be proficient in utilizing the Secura application, Adjudication Level 2 and Cognifit FaceVACS DBScan and Examiner tools for the purpose of identity acceptance or investigation.
- Understand the Adjudication Level 2 form and form utilities.

## Recommended EDC Secura Training for Facial Recognition Analysts

### EDC Secura Training Course Developed for Customer

#### Lesson – Overview of the Secura System

##### Student Learning Outcomes:

- Describe how Secura identification software is used.
- Identify the unique Secura workflows.
- Describe how Secura manages credentials.
- Describe the Secura enrollment and data capture process.

#### Lesson – Principles of Facial Recognition

##### Student Learning Outcomes:

- Define how in digital photography, pixels are represented by gray scale values.
- Describe how pixel gray scale values can be utilized to identify facial features.
- Describe how separate facial images can be matched electronically.
- Define FIR.
- Differentiate 1:N, 1:R and 1:1 image comparison.

#### Lesson – The Home Tab Operations

##### Student Learning Outcomes:

- Sign in and sign out of the Secura application.
- Identify the individual Secura Main Menu tabs.
- Perform Application searches utilizing the Application Status search utilities.
- Identify the application enrollee information.
- Perform information sorting.

#### Lesson – Special Handling Operations

##### Student Learning Outcomes:

- Describe why enrollments are moved to the Special Handling queue.
- Identify the two outcomes of Special Handling.
- Perform searches utilizing the Special Handling search utilities.
- Utilize the Special Handling form and form functions to vet applications.
- Utilize the Special Handling form Correct Photo utility to perform corrections to non ICAO compliant photos.

#### Lesson – Adjudication Level 1 Operations

##### Student Learning Outcomes:

- Describe why an adjudication lead is created.

- Define the role of the Adjudication Level 1 clerk.
- Describe why leads appear in the Adjudication Level 1 queue.
- Define Reason Code.
- Identify the Adjudication Level 1 form and form utilities.
- Utilize the Adjudication Level 1 form utilities to approve or escalate a lead.

#### Lesson – Adjudication Level 2 Operations

##### Student Learning Outcomes:

- Define the role of the Adjudication Level 2 clerk.
- Describe why a lead moves to the Adjudication Level 2 queue.
- Identify the Adjudication Level 2 form and form utilities.
- Utilize the Adjudication Level 2 form utilities to approve a lead or to escalate the lead for further investigation.
- Identify FaceVACS Examiner tools utilized by the Facial Recognition Analyst to examine photos.

#### Lesson – Cognitec Examiner

##### Student Learning Outcomes:

- Create, load and view cases
- Add subjects and probes to the investigation case
- Utilize the Enhance, Annotate and identify utilities
- Utilize the Inspection Window utilities to examine subject and probes
- Utilize the Filter enhancement tools to enhance images

#### Lesson – Reports

##### Student Learning Outcomes:

- Query reports by report type.
- Describe information that can be included in reports.
- Perform report query filter operations.
- View, export and print reports.

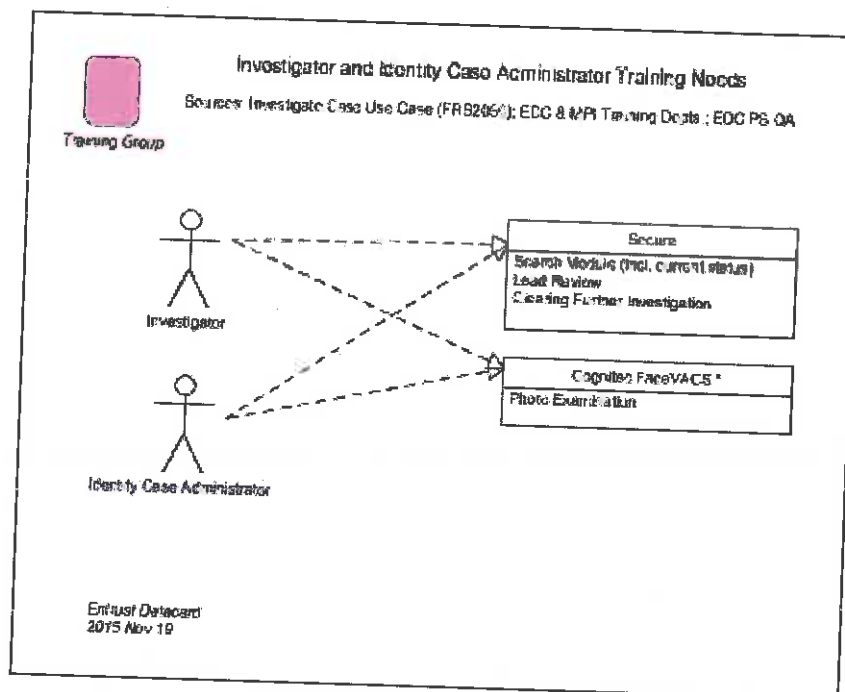
#### Training Methods

The EDC, Secura application training for Facial Recognition Analysts utilizes:

- Presentation of information related to the Capture Manager, Secura and Cognitec application processes and graphical user interfaces.
- Instructor-led hands-on practice utilizing the Capture Manager, Secura and Cognitec applications and graphical user interfaces.
- Student proof of learning exercises to determine students' understanding.

**Role: Identity Case Administrators & Investigators****Role of Identity Case Administrator & Investigators**

When the Facial Recognition Analyst recommends a case for further investigation it is the responsibility of the Identity Case Administrator and Investigators to make the final determination for acceptance or rejection of the identity.



The Identity Case Administrator and Investigators must:

- Understand the lead generation process.
- Be proficient in utilizing the Capture Manager application, Secura application, Adjudication Level 2 and Cognitec FaceVACS DBScan and Examiner tools for the purpose of identity acceptance or rejection.
- Understand the Search form and form utilities.

**Recommended EDC Secura Training for Identity Case Administrators**

**EDC Secura Training Course Developed for Customer**

**Lesson – Overview of the Secura System**

**Student Learning Outcomes:**

- Describe how Secura identification software is used.
- Identify the unique Secura workflows.
- Describe how Secura manages credentials.
- Describe the Secura enrollment and data capture process.

**Lesson – Principles of Facial Recognition**

**Student Learning Outcomes:**

- Define how in digital photography, pixels are represented by gray scale values.
- Describe how pixel gray scale values can be utilized to identify facial features.
- Describe how separate facial images can be matched electronically.
- Define FIR.
- Differentiate 1:N, 1:R and 1:1 image comparison.

**Lesson – The Home Tab Operations**

**Student Learning Outcomes:**

- Sign in and sign out of the Secura application.
- Identify the individual Secura Main Menu tabs.
- Perform Application searches utilizing the Application Status search utilities.
- Identify the application enrollee information.
- Perform information sorting.

**Lesson – Special Handling Operations**

**Student Learning Outcomes:**

- Describe why enrollments are moved to the Special Handling queue.
- Identify the two outcomes of Special Handling.
- Perform searches utilizing the Special Handling search utilities.
- Utilize the Special Handling form and form functions to vet applications.
- Utilize the Special Handling form Correct Photo utility to perform corrections to non ICAO compliant photos.

**Lesson – Adjudication Level 1 Operations**

**Student Learning Outcomes:**

- Describe why an adjudication lead is created.



- Define the role of the Adjudication Level 1 clerk.
- Describe why leads appear in the Adjudication Level 1 queue.
- Define Reason Code.
- Identify the Adjudication Level 1 form and form utilities.
- Utilize the Adjudication Level 1 form utilities to approve or escalate a lead.

#### **Lesson – Adjudication Level 2 Operations**

##### **Student Learning Outcomes:**

- Define the role of the Adjudication Level 2 clerk.
- Describe why a lead moves to the Adjudication Level 2 queue.
- Identify the Adjudication Level 2 form and form utilities.
- Utilize the Adjudication Level 2 form utilities to approve a lead or to escalate the lead for further investigation.
- Identify FaceVACS Examiner tools utilized by the Facial Recognition Analyst to examine photos.

#### **Lesson – Cognitec Examiner**

##### **Student Learning Outcomes:**

- Create, load and view cases
- Add subjects and probes to the investigation case
- Utilize the Enhance, Annotate and identify utilities
- Utilize the Inspection Window utilities to examine subject and probes
- Utilize the Filter enhancement tools to enhance images

#### **Lesson – Reports**

##### **Student Learning Outcomes:**

- Query reports by report type.
- Describe information that can be included in reports.
- Perform report query filter operations.
- View, export and print reports.

#### **Lesson – The Search Operations**

##### **Student Learning Outcomes**

- Define the role of the Identity Case Administrator.
- Utilize the Search page, Search utilities to perform applicant searches.
- Identify Potential Fraud records.
- Identify the Search form and form utilities.
- Utilize the Search form utilities.
- Clear the Investigation.
- Verify the case is approved.

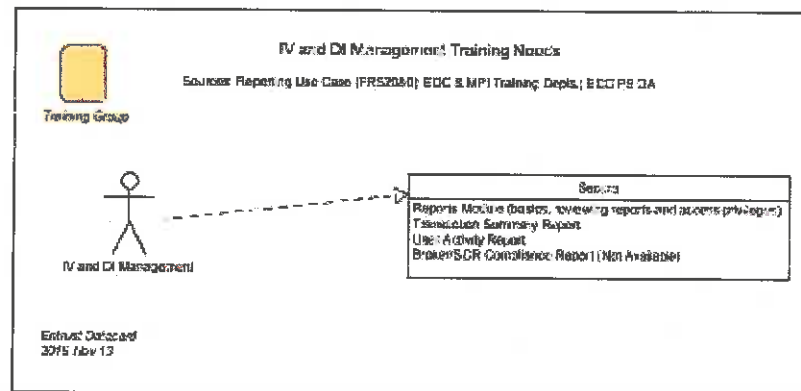
## Training Methods

The EDC, Secura application training for Identity Case Administrators utilizes:

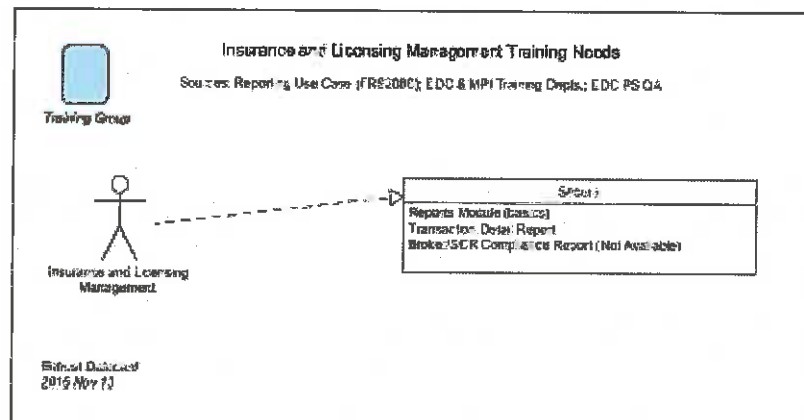
- Presentation of information related to the Capture Manager, Secura and Cognitec application processes and graphical user interfaces.
- Instructor-led hands-on practice utilizing the Capture Manager, Secura and Cognitec applications and graphical user interfaces.
- Student proof of learning exercises to determine students' understanding.

**Roles:****IV and DI Management****Insurance and Licensing Management****Role of IV and DI Management**

IV and DI Management utilize the Secura application software to generate reports, view users and roles and engage in audit activities.

**Role of Insurance and Licensing Management**

Insurance and Licensing Management utilize the Secura application software to generate reports.



IV and DI Management must:

- Understand the Secura application software Reports and Users and Roles tabs functions.

Insurance and Licensing Management must:

- Understand the Secura application software Reports tab.

**Recommended EDC Secura Training for IV and DI Management and Insurance and Licensing Management**

**EDC Secura Training Course Developed for Customer**

**Lesson – Reports**

**Student Learning Outcomes:**

- Query reports by report type.
- Describe information that can be included in reports.
- Perform report query filter operations.

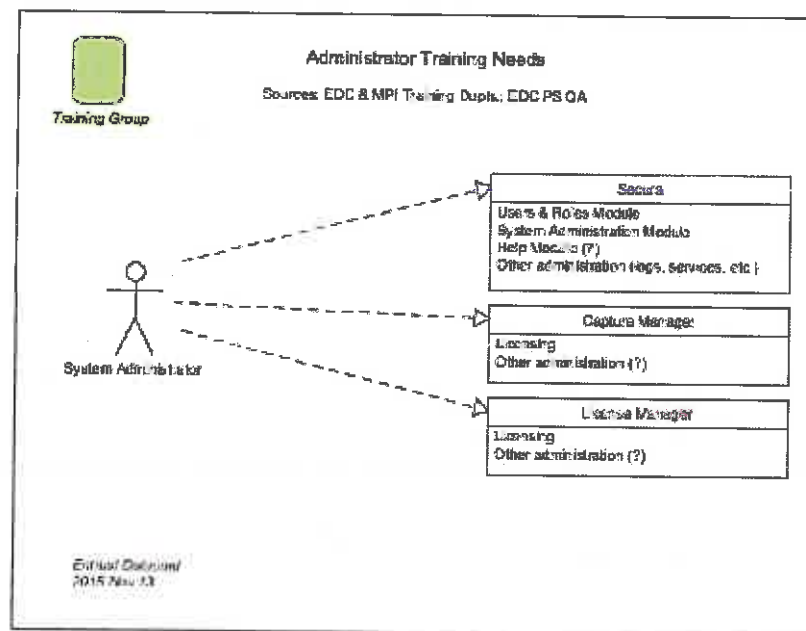
**Lesson – Users and Roles**

**Student Learning Outcomes:**

- Utilize the Users tab functions to: import users; export users; update a user and delete a user.
- Utilize the Roles tab functions to: add a role; export a role; update a role; delete a role and add user(s) to a role.

**Role: Administrator****Role of Administrator**

The Administrator manages user access to the system and system user privileges, and performs system maintenance tasks related to licenses, system logs, process and services. In addition, the Administrator - working with EDC technical support and engineering - installs software upgrades and troubleshoots and resolves system issues.

**The Administrator must:**

- Utilize the functions of the Secura application software's: Reports, Users and Roles, and System Administration modules.
- Perform system maintenance tasks related to licenses, system logs, and process and services.
- Work with EDC technical support and engineering to troubleshoot and resolve system issues.
- Install software revisions and upgrades.

## **Recommended EDC Secura Training for Administrators**

### **EDC Secura Training Course Developed for Customer**

#### **Lesson – Reports**

##### **Student Learning Outcomes:**

- Query reports by report type.
- Describe information that can be included in reports.
- Perform report query filter operations.

#### **Lesson – Users and Roles**

##### **Student Learning Outcomes:**

- Utilize the Users tab functions to: import users; export users; update a user and delete a user.
- Utilize the Roles tab functions to: add a role; export a role; update a role; delete a role and add user(s) to a role.

#### **Lesson – System Administration**

##### **Student Learning Outcomes:**

- Interpret problem descriptions in the Problem Applications table.
- Utilize the Restart function to restart failed processes.
- Generate audit reports utilizing the Audit functionality.

## Exhibit B: Sample Test Documentation



### XX Project Test Plan

Authorized for issue by:

Customer Project Manager

Signature

Date

Veridos Project Manager

Signature

Date

Date Here

**CONFIDENTIAL**

State of West Virginia  
RFP to Provide Driver's License and ID Cards

Page 303 / 340

**VERIDOS**



**IDENTITY SOLUTIONS**

by Gleescke+Devrient  
and Bundesdruckerei

**VERIDOS**

**IDENTITY SOLUTIONS**  
by Gleescke+Devrient  
and Bundesdruckerei

### Revision History

Version	Date	Author	Summary of Changes

## Table of Contents

1.	Introduction .....	3
1.1	Purpose .....	4
1.2	Scope and Objectives .....	4
1.3	Definitions and Acronyms .....	5
1.4	Issues, Risks, and Assumptions .....	5
1.5	Related Documents .....	5
2.	Items to Be Tested .....	8
3.	Features to Be Tested .....	6
4.	Features Not to Be Tested .....	7
5.	Test Preparation .....	7
5.1	Overall Approach to Testing .....	7
5.2	Test Specifications .....	8
5.3	Order of Test Execution .....	10
5.4	Test Documents .....	10
5.5	Reviews .....	12
6.	Recording of Test Results .....	12
7.	Correction of Faults .....	13
8.	Archiving .....	14
9.	Test Summary Report .....	14
10.	Entry Criteria .....	14
11.	Item Pass/Fail Criteria .....	15
12.	Exit Criteria .....	16
13.	Test Suspension and Resumption Criteria .....	16
14.	Environmental .....	17
15.	Responsibilities .....	17
15.1	General Roles .....	18
15.2	Specific Responsibilities .....	18
16.	Testing Tasks and Schedules .....	18
17.	Additional Sections .....	19

## 1. Introduction

Describe the specific purpose of the plan, the scope and objectives of the tests, definitions, and related documents.

For a particular project there may be a number of test stages, with each test stage dealing with a different level or facet of the product, e.g. unit/module, integration, system, acceptance tests. The description and scope of these test stages should be covered in a Test Strategy Plan for the project.

Each of these test stages will have a documented Test Plan like this. The test plan formally documents the scope, approach, resources, criteria, and schedules of the testing activities for a particular test stage. It also identifies the test items, the features to be tested, the testing tasks, testing responsibilities, and any risks requiring contingency planning.

### 1.1 Purpose

Delineate the specific purpose of this plan.

#### *Integration Test Example*

Integration Testing tests the interface between units, verifies that data is passed and transformed correctly and that there are no side effects.

This Integration Test Plan is being written to:

- Define the integration testing process to be followed
- Identify human, hardware, data and software resources required
- Present a high-level schedule for Integration Test designing, preparation and execution
- Determine responsibilities and ownership of activities and deliverables involved with Integration Testing

### 1.2 Scope and Objectives

Describe the specific scope and objectives of the tests covered by the plan. A statement should be included on the principles of dealing with the introduction, if at all, of new versions of software during testing.

#### *Integration Test Example*

This Test Plan covers all integration testing activities as defined in the Test Strategy Plan.

- Identifies tests to reveal any defects in the way components of the system are integrated
- Describes processes to resolve any defects found

#### *System Test Example*

Objectives:

- » To detail the necessary activities to prepare for and to conduct the tests
- » To assign to all responsible persons, departments and organization the tasks which they are to perform with respect to system testing
- » To plan a schedule to be followed in the performance of system testing tasks
- To define the sources of information used to prepare the plan and design the tests
- » To define the tools and environment needed to conduct the system tests
- » To identify test specification documents and test reporting documents and forms relating to system tests
- To describe defect reporting procedures and defect correction procedures.

#### Scope

- This test plan covers a full systems test of the <System>. It includes:
  - Multiprogramming functionality
  - Job control
  - Operator and user procedures
  - User documentation
  - GUI usability
  - Security
  - Recovery
  - Performance

### 1.3 Definitions and Acronyms

Define or provide a reference to the definition of all terms, acronyms, and notations required to properly interpret this plan.

### 1.4 Issues, Risks and Assumptions

State the issues, risks, and major assumptions associated with the plan. For any issue/risk provide the details of the contingency/mitigation plans to reduce the likelihood and impact of such issues and risks.

### 1.5 Related Documents

List all documents that were used in the production of the test plan and/or tests. This information includes:

- A complete list of all documents used
- Each document by title, report number, if applicable, date, and publishing organization
- » The sources from which the referenced documents can be obtained

- Its relationship to the test plan and/or tests

## 2. Items to Be Tested

Identify the software or hardware items that are to be tested. For each item identified the following information should be provided:

- Item Identifier
- Name and brief description
- Version to be tested

Significant items that are to be excluded from testing should also be identified.

### Integration Test Example

The integration of units that make up the «Project Name» system will be tested.

Integration testing tests the interface between units, verifies that data is passed and transformed correctly and that there are no side effects.

### Test Items

For this integration test, each integration baseline is considered a Test Item. The meaning of the term "baseline" as it is applied to integration testing is described in Section 5.1.

Item Identifier	Description	Comment
Baseline 0	Unit 1	
Baseline 1	Unit 2	
Baseline 2	Baseline 0 + Unit 3	
Baseline 3 ...	Baseline 1 + Unit 4	
Baseline n		

## 3. Features to Be Tested

Identify all the software/hardware features and combination of features to be tested. For each feature include a reference to the sections of the base document where the requirements for the feature were defined, e.g. Requirements Definition, Functional Specification, Detail Design, Program Specification.

### Integration Test Example

Each Baseline is a test item. For each test item, features to be tested are listed. For this integration test, "features" are the details of the interface between units.

Test Item	Feature Description	Reference
Baseline 0	Nothing to test	
Baseline 1	Nothing to test	
Baseline 2	1. <Feature>	
	2. <Feature> ...	
	n. <Feature>	
Baseline 3 ...	1. <Feature>	
	2. <Feature> ...	
	n. <Feature>	
Baseline n	1. <Feature>	
	2. <Feature> ...	
	n. <Feature>	

#### 4. Features Not to Be Tested

Identify all features and significant combination of features that will not be tested and the reasons for their exclusion.

##### Integration Test Example

The following items or features will not be tested:

- Baseline 0 and Baseline 1

Not tested here because they serve as starting points with no interface. The units represented by these baselines have been tested in the Unit Tests.

- » Communications Network

Will not be tested during the integration testing phase, but will be tested during Acceptance Testing.

#### 5. Test Preparation

Describe the overall approach to the testing; test specifications and order of execution; test documentation; and the reviews required.

##### 5.1 Overall Approach to Testing

Describe the overall approach to testing covered by the plan.

*Integration Test Example*

- Integration Testing tests the interface between units, verifies that data is passed and transformed correctly and that there are no side effects.
- A scaffolding of stubs, drivers, and a test database will be constructed to represent the system and enable testing. As a unit is transmitted to Integration Testing, it will be scheduled to replace its associated stub.
- Only one unit at a time will be inserted into the scaffolding for testing. The state of the system will be saved, documented, and labeled with a "baseline" number that will be incremented with each insertion.
- If errors are found, regression testing will be conducted, first on the unit, then on the baseline where the errors were found.
- Every effort will be made to schedule several baselines to be tested separately but in parallel.

## 5.2 Test Specifications

Describe what test specifications, i.e. test design specifications, test cases, test procedure specifications will be used for testing. This includes a description of the purpose of each type of test specification and how it should be used. The format and content of test specifications is given in the Test Documentation Plan. A brief description of any rules or standard for the creation of test data should be given here.

For a particular test plan, the actual test specifications used for the tests should be given either as appendices or as separate but attached document.

A list is given which traces each test design and/or test case to a particular feature given in section 3 of the plan.

*Integration Test Example*

Test Specifications will be covered by three document types:

**NOTE:** The examples in this document are assigned unique document ID's as a way of associating the related documents.

- Integration Test Design Specifications (TDSxx) is a single document that will contain all the Test Design Specifications for Integration Testing.
- A Test Design Specifications document refines the test approach and identifies the features to be covered by the design and its associated tests. It also identifies the test cases and test procedures, if any, required to accomplish the testing and specifies the feature pass/fail criteria.
- This plan calls for the following Test Design Specifications to be included in the document TDSxx.

Test Design Specification ID	Description	Feature Reference
TDSxx/001	<Name or Description>	Baseline 3 Features 1, 2 & 3
TDSxx/002	<Name or Description>	Baseline 3 Feature 4
<Test Design ID>	<Name or Description>	
<Test Design ID>	<Name or Description>	

- Integration Test Case Specifications (TCSxx) is a single document containing all the Test Cases used during Integration Testing.

A Test-Case Specification document specifies the actual values used for input, along with the anticipated outputs and environmental conditions and any constraints.

Because the necessary Test Cases cannot be known until a Test is designed, specific Test Case Specifications are not listed in this Test Plan. Specific Test Cases will be called for in the Test Design Specification and specified (detailed) in the Integration Test Case Specifications Document (TCSxx).

Test Case Specifications within this document will be identified by the Document ID followed by a sequential number identifying the Test Case Specification.

Example: TCSxx/003 for Integration Test Case 003.

Integration Test Procedure Specifications (TPSxx) is a single document that contains all the Test Procedures used during Integration Testing

A Test Procedure Specification identifies all steps required to operate the system and exercise the specified test cases in order to implement the associated test design.

Because the necessary Test Procedures cannot be known until the Test is designed and Test Cases are specified, specific Test Procedures are not listed in this plan. Specific Test Procedures will be called for in the appropriate Test Design Specification, cross-referenced in the associated Test Case Specification(s) and specified (detailed) in the Integration Test Procedure Specifications (TPSxx)

Test Procedure Specifications within this document will be identified by the Document ID followed by a sequential number identifying the Test Procedure Specification.

Example: TPSxx/003 for Integration Test Procedure 003.

### 5.3 Order of Test Execution

Identify the order of test execution. This should be in the form of a list of actual test cases, possibly grouped by test design. If parallel activities take place then this should be indicated. Ideally this list should also be grouped as daily test execution lists.

If this list is large then it should be given as an appendix or as a separate document with a reference to that document given here. The other document should be attached to the Test Plan.

*Integration Test Example*

Task Number	Test Procedure	Prerequisite Task Numbers
1	TPSxx/001	
2	TPSxx/002	
3	TPSxx/005	1
4	TPSxx/003	2
5	TPSxx/009	3
6	TPSxx/007	4
7	TPSxx/008	5
8	TPSxx/010	5, 7

### 5.4 Test Documents

Identify what test documents will be used to record the test process. The standards for test documentation are given in the Test Documentation Plan.

For each document identified the following information should be provided:

- Name of document
- Purpose
- Example of the form, if applicable
- Who is responsible for production and issue
- Who should use the document
- Explanation of how to use the document

If this information is given in another document, then only a list of the documents should be given and a reference made to the other document.

#### *Integration Test Example*

In addition to the Test Documents described in Section 5.2, test reporting is covered by the following document types. Their use is described in Section 6 and Section 7 of this document.

- Integration Test Item Transmittal Reports (TTRxx) is a collection of individual Transmittal Report Forms, each identifying a test item being formally transmitted for testing. These forms will be controlled and forwarded by Configuration Management.
- Integration Test Items are the sequentially numbered Baselines – each Baseline representing a certain set of Units integrated into the partially completed system. A TTR will be numbered in accordance with the Baseline it represents. It will also contain a version identifier. (I.e. TTR0xx001/1.5 represents Baseline001, version 1.5).
- Transmittal to Integration Testing will be initiated by the Unit Testing Activity when the Unit has met its exit criteria. A new baseline will then be generated and approved by Configuration Management.
- The standard Transmittal Report Form is found in the appendix.
- Integration Test Logs (TLxx) is a collection of individual Test Logs.
- A Test Log is chronological record of what occurred during test execution. For automated tests, it should be produced by the testing software, drivers or instrumented code. For manual tests, each case tested must be logged.
- The standard Test Log is found in the appendix.
- Integration Test Incident Reports (TIRxx) is a collection of reports, each describing any event that occurs during testing that requires further investigation. This includes:
  - Defects discovered in the Items being tested
  - Defects discovered in the Test Procedures and Test Cases or Test Data
  - Problems encountered regarding the Test Environment
- The standard Test Incident Report Form is found in the Appendix.
- Integration Test Summary Reports (TSRxx) is a collection of reports that summarize the testing activities associated with one or more Test Design Specifications.

- Integration Test Fault Reports (TFRoc) is a collection of Fault Reporting Forms that formally documents all faults, when they occurred, who found them, who is to resolve the fault, when resolved and how.
- The standard Fault Reporting Form is found in the Appendix.

### 5.5 Reviews

Describe the reviews that will be performed on the test plan, test specifications, test results, etc.

If this is documented in a Verification and Validation (V&V) or Independent Verification & Validation (IV&V) Plan for the project, or some other document, then only a list of reviews need be given here and a reference to the applicable plan and/or other documents.

If no V&V/IV&V or other such document exists for the project then full details of the reviews should be given here. For each review identified the following information is provided:

- Name of review
- Purpose
- Items to be reviewed
- Criteria for acceptance
- Attendees and their responsibilities
- Details of the procedures for calling, running, follow-up, etc. of the review and re-reviews

## 6. Recording of Test Results

Describe how the test results will be recorded and analyzed. This information states what data will be recorded, by whom, and where. It should also identify the organizational elements/individuals responsible for controlling such data and documents.

The procedures for analyzing the test results will be described. These procedures can vary from the specification of informal daily review meetings through to formal meetings with the client to review the test results. These "reviews" are distinct from the reviews given in section 2.5.5 which cover test plans, specifications, and the test report.

#### Example

Any unexpected software error or test behavior encountered during the execution of any Test Procedure must be recorded by the tester in a Test Incident Report.

Following execution of any test, automated or manual Test Logs are reviewed by the Test Team to be sure that all incidents are reported.

Test Incident Reports are then examined by the Fault Review Team. All Incidents are classified as:

- Class-A Software fault where testing cannot continue until it is resolved
- Class-B Software fault where testing can continue
- Test Fault where the defect is in the test case, test procedure or test data, driver, or stub.
- Open Issue where the system works according to specification but still is questionable. (Open issues will later be resolved by a Change Request or by closing the issue)
- Closed Issue where there is no fault.

The test team begins a Fault Report Form for each Classified Fault or Open Issue. This form is then sent to Change Management for approval. This form will be updated as this Fault proceeds through the correction process (See Section 7 of this plan.

## 7. Correction of Faults

Describe how faults are to be recorded, notified, fixed, new versions of the software introduced, and what and how re-testing is to be performed.

If all or some of this information is contained in a Configuration Management Plan (CMP) for the project, or some such document, then reference to those documents only need be given in the appropriate place.

If no such document exists then full details will be given here. This information should cover:

- How faults are to be recorded and by whom, including allocation of their severity
- How faults are to be notified to the fault team, by whom, and information required
- How faults are to be allocated and tracked within the fault team
- How the status of faults are to be reported and tracked, and to whom the report will be distributed
- How fixes are to be verified and controlled and by whom
- How, when and under what conditions new versions of software will be introduced into the testing environment and by whom
- The principles of re-testing of the new software both before issue into the test environment and during testing. This will also define responsibilities and authorities.

**8. Archiving**

Describe the archiving of test documentation, test data, and test results. This information includes:

- Identification of what is to be archived
- In what form
- Where it is to be stored and for how long
- Responsibilities for archiving and the archiving process

**9. Test Summary Report**

Describe the format and contents of the formal Test Summary Report, responsibilities for supplying data for, and production of, the Test Summary Report. The format and contents of the Test Summary Report is given in the Test Documentation Plan.

The information required for this section includes:

- The purpose and use of the Test Summary Report
- Description of the data required and where it can be obtained from
- The format and contents of the report
- Identification of the responsibilities for producing the data and actual production of the report
- The distribution list for the report

*Integration Test Example*

Following completion of Integration testing, the Test Manager will produce an Integration Test Summary Report in accordance with the Test Documentation Standards. This report will include summaries of faults found and corrected in each step of Integration testing. Test Logs and Fault Logs will be used as source material.

**10. Entry Criteria**

Describe the tasks and conditions that need to be satisfied before testing can be commenced. This does not include those tasks specifically related to the test activities covered by the plan as these are covered by section 14 of the plan.

The information provided may cover such areas as:

- Software item availability
- Hardware (not test equipment)

- Environmental software
- Completion of other testing, e.g. completion of hardware acceptance testing before system testing
- Availability of documentation, not test documentation, such as user manuals

Identify those organizational elements/individuals responsible for ensuring those tasks are completed and, if possible, the planned date for completion.

*Integration Test Example*

No Integration Test Item (Baseline) will be tested until the following criteria are met:

- The Units involved have successfully exited from Unit Tests
- Configuration Management has transmitted the Baseline with an accompanying Integration Test Transmittal Report
- Necessary Test Software, drivers and stubs have been correctly compiled and installed in the Integration test environment
- All dependencies identified in the test specifications are satisfied
- The appropriate test environment is complete and available
- The planned test staff is available and trained
- Integration test documentation (Test Design Specifications, Test Case Specifications, Test Procedure Specifications) has been reviewed and approved
- Testing has been scheduled

All completed Test Procedures, Cases, and Test Data must be stored on-line in an area that is protected by read-only security and managed by the Test Data Administrator.

Similarly, all test data must be copied to the local test environment before tests are run. Other network users must be blocked from accessing the integration test environment, and testers must use Test Data and Test Procedures and Cases only from the local testing area.

**11. Item Pass/Fail Criteria**

Describe the criteria to be used to determine whether each test item has passed or failed. If these criteria are based on category of faults, e.g. Category A, B, or C, then give a clear and precise definition of each of these categories.

## 12. Exit Criteria

Describe the criteria to be used to determine exit from testing. This should cover such areas as:

- » Test coverage required
- » Number and type of faults allowed, plans to fix such faults
- » Fault detection rates
- » Errors in documentation

Details are given of the process of evaluation against the criteria, the organizational elements/individuals responsible, and any formal documents used to signify successful exit from testing.

Details are provided of the actions and activities to be followed:

- If the test exit criteria are NOT met, include impact analysis
- If the test exit criteria are met e.g. document and obtain concurrence

**Note:** This section is of crucial importance if contractual liabilities result from failure to exit the test.

## 13. Test Suspension and Resumption Criteria

Describe the criteria used to suspend all or a portion of the testing activity on the test items associated with the plan. Also specify the testing activities that must be repeated when testing is resumed, together with any other procedures or testing required prior to reissue of the test items into testing.

### Integration Test Example

#### Suspension Criteria

- If the system crashes for any external reason
- If there is no response for 5 minutes
- If the test causes the system to crash
- If execution of a test case fails to provide prerequisites for the next test case.

#### Resumption Criteria

- If the Test Suspension is deemed by the Test Fault Team to be due to external reasons, the test can resume after the proper test environment has been reestablished. The test should restart the entire Test Procedure that was in execution at the time of the Test Suspension.

- If the Test Suspension is deemed by the Test Fault Team to be due to a defect in the test itself, testing can resume when the test defect has been corrected. The test should restart the entire Test Procedure that was in execution at the time of the Test Suspension.
- If the Test Suspension is deemed by the Test Fault Team to be due to a fault in the item being tested, the test can resume only when a new version of the test item is transmitted by Change Management.

#### 14. Environmental

Specify both the necessary and desired properties of the test environment. This covers:

- » The physical characteristics of the facilities including hardware configuration, communications, terminals, system and environmental software (including levels if applicable), and their mode of usage, e.g. stand-alone, exclusive use
- » Supplies required for the testing activities, e.g. special stationery, computer paper, checks, etc.
- » Levels of security that must be provided for the test facilities, system software, etc.
- » Special test tools required - both hardware and software (Note there must be described procedures for controlling and verifying these tools)
- » Other testing needs, e.g. office space, secure storage space, special access

Identify the source for all needs which are not currently available to the test group.

#### 15. Responsibilities

Identify the organizational elements/individuals necessary for managing, controlling, designing, preparing, executing, witnessing, checking, and evaluating the testing activities. Also identify the number and duration required of the resource. The information provided should include:

- Name of Resource
- Resource Identifier (used in Task Schedule)
- If applicable, number of this resource required
- Responsibilities as they apply to testing
- Duration required
- Organization providing
- Any special training required

- Work location

## 15.1 General Roles

### Test Manager

The Test Manager is responsible for the development and implementation of test strategies and plans. In addition, all test procedures, standards and requirements are ultimately the responsibility of the Test Manager. He/she is the primary interface with the development organization and will facilitate scheduling and tracking of test items.

### Test Data Administrator

The Test Data Administrator is responsible for the design, development, and support of the Baseline Management System. As this system becomes more stable, the position requirements may shift more toward organizational skills than system analyst skills.

### Test Case Administrator

The Test Case Administrator is responsible for maintaining the organization of all tests and providing metrics reporting. It is also his/her role to provide structure, standards, and direction in the development of Test Procedures, Specifications, and Cases. Development of high usage routines and ad hoc inquiries falls within the duties of this position.

### Test Supervisor

The Test Supervisor is responsible for day-to-day direction and personnel activities associated with Test Specialists. Applicable problems should be escalated to the Test Supervisor.

### Test Specialists

Test Specialists are responsible for planning, designing, and scripting all tests for their assigned areas. This requires expertise in a specific area as well as a good understanding of the complete system. They are required to logically identify problems and use a structured approach to assure each area has been tested according to program specifications.

## 15.2 Specific Responsibilities

Name	Role	Responsibilities	Estimated Start Date	Estimated Duration	Required Training

## 16. Testing Tasks and Schedules

Describe all testing tasks necessary to prepare for, perform, and evaluate the testing. Identify all tasks interdependencies. For each task the following should be provided:

- Name of Task
- Purpose
- Any special skills required
- Duration of task
- If required, identification of specific resource to perform the task
- Any dependencies

Provide a schedule of the test tasks. This can be tabular or a Gantt chart. Also, show major milestones and specifically named resources (see section 15 above) to perform the tasks.

Example

Task	Special Skills	Responsibility	Finish Date
Prepare Integration Test Plan		Test Manager	
Prepare Test Design Specification		Test Case Admin	
Construct Test Database		Test Specialist	

## 17. Additional Sections

Additional sections may be added at the end, as required. Some of the material may appear in other documents. If so, reference those documents in the body of the plan.

## **Project Test Strategy Plan**

**Authorized for issue by:**

<Customer PM Name>

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Project Manager

Veridos Project Manager

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**Date Here**

Revision History

Version	Date	Author	Summary of Changes

## Table of Contents

1.	Introduction .....	23
1.1	Purpose .....	23
1.2	Definitions and Acronyms .....	23
1.3	Assumptions .....	23
1.4	Dependencies .....	23
1.5	Related Documents .....	23
2.	Testing Scope .....	24
2.1	Components Covered .....	24
2.2	Summary of Tests .....	24
2.3	Tests Required .....	25
3.	Test Strategy .....	26
3.1	Strategies .....	26
3.2	Methodologies and Techniques .....	26
4.	Test Documentation .....	27
4.1	Test Plans .....	27
4.2	Supporting Test Plan Documentation .....	27
5.	Test Responsibilities .....	28
5.1	General Testing Responsibilities .....	28
5.2	Test Documentation Responsibilities .....	28
6.	Test Environments/Test Data .....	28
6.1	Test Environment Summary .....	28
6.2	Test Environment Preparation .....	28
6.3	Test Environment Management .....	28
6.4	Test Environment Configuration .....	28
6.5	Test Data Requirements .....	29
6.6	Test Data Management .....	29
7.	Fault Reporting .....	29
7.1	Defect Reporting System .....	29
7.2	Defect Lifecycle Process .....	29
7.3	Defect Priorities .....	29
8.	Tools and Training .....	30
8.1	Tools .....	30
8.2	Training .....	30
9.	Record Collection, Maintenance and Retention .....	30

## 1. Introduction

### 1.1 Purpose

Describe the purpose of the plan, e.g. this plan will identify the major types of tests, which will be performed on the components of the system, the test plans to be created, the supporting test documents, test logs/reports and the responsibilities for the testing activities.

This document should also identify any testing requirements specified by the client, e.g. the test strategy and plans must conform to the IEEE standards.

### 1.2 Definitions and Acronyms

Define all terms required to properly interpret this plan.

*Example*

Acceptance Criteria (IEEE)	The criteria software component must meet to successfully complete a test phase or satisfy delivery requirements.
Change Control (IEEE)	The process, by which a change is proposed, evaluated, approved (or rejected), scheduled and tracked.
Inspection (IEEE)	A formal evaluation technique in which deliverables are examined in detail by a person or group other than the author to detect faults, violations of standards, and other problems.
Integration Tests	Progressive tests that enable software objects to be combined into systems.
Regression Tests	Re-runs of tests to discover unintended side effects of software modification.

### 1.3 Assumptions

List all assumptions that have been made in preparing this plan.

### 1.4 Dependencies

Describe how the testing process will interact with other project plans. A list should be given of all related plans with a brief description of the interaction.

### 1.5 Related Documents

Identify any other documents and their version that are related to or contain details relevant to this plan. Identify each document by title, number, date and publishing organization. Specify the sources of the referenced documents.

*Example*

*The following documents are referenced in this document:*

- Requirements Definition <Project Name>, <Version>, <Date>
- Logical Design Specification <Project Name>, <Version>, <Date>

## **2. Testing Scope**

Identify the components to be tested and the tests that are to be carried out on each component.

### **2.1 Components Covered**

Briefly identify the components (units and subsystems) that are to be tested during the project.

### **2.2 Summary of Tests**

Identify the types of tests that will be performed during the project. The tests should be given their generic type as a title, e.g. unit/module tests, system test, acceptance test. This section should be brief, as further details of the tests themselves will be given in the next section.

**Note:** Each test type listed will be the subject of a separate documented Test Plan.

**Note:** The testing process must cover tests of software and components from third parties and those being produced by the client.

*Example**Test activities will include:*

- Integration Testing - Integration tests of inter-relationships between software modules and interfaces to <existing legacy system>. Integration Testing is covered by the Integration Test Plan Document (TP01).
- System Testing - Tests the functionality of the entire system as specified in Logical Design Specification [02]. System Testing is covered by System Test Plan Document (TP02).
- Acceptance Tests - Tests the functionality of the entire system as specified in Requirements Specification [01]. The intent is to demonstrate to <Client> that the system functions as specified. Acceptance Testing is covered by Acceptance Test Plan Document (TP03).
- Regression Tests - Several iterations are expected of all types of tests as well as Document Inspections due to: Change Requests, Fault Correction and new Software Versions. The purpose of such Regression Testing is to verify that changes work as specified and that defects have not been introduced due to the change. Regression Testing is covered by Test Plan Document (TP04).
- Unit Testing - Tests individual software objects identified in the Logical Design Specification [2] and finalized in the Detail Design Specification [4]. Unit testing is covered by Test Plan Document (TP05).

**2.3 Tests Required**

For each test type described in section 2.2 above, the following information should be provided (in any order).

- Name of the test
- Components covered by the test
- Objective of the test
- Brief description of the documents against which the tests will be based, e.g. Requirements Definition, Design Specification
- The organization(s) responsible for producing the test plan, test documentation, and for conducting the test
- Brief description of the acceptance criteria, entrance and exit criteria
- The timetable for production of the test plan, test documents and running the test. The test plan and test documentation are normally stated as a number of weeks before the test is due to run; while the test itself is related to a major milestone.
- Any requirements for the reviews of the test plan, documents, test outputs, etc.

### 3. Test Strategy

#### 3.1 Strategies

Describe the general approach and strategy that will be used to perform each level of testing. Particular attention should be given to the processes of producing test drivers, test stubs, etc. which are to be used. The details will cover how they are to be produced, by whom, their purpose and use, how they are to be controlled, tested, and supported.

##### *Example*

*The overall testing strategy will be incremental, from the bottom up.*

- Unit Testing
  - *Unit testing will test the functionality of each unit.*
  - *Drivers and test data will be constructed as necessary. The specification for the driver will be part of the Unit Test Plan.*
  - *Every effort will be made to schedule several units to be tested separately but in parallel.*
- Integration Testing
  - *Integration Testing will test the interface between units; verify that data is passed and transformed correctly and that there are no side effects.*
  - *Scaffolding of stubs, drivers and a test database will be constructed to represent the system and enable testing. As a unit is transmitted to Integration Testing, it will be scheduled to replace its associated stub.*
  - *Only one unit at a time will be inserted into the scaffolding for testing. The state of the system will be saved, documented and labeled with a "baseline" number that will be incremented with each insertion.*
  - *If errors are found, regression testing will first be conducted on the unit, and then on the baseline where the errors were found.*
  - *Every effort will be made to schedule several baselines to be tested separately but in parallel.*

#### 3.2 Methodologies and Techniques

Describe the methodology or testing techniques that will be used.

##### *Examples*

*The project test plans will meet the requirements in IEEE.*

*Technique examples are:*

- *Black Box Techniques*
- *White Box Techniques*
- *Static Techniques, which include:*

- Formal Inspection
- Structured Walkthrough
- Peer Review

#### 4. Test Documentation

Describe the test documentation to be produced and used on the project. Details of the types of supporting test documentation, their purpose and use are normally provided in the Test Documentation Plan. If such a document will not be produced, then full details of the test documents should be given here.

##### 4.1 Test Plans

Include all identified test plan documents, which will be produced for this project, e.g. Test Plan, Acceptance Test Plan.

The details for each test plan document listed should include:

- Name of document
- Purpose of the document
- Outline of the document's structure and contents

##### 4.2 Supporting Test Plan Documentation

Identify the types of supporting test plan documents, which will be used in the design, execution, and reporting of tests. These documents will be produced during the development and testing phases to support the planning and execution of the specified tests. Various document types, which may be used, are:

**Test Design Specifications** - A Test Design Specification refines the test approach. It identifies test cases and test procedures required to accomplish the testing and specify the feature pass/fail criteria.

**Test Case Specifications** - A Test Case Specification details the actual values used for input along with the anticipated outputs or results for a Test Design.

**Test Procedure Specifications** - A Test Procedure Specification lists the steps required to operate the system and exercise a particular test case associated with a test design.

**Test Logs** - A Test Log records what occurred during test execution.

**Test Incident Reports** - A Test Incident Report describes any event that occurs during testing that requires further investigation.

**Test Summary Reports** - A Test Summary Report summarizes the testing activities for each Test Design associated with a Test Plan.

**Fault Reports** - A Fault Report formally documents all faults, when they occurred, who found them, who is to resolve the fault, when it is resolved and how.

## VERIDOS

Identity Solutions  
by Giesecke+Devrient  
and Bundesdruckerei

**Test Item Transmittal Reports** - A Test Item Transmittal Report identifies items being transmitted for testing. The following documents contain all Transmittal Reports associated with a particular test plan.

## 5. Test Responsibilities

### 5.1 General Testing Responsibilities

Describe the specific responsibilities for planning and executing the testing of the various components within the project. This section must cover the approval and authorization of use of test plans, test documentation, etc. This section should describe the responsibilities of the client and third parties.

*Example*

- Test Manager

*Veridos will assign a Test Manager who is responsible for the development and implementation of test strategies and plans. The Test Manager is responsible for maintaining the organization of all tests and providing metrics reporting.*

- Test Specialists

*Test Specialists are responsible for planning, designing and scripting all tests for their assigned areas.*

- Customer

*The customer will review and approve all test plans and reports and provide test data as specified in the test plans.*

### 5.2 Test Documentation Responsibilities

Describe the specific responsibilities within the project for the production (and use) of the test documentation listed in section 4 of the plan.

This is best grouped by test type. For each test type given in section 2, provide a matrix indicating who is responsible for producing the test document and who is responsible for using it.

## 6. Test Environments/Test Data

### 6.1 Test Environment Summary

Define the number of test environments needed, and the purpose and location of each test environment.

### 6.2 Test Environment Preparation

Define the steps needed to prepare the test environment(s) ready for test execution.

### 6.3 Test Environment Management

The test team controls the test environment(s) and the timing of each installation of software onto it. Once code has been released to the test team and installed on the test

environment, the test environment is the master. If a defect is raised by the test team and the installation and configuration of the test environment has been verified to be correct, it remains a defect until the test team has agreed that it has been closed successfully.

#### 6.4 Test Environment Configuration

Define the configuration requirements for each test environment to be used.

#### 6.5 Test Data Requirements

Define the test data requirements and from where the data should be obtained. If test data is to come from a live source, ensure that this is stated and who is responsible for providing it.

#### 6.6 Test Data Management

Define any procedures for the resetting or reloading of test data.

### 7. Fault Reporting

#### 7.1 Defect Reporting System

Describe the system to be used for reporting defects.

##### Example

*All test incidents found in the Component Integration, System and User Acceptance Test phase will be recorded as defects. This project will use the XXXX Defect Tracking System. The Test Manager, the Project Manager and a User representative will review the priorities of all outstanding defects on a regular basis. This will ensure that defect priorities are set consistently and correctly and that both a technical and a business input to the process are received. It will also focus on ensuring that no faults that could threaten the successful execution of the User Acceptance Test are left unresolved.*

#### 7.2 Defect Lifecycle Process

Describe the standard Defect Lifecycle Process as per the chosen Defect Tracking System.

#### 7.3 Defect Priorities

Describe the different statuses that will be assigned to each defect for purposes of categorization.

##### Example

*This project will use 4 defect priorities as defined below:*

- 1. Critical, system cannot be implemented*
- 2. Serious, must be fixed as soon as possible*
- 3. Minimal, scheduled fix required*
- 4. Cosmetic, fix when convenient*

## 8. Tools and Training

### 8.1 Tools

Identify all testing tools and provide for each:

- Name of test tool, its purpose and supplier
- How and when it will be used
- Calibration requirements

On many projects, it may be necessary to evaluate and select suitable test tools. The purpose, process and selection criteria for the evaluation should be documented and these activities must be planned and scheduled.

### 8.2 Training

Describe any specialized training for testing, if any, that is required. If this is described in another document (e.g., Training Plan) then provide just a list of training needs here, plus a reference to the other document. This section should cover the test training required by the project team, and the client.

## 9. Record Collection, Maintenance and Retention

Describe the procedure for collecting and maintaining all test plans and the test results.

**CONFIDENTIAL**

State of West Virginia  
RFP to Provide Driver's License and ID Cards

Page 332 / 340

**VERIDOS**

**IDENTITY SOLUTIONS**  
by Giesecke+Devrient  
and Bundesdruckerei

**VERIDOS**

**IDENTITY SOLUTIONS**  
by Giesecke+Devrient  
and Bundesdruckerei

## **Project Test Summary Report**

Authorized for issue by:

Project Manager

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Veridos

Project Manager

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Date Here

**CONFIDENTIAL**

State of West Virginia  
RFP to Provide Driver's License and ID Cards

Page 333 / 340

**VERIDOS**

**IDENTITY SOLUTIONS**  
by Giesecke+Devrient  
and Bundesdruckerei

**VERIDOS**

Identity Solutions  
by Giesecke+Devrient  
and Bundesdruckerei

**Revision History**

Version	Date	Author	Summary of Changes

## Table of Contents

1.	Introduction .....	3
1.1	Purpose .....	34
1.2	Scope .....	34
1.3	Definitions and Acronyms .....	34
1.4	Assumptions .....	34
1.5	Dependencies .....	34
1.6	Related Documents .....	34
2.	Test Summary Identifier .....	34
3.	Summary .....	34
4.	Variances .....	34
5.	Comprehensiveness Assessment .....	34
6.	Summary of Results .....	35
7.	Evaluation .....	35
8.	Summary of Activities .....	35
9.	Approvals .....	35

**1.1 Purpose**

Describe the specific purpose of this plan.

**1.2 Scope**

Identify the items this plan covers.

Describe the relationship to other project plans along with any specific organizational interfaces required for the execution of the plan.

**1.3 Definitions and Acronyms**

Define or provide a reference to the definition of all terms required to properly interpret the plan. Describe the acronyms and notations used in the plan.

**1.4 Assumptions**

List the assumptions that have been made in preparing this plan.

**1.5 Dependencies**

State any dependencies on other documents, systems, applications, people, etc.

**1.6 Related Documents**

Identify any other documents and their version that are related to or contain details relevant to this plan.

**2. Test Summary Identifier**

**3. Summary**

**4. Variances**

Example:

*Conditions identified during the testing resulted in changes to the Detail Design Specifications to handle rounding errors. This caused subsequent changes to the code. 5 new test cases were developed.*

**5. Comprehensiveness Assessment**

This is where test coverage is summarized.

Example:

The following summarized the coverage for each Test Design. For each test, a detailed matrix is attached to this document, relating the Case ID to the System Specification Reference. This is for Requirements Coverage and Design Coverage, Domain Coverage and Exception Coverage.

There is another attached document supporting the Branch, Subroutine and Condition Coverage claims by Flow charts, decision tables and in some cases, code instrumentation.

## **6. Summary of Results**

Example:

Five of the test cases exposed faults involving rounding errors. The error *was* fixed by use of a different data type. The test cases at fault were rerun and all features passed.

## **7. Evaluation**

Example:

Unit testing passed its comprehensiveness criteria. 19 faults found. Three faults remain uncorrected These are Class-B faults. Resolution is still pending.

## **8. Summary of Activities**

Example:

Unit Test Activities begun 21 Jan 2014 and was complete 4 May 2014.

## **9. Approvals**

## Exhibit C: Sample Project Work Plan

Thu 8/28/18 WVA project plan.mpp									
ID	WBS	Task Name	Instructions	Duration	Start	Finish	Resource Name	Units	Month 21
									8/18 6/19
1		WVA Card Production Solution		351days	Wed 8/1/18	Fri 12/5/18			
2	1	Complete Commercial Requirements		25days	Wed 8/1/18	Wed 8/5/18			
3	1.1	Receipt of Notice of Award		0days	Wed 8/1/18	Wed 8/1/18	WVA,EDC		
4	1.2	Receipt of Notice to Proceed	2	10days	Wed 8/1/18	Tue 8/14/18			
5	1.3	Execution of PRIME Contract	2	20days	Wed 8/1/18	Tue 8/28/18	Veridos,WVA		
6	1.4	Schedule Project Kickoff Meeting	3	10days	Wed 8/15/18	Tue 8/28/18	WVA		
7	1.5	Conduct Project Kick-off		2days	Tue 8/14/18	Wed 8/28/18	EDC,Veridos,W		
8	1.5.1	Complete Commercial and Technical Overview	5	1.5days	Tue 8/14/18	Wed 8/28/18	EDC,Veridos,W		
9	1.5.2	Complete the Solution Demonstration	7	0.5days	Wed 8/28/18	Wed 8/28/18	EDC,Veridos,W		
10	2	Phase 1 Planning		84days	Thu 8/9/18	Thu 9/27/18			
11	2.1	Provide Project Management Plan		5days	Thu 8/9/18	Thu 8/13/18	Veridos		
12	2.1.1	Develop Project Management Plan/PMP	6	5days	Thu 8/9/18	Wed 8/12/18	Veridos		
13	2.1.2	Conduct Review of Plan/PMP with WVA	11	1day	Thu 8/13/18	Thu 8/13/18	Veridos,EDC		
14	2.1.3	Approve Plan	12	0days	Thu 8/13/18	Thu 8/13/18	WVA		
15	3	Phase 2 Analysis		45days	Thu 8/9/18	Wed 11/7/18			
16	3.1	Complete WVA Gap Analysis		20days	Thu 8/9/18	Wed 10/3/18	Veridos		
17	3.1.1	Conduct WVA Gap Analysis	5	10days	Thu 8/9/18	Wed 8/19/18	EDC,Veridos		
18	3.1.2	Document & Analyze Findings of WVA Analysis	16	5days	Thu 9/20/18	Wed 9/26/18	EDC,Veridos		
19	3.1.3	Develop Recommendations	17	5days	Thu 9/27/18	Wed 10/3/18	EDC,Veridos		
20	3.1.4	Communicate Findings & Recommendations	18	0days	Wed 10/3/18	Wed 10/3/18	Veridos		
21	3.2	Develop Implementation Plan	6	45days	Thu 8/9/18	Wed 11/7/18	Veridos,EDC,W		
22	4	Phase 3 & 4 Design & Development		190days	Mon 9/17/18	Fri 9/17/19			
23	4.1	Card Fulfillment Work package		188days	Mon 9/17/18	Wed 9/9/19	Veridos		
24	4.1.1	Provide card designs/artfile		5days	Mon 9/17/18	Fri 9/21/18	WVA		
25	4.1.2	Create DL & ID card proofs	23	15days	Mon 9/24/18	Fri 10/12/18	Veridos		
26	4.1.3	Review card proofs & provide feedback	24	5days	Mon 10/15/18	Fri 10/19/18	WVA		
27	4.1.4	Update card proofs	25	10days	Mon 10/22/18	Fri 11/2/18	Veridos		
28	4.1.5	Approve card proofs	26	5days	Mon 11/5/18	Fri 11/9/18	WVA		
29	4.1.6	Manufacture press proof samples	27	20days	Mon 11/12/18	Fri 12/7/18	Veridos		
30	4.1.7	Review press proof samples and provide feedback	28	5days	Mon 12/10/18	Fri 12/14/18	WVA		
31	4.1.8	Approve press proofs and place order	29	0days	Fri 12/14/18	Fri 12/14/18	WVA		
32	4.1.9	Manufacture approved UAT DL & ID cards	30	40days	Mon 12/17/18	Fri 2/8/19	Veridos		
33	4.1.10	Vault UAT cards into inventory	31	3days	Mon 2/11/19	Wed 2/13/19	Veridos		
34	4.1.11	Manufacture approved Production DL & ID cards	31	60days	Mon 2/11/19	Fri 5/3/19	Veridos		
35	4.1.12	Vault Production cards into inventory	33	3days	Mon 5/6/19	Wed 5/8/19	Veridos		
36	4.2	Card Fulfillment System		145days	Mon 11/19/18	Fri 6/7/19	Veridos		
37	4.2.1	Complete Requirements Gathering		13days	Mon 11/19/18	Wed 12/5/18	Veridos		
38	4.2.2	Complete Technical Specifications	36	130days	Thu 12/6/18	Mon 12/24/18	Veridos		

Thu 6/28/18 WVA project plan.mpg

ID	WBS	Task Name	Predecessors	Duration	Start	Finish	Resource Names	Notes	March 21
38	5.2.3	Review Technical Specifications	37	1day	Tue 12/25/18	Tue 12/25/18	Veridos		3/28
39	5.2.4	Approve Technical Specifications	38	0days	Tue 12/25/18	Tue 12/25/18			5/19
40	4.2.3	Complete Solution Development	39	84days	Wed 12/26/18	Mon 4/22/19	Veridos		
41	4.2.3	Integration & QA	40	34days	Tue 4/23/19	Fri 6/7/19	Veridos		
42	4.3	Develop DL Solution		125days	Mon 11/26/18	Fri 5/17/19			
43	4.3.1	Complete System Development		105days	Mon 11/26/18	Fri 4/19/19	EDC		
44	4.3.1.1	Development of Secure FRS Solution Specification		20days	Mon 11/26/18	Fri 12/21/18	EDC		
45	4.3.1.2	Complete FRS Data Model	44FS-Edays	5days	Mon 12/31/18	Fri 1/4/19	EDC		
46	4.3.1.3	Complete Data Migration Utilities	45	5days	Mon 1/7/19	Fri 1/11/19	EDC		
47	4.3.1.4	Complete Production Integration	46	10days	Mon 1/14/19	Fri 1/25/19	EDC		
48	4.3.1.5	Complete External Messaging Integration	46	15days	Mon 1/7/19	Fri 1/25/19	EDC		
49	4.3.1.6	Complete Workflows and User Interfaces	48	30days	Mon 1/28/19	Fri 3/8/19	EDC		
50	4.3.1.7	Complete Solution Reports	48	30days	Mon 3/11/19	Fri 4/19/19	EDC		
51	4.3.2	Complete Solution Documentation		105days	Mon 12/24/18	Fri 5/17/19	EDC		
52	4.3.2.1	Develop Data Migration Plan	45SS+10days	10days	Mon 1/14/19	Fri 1/25/19	WVA,EDC		
53	4.3.2.2	Development of System Integration Test/SIT Plan	44	20days	Mon 12/24/18	Fri 1/18/19	EDC		
54	4.3.2.3	Development of User Acceptance Test/UAT Plan	53	20days	Mon 1/21/19	Fri 2/15/19	WVA		
55	4.3.2.4	Complete Solution Documentation - Operator	49	10days	Mon 3/11/19	Fri 3/22/19	EDC		
56	4.3.2.5	Complete Solution Documentation - Admin	50	20days	Mon 4/22/19	Fri 5/17/19	EDC		
57	5	Phase 5 Testing		62days	Mon 4/22/19	Tue 7/16/19			
58	5.1	Solution Deployment to TEST Environments		62days	Mon 4/22/19	Tue 7/16/19			
59	5.1.1	Install - Integration Test Environment	43	1day	Mon 4/22/19	Mon 4/22/19			
60	5.1.2	Complete Data Migration for Integration Testing	59	1day	Tue 4/23/19	Tue 4/23/19			
61	5.1.3	Complete Development Integration Testing/DIT	58,43	15days	Tue 4/23/19	Mon 5/13/19	EDC		
62	5.1.4	Complete System Integration Testing/SIT		20days	Tue 5/14/19	Mon 6/18/19			
63	5.1.4.1	Conduct End-to-End Integrated Testing	61	20days	Tue 5/14/19	Mon 6/18/19	EDC,WVA		
64	5.1.5	Install - User Acceptance Environment/UAT	53FF-32days	30days	Mon 6/3/19	Wed 6/6/19	EDC,WVA		
65	5.1.6	Complete Data Migration for UAT Testing	64	20days	Thu 6/6/19	Fri 6/7/19			
66	5.1.7	Complete User Acceptance Testing/UAT	65	20days	Mon 6/10/19	Fri 7/5/19	WVA		
67	5.1.8	Performance testing	66	70days	Mon 7/8/19	Tue 7/16/19			
68	5.1.9	Card Production User Acceptance Testing	41	14days	Mon 6/10/19	Thu 6/27/19	Veridos		
69	6	Phase 6 Deployment		43days	Fri 6/7/19	Tue 8/16/19			
70	6.1	WVA sign-off to implement		43days	Fri 6/7/19	Tue 8/16/19			
71	6.1.1	Environment Install - Production/PROD Environment	66FF-5days	5days	Wed 6/25/19	Fri 6/25/19	EDC,WVA		
72	6.1.2	Environment Install - Disaster Recovery/DR Environment	71	5days	Mon 7/1/19	Wed 7/3/19	EDC,WVA		
73	6.1.3	Complete Data Migration for Production	71	20days	Mon 7/1/19	Fri 7/26/19			
74	6.1.4	Complete Promotion to Production		45days	Fri 6/7/19	Tue 8/6/19			
75	6.1.4.1	Implement Card Fulfillment System		43days	Fri 6/7/19	Tue 8/6/19			

Thu 6/28/18 WVA project plan map									
ID	WBS	Task Name	Predecessors	Duration	Start	Finish	Resource Names	Notes	March 21
									3/13
									5/29
26	6.1.4.1.1	Approve Promotion of Code into Production	68	3days	Thu 6/27/19	Thu 6/27/19			
27	6.1.4.1.2	CODE FREEZE	66FF-10days	11days	Fri 6/7/19	Fri 6/21/19			
28	6.1.4.1.3	Install Application and On-line Services	76FS-14days	10days	Thu 7/18/19	Wed 7/31/19	Vendos		
29	6.1.4.1.5	Go Live	78	1day	Thu 8/2/19	Thu 8/2/19			
30	6.1.4.1.4	First Run Assistance	79	3days	Fri 8/2/19	Tue 8/6/19	Veridos		
81	7	Provide Training		200days	Thu 10/4/18	Wed 7/10/19			
82	7.1	Develop Training Plan	15	30days	Thu 10/4/18	Wed 11/14/18	EDC,WVA		
83	7.2	Approve Training Plan	82	58days	Mon 4/22/19	Wed 7/10/19	WVA		
10	7.2.1	Complete Training Readiness		58days	Mon 4/22/19	Wed 7/10/19	WVA		
11	7.2.1.1	Identify training populations		15days	Mon 4/22/19	Fri 5/10/19	EDC,WVA		
12	7.2.1.1.1	Identify UAT personnel for training	50	15days	Mon 4/22/19	Fri 5/10/19			
13	7.2.1.1.2	Identify personnel for Operator course	50	15days	Mon 4/22/19	Fri 5/10/19			
14	7.2.1.1.3	Identify personnel for Secura Admin course	50	15days	Mon 4/22/19	Fri 5/10/19			
15	7.2.1.1.4	Identify personnel for Secura Adjudication	50	15days	Mon 4/22/19	Fri 5/10/19			
16	7.2.1.1.5	Identify personnel for Train the Trainer course, if required	50	15days	Mon 4/22/19	Fri 5/10/19			
91	7.2.1.2	Schedule trainees		58days	Mon 4/22/19	Wed 7/10/19	EDC,WVA		
92	7.2.1.2.1	schedule UAT training, if required	84SS-15days	6days	Mon 5/13/19	Fri 5/17/19			
93	7.2.1.2.2	schedule Secura Administrator training classes	94SS-15days	10days	Mon 4/22/19	Fri 5/3/19			
94	7.2.1.2.3	Schedule Secura Training classes		43days	Mon 5/13/19	Wed 7/10/19			
95	7.2.1.2.3.1	schedule Operator training for UAT personnel, if required	84SS-15days	5days	Mon 5/13/19	Fri 5/17/19			
96	7.2.1.2.3.2	schedule Operator training for UAT personnel, if required	84SS-15days	5days	Mon 5/13/19	Fri 5/17/19			
97	7.2.1.2.3.3	schedule Secura Operator classes for Pilot site personnel	118SS-20days	5days	Thu 6/6/19	Wed 6/12/19			
98	7.2.1.2.3.4	schedule Secura Adjudication training for Pilot personnel	118SS-20days	5days	Thu 6/6/19	Wed 6/12/19			
99	7.2.1.2.3.5	Schedule Secura Operator Training for Implementation sites	97	20days	Thu 6/13/19	Wed 7/10/19			
100	7.2.1.2.3.6	Schedule Secura Adjudication Training for Implementation	97	20days	Thu 6/13/19	Wed 7/10/19			
101	7.2.1.3	Prepare Training room (s)	94SS	5days	Mon 5/13/19	Fri 5/17/19			
102	7.2.1.4	Complete updates to training materials	51	25days	Mon 5/20/19	Fri 6/21/19			
103	7.2.1.5	Ship training materials	102	3days	Mon 6/24/19	Wed 6/28/19	EDC		
104	7.3	Deliver Secura Administration Training for WVA Administrators and IT staff		4days	Thu 6/13/19	Tue 6/18/19	EDC		
105	7.3.1	Mobilize Trainer to Training site	118SS-15days	1day	Thu 6/13/19	Thu 6/13/19			
106	7.3.2	Conduct Secura System Administration Training	105	2days	Fri 6/14/19	Tue 6/18/19			
107	7.4	Deliver Secura Operator Training	118SS-15days	2days	Thu 6/13/19	Thu 6/13/19	EDC		
108	7.5	Deliver Secura Adjudication Training - roles based on Business Use cases	118SS-15days	4days	Thu 6/13/19	Tue 6/18/19			
109	7.6	Deliver "Train the Trainer Course"	106	4days	Wed 6/19/19	Mon 6/24/19			
110	8	Complete DLO Site Installations		131days	Wed 6/6/19	Thu 12/5/19			
111	8.1	Complete Pilot Phase		51days	Wed 6/6/19	Thu 9/15/19			
112	8.1.1	Conduct Site Readiness		15days	Wed 6/6/19	Wed 6/26/19			

Thu 8/28/13 WVA project plan.mso									
ID	WBS	Task Name	Predecessors	Duration	Start	Finish	Resource Names	Notes	March 21
113	8.1.1.1	Lock Down Pilot Schedule	64	0days	Wed 6/5/19	Wed 6/5/19			5/19
114	8.1.1.2	Stage Equipment Deliveries for each Pilot Site	113SS-15days	4days	Thu 6/13/19	Tue 6/18/19			6/19
115	8.1.1.3	Ship Equipment for each Pilot Site	114	5days	Wed 6/19/19	Tue 6/25/19			
116	8.1.1.4	Confirm Delivery of Equipment for each Pilot Site	115	1day	Wed 6/25/19	Wed 6/26/19			
117	8.1.1.5	Confirm Training of Staff at each Pilot Site	115SS-10days	5days	Thu 6/20/19	Wed 6/26/19			
118	8.1.2	Install Pilot DLO Sites		1day	Thu 7/4/19	Thu 7/4/19	EDC		
119	8.1.2.1	Install Pilot Site #1	72	1day	Thu 7/4/19	Thu 7/4/19			
120	8.1.2.2	Install Pilot Site #2	72	1day	Thu 7/4/19	Thu 7/4/19			
121	8.1.2.3	Install Pilot Site #3	72	1day	Thu 7/4/19	Thu 7/4/19			
122	8.1.3	Receipt of Acceptance of Pilot Phase	79	10days	Fri 8/2/19	Thu 8/15/19	WVA		
123	8.2	Receipt of Acceptance of Implementation Phase	76	0days	Thu 8/27/19	Thu 8/27/19	WVA		
124	8.3	Provide Warranty Support	79	26days	Fri 8/2/19	Thu 12/5/19			
125	8.4	Project Closure		26days	Fri 8/2/19	Thu 8/29/19	Veridos		
126	8.4.1	Finalize Documentation	79	20days	Fri 8/2/19	Thu 8/29/19	Veridos		
127	8.4.2	Handover to Relationship Managers	79	1day	Fri 8/2/19	Fri 8/2/19	Veridos		

# VERIDOS

IDENTITY SOLUTIONS

by Giesecke+Devrient  
and Bundesdruckerei

July 2, 2018

Melissa Pettrey, Senior Buyer  
Department of Administration, Purchasing Division  
2019 Washington Street East  
Charleston, WV 25305-0130

06/29/18 09:59:15  
WV Purchasing Division

**RE: RFP DMV1800000001**

**Dear Ms. Pettrey,**

On behalf of Veridos America, Inc. we are pleased to present sample cards for our proposal in response to West Virginia Division of Motor Vehicles (WVDMV), to **RFP DMV1800000001** Driver's License and ID Card.

Our Technical and Cost Proposals are being submitted in a separate package. Please include the sample cards with our proposal package to be considered as part of the evaluation process.

Sincerely,



Kathleen Synstegaard  
Director, Sales USA



# West Virginia

## DRIVER'S LICENSE

USA



1,2 NAME  
DOE,  
JOHN

8 2020 ENTERPRISE PKWY  
BLUEFIELD WV 24701

4d NUMBER  
1234-5678-9100

4a ISS 08/08/2018 4b EXP 08/08/2022

5 DD ABC123456789 16 HGT 6' 0"

15 SEX M

9 CLASS D

9a END NONE

12 REST X

3 DOB 10/30/1992

18 EYES BLU



HZ9004060

**Endorsements: NONE**

**Restrictions: X - Corrective lenses**

**DOB: 10/30/1992**