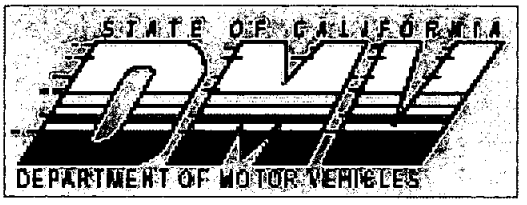


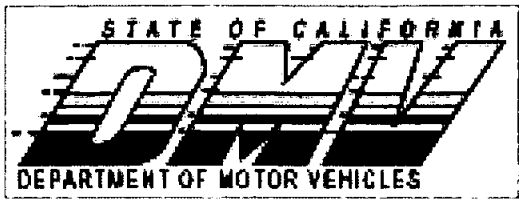
Driver License / Identification / Salesperson Contract Feasibility Study Report

PCAS #05-533

Department of Motor Vehicles

Licensing Operations Division

Revised June 2, 2006



Driver License / Identification / Salesperson Contract Feasibility Study Report

Department of Motor Vehicles

PCAS #05-533

Licensing Operations Division

Revised June 2, 2006

Driver License/Identification/Salesperson Contract
Feasibility Study Report
Summary of Changes
June 2, 2006

Section 2A: Executive Summary

- Estimated project start date was changed from 4/27/06 to 7/14/06.

Section 2D: Budget Information

- One-Time costs increased from $1,874,087 to $1,889,087 due to the $15,000 in additional one-time telecommunications costs for two T-1 lines and a DS3 circuit.
- Continuing costs decreased from a total of $9,601,886 to $9,572,630 due to the recalculation of continuing telecommunications costs at $6,310/month.

Section 2E: Vendor Project Budget

- The IV&V budget of $221,025 was split -- $147,054 for IPOC and $73,971 for IV&V.

Section 3: Business Case

- Added language to build the business case for a biometric logon.

Section 4: Baseline Analysis

- Added language describing current lack of an audit trail since the VCS does not require a user-specific identification and password. A generic identification and password are used instead.

Section 5: Proposed Solution

- Added language to include a separate IPOC category in the project resource requirements table.
- The one-time costs table was updated to split the costs between IV&V and IPOC and the one-time telecommunications costs were added.
- Added language why a biometric logon is part of the solution.

Section 6: Project Management

- Revised the project organization chart and project roles table to include the IPOC.
- Changed the project schedule to reflect a 4/13/06 start date and estimated 6/7/06 end date for control agency review and approval.

Section 7: Risk Management Plan

- Revised portions to include IPOC involvement.

Section 8: Economic Analysis Worksheets

- Added one-time telecommunications cost of $15,000 in FY 07/08.
- Adjusted continuing telecommunications costs downward by a total of $29,256 to reflect a recalculation of costs at $6,310 per month.
- Added text to indicate the biometric logon was included in the per card costs.

DOCUMENT CONTROL

Date	Version	Description
11/7/05	1.0	Draft FSR for DMV review
11/15/05	1.7	Incorporates edits from DMV and Business Advantage Team
11/18/05	1.8	Merged version of edited and submitted
11/29/05	1.9-2	Draft incorporating cost revisions
12/2/05	1.9-2	Draft incorporating all comments
12/6/05	1.9-3	Draft incorporating all comments through 12/5
12/7/05	2.0	Draft for executive review and signature
12/9/05	2.1	Revised per Budgets' request
12/13/05	2.2	Revised per Budget's request
12/14/05	3.0	First draft to Agency
12/19/05	3.1	Revised to include DGS service fees
12/20/05	4.0	Submitted to DOF
3/23/06	4.5	Revision reflecting addition of identity document imaging for concurrent review
4/3/06	4.6	Incorporates comments from concurrent review
6/2/06	5.0	Incorporates comments from DOF

TABLE OF CONTENTS

List of Figures

List of Tables

1. Executive Project Approval Transmittal

Information Technology Project Request

Feasibility Study Report Executive Approval Transmittal

Department Name
Department of Motor Vehicles
Project Title (maximum of 75 characters)
Driver License / Identification / Salesperson License Contract

Project Acronym	Department Priority	Agency Priority
DL/ID/SP	1	

APPROVAL SIGNATURES

I am submitting the attached Feasibility Study Report (FSR) in support of our request for the Department of Finance's approval to undertake this project.

I certify that the FSR was prepared in accordance with State Administrative Manual Sections 4920-4930.1 and that the proposed project is consistent with our information technology strategy as expressed in our current Agency Information Management Strategy (AIMS).

I have reviewed and agree with the information in the attached Feasibility Study Report.

Chief Information Officer	Date Signed
Printed name: Bernard C. Soriano, Ph.D.	12/21/05
Budget Officer	**Date Signed**
Printed name: Jean Shiomoto	12.21.05
Chief Deputy Director	**Date Signed**
Printed name: Ken Miyao	12/21/05
Agency Secretary	**Date Signed**
Printed name: Sunne Wright McPeak	1-17-06

2. Project Summary Package

Section A: Executive Summary

Section B: Project Contacts

Section C: Project Relevance to State and/or Department/Agency Plans

Section D: Budget Information

Section E: Vendor Project Budget

Section F: Risk Assessment Information

INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION A: EXECUTIVE SUMMARY

1.	**Submittal Date**	4/13/2006 (Resubmitted June 2, 2006)

		FSR	SPR	PSP Only	Other:	
2.	**Type of Document**	X				
	Project Number	**PCAS #**	05-533	**DOF #**		

			Estimated Project Dates	
			Start	**End**
3.	**Project Title**	Driver License / Identification / Salesperson License Contract	07/14/06	06/30/08
	Project Acronym	DL/ID/SP		

4.	**Submitting Department**	Department of Motor Vehicles
5.	**Reporting Agency**	Business Transportation and Housing

6. Project Objectives

1. Fully Implement a new DL/ID/SP card solution by May 11, 2008:
   - -- Begin development of the solution by July 2007.
   - -- Begin phased implementation by February 2008.
   - -- Fully transition DL/ID/SP records from current system by February 2008 to coincide with first phase of field office implementations.
2. Improve the ability to verify the identity of all applicants:
   - -- Implement immediate verification that a newly captured print matches existing print image.
   - -- Implement an objective photo match process to identify potential fraud.
   - -- Reduce the number of fraud and identity theft cases.
3. Adhere with AAMVA Standards:
   - -- Implement tamper-proof security features most effective in reducing fraud.
   - -- Include both overt and covert security features.
   - -- Provide at least the same number of security features presently included in DL/ID/SP cards.
   - -- Provide updated security features to deter counterfeiting.
4. To comply with the REAL ID Act and clarifying federal regulations:
   - -- Provide ability to digitally capture images of identity source documents for CA DL/ID cardholders.
   - -- Minimize service delays so that the average time to process a transaction in the field office does not exceed 10 minutes for an original application and 8.5 minutes for a renewal.

8.	**Major Milestones**	**Estimated Start Date**	**Estimated End Date**
	FSR Approved	04/13/06	06/07/06
	Approval and Release of RFP	01/16/06	06/29/06
	Select Vendor & Award DL/ID/SP Contract	07/14/06	07/02/07
	System Designed and Developed	07/03/07	12/11/07
	Testing Completed	10/10/07	02/14/08
	Training	02/20/08	05/07/08
	Phased Implementation	02/20/08	05/08/08
	PIER	10/15/08	04/13/09
	Key Deliverables		
	Approved FSR		06/07/06
	RFP Release Approval		06/29/06
	Contract Signed with DL/ID/SP Vendor		07/02/07
	Design Document Completed		10/02/07
	Unit Testing Sign-Off		12/13/07
	User Acceptance Sign-Off		02/14/08
	Staff Training Completed		05/07/08
	System Fully Implemented		05/08/08
	PIER Completed and Sent to Department of Finance		04/13/09

7. Proposed Solution

The proposed solution will transition support of current DL/ID/SP card production to a new contractor. This solution will include:
- -- Hardware and software to capture, store, and retrieve, images and demographics;
- -- Verification that a newly captured fingerprint image matches the one on file and that a newly captured photo does not match one on file attached to another record;
- -- A database at a centralized location with a redundant system and backup at a separate site;
- -- A card production facility to produce DL/ID/SP cards;
- -- Audit and tracking capabilities; and,
- -- Hardware and software to digitize, store and display identity source documents and track validation of digitized documents.

INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION B: PROJECT CONTACTS

Project #	
PCAS	**DOF**
05-533	
Doc. Type	FSR

Executive Contacts								
	First Name	**Last Name**	**Area Code**	**Phone #**	**Ext.**	**Area Code**	**Fax #**	**E-Mail**
Agency Secretary	Sunne	Wright McPeak	(916)	323 - 5405		(916)	323- 5440	btorres@bth.ca.gov (Belen Torres - assistant)
Director	George	Valverde	(916)	657- 6940		(916)	657- 7393	gvalverde@dmv.ca.gov
Budget Officer	Jean	Shiomoto	(916)	657- 7068		(916)	657- 6851	jshiomoto@dmv.ca.gov
CIO/ISD Div Chief	Bernard C.	Soriano	(916)	657- 7626		(916)	657- 8044	bsoriano@dmv.ca.gov
Project Sponsor	John	McClellan	(916)	657- 6534		(916)	657- 6261	jmcclellan@dmv.ca.gov

Direct Contacts								
	First Name	**Last Name**	**Area Code**	**Phone #**	**Ext.**	**Area Code**	**Fax #**	**E-Mail**
Doc. Prepared By	Crystal	Cooper	(916)	657 8295		(916)	657 8344	ccooper2@dmv.ca.gov
Business Contact	Wesley	Goo	(916)	657- 8976		(916)	657- 3971	wgoo@dmv.ca.gov
IT Contact	Darlene	Wheeler	(916)	657- 8608		(916)	657- 6565	dwheeler@dmv.ca.gov
Project Manager	Wesley	Goo	(916)	657- 6269		(916)	657- 3971	wgoo@dmv.ca.gov
Program Lead	Marilyn	Meek	(916)	657- 1366		(916)	657- 3971	mmeek@dmv.ca.gov

INFORMATION TECHNOLOGY PROJECT SUMMARY
SECTION C: PROJECT RELEVANCE TO STATE AND/OR DEPARTMENT PLANS

1.	**What is the date of your current Operational Recovery Plan (ORP)?**	**Date**	10/15/2004
2.	**What is the date of your current Agency Information Management Strategy (AIMS)?**	**Date**	08/2005
3.	**For the proposed project, provide the page reference in your current AIMS and/or Strategic Business Plan.**	**Doc.**	SITP
		Page #	7

Project #	
PCAS	**DOF**
05-533	
Doc. Type	FSR

		Yes	**No**
4.	**Is the project reportable to control agencies?**	X	
	If YES, CHECK all that apply:		
X	a) The project involves a budget action.		
	b) A new system development or acquisition that is specifically required by legislative mandate or is subject to special legislative review as specified in budget control language or other legislation.		
	c) The project involves the acquisition of microcomputer commodities and the agency does not have an approved Workgroup Computing Policy.		
X	d) The estimated total development and acquisition cost exceeds the departmental cost threshold.		
	e) The project meets a condition previously imposed by Finance.		

INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION D: BUDGET INFORMATION

Project #	
PCAS	DOF
05-533	
Doc. Type	FSR

Budget Augmentation Required?												
	No		If YES, indicate fiscal year(s) and associated amount:									
	Yes		FY	2005/06	FY	2006/07	FY	2007/08	FY	2008/09	FY	2009/10	FY	
				$0		$0		$632,674		$2,315,547		$0		

PROJECT COSTS

1.	Fiscal Year	2005/06	2006/07	2007/08	2008/09	2009/10		TOTAL
2.	One-Time Cost	0	691,655	1,197,432	0	0		$1,889,087
3.	Continuing Costs	0	0	1,061,593	8,467,324	0		$9,528,917
4.	TOTAL PROJECT BUDGET	$0	$691,655	$2,259,025	$8,467,324	$0		$11,418,004

SOURCES OF FUNDING

5.	General Fund							$0
6.	Redirection		691,655	1,626,351	6,151,777	0		$8,469,783
7.	Reimbursements							$0
8.	Federal Funds							$0
9.	Special Funds							$0
10.	Grant Funds							$0
11.	Other Funds--Motor Vehicle Account		0	632,674	2,315,547			$2,948,221
12.	PROJECT BUDGET	$0	$691,655	$2,259,025	$8,467,324	$0		$11,418,004

PROJECT FINANCIAL BENEFITS

13.	Cost Savings/Avoidances							$0
14.	Revenue Increase							$0

Note: The totals in Item 4 and Item 12 must have the same cost estimate.

Additional Information: Redirected Division Funding Source

Division(s) Funding the One-Time Costs:	
Division(s) Funding the Continuing Costs:	

INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION E: VENDOR PROJECT BUDGET

Vendor Cost for FSR Development (if applicable)	$154,525
Vendor Name	Business Advantage Consulting

Project #	
PCAS	**DOF**
05-533	
Doc. Type	FSR

VENDOR PROJECT BUDGET

1.	**Fiscal Year**	2005/06	2006/07	2007/08	2008/09	2009/10	00/01	**TOTAL**
2.	**Primary Vendor Budget**			1,041,997	8,335,971			$9,377,968
3.	**Independent Oversight Budget**		0	147,054				$147,054
4.	**IV&V Budget**		0	73,971				$73,971
5.	**Other Contract Services Budget - DGS**		80,000	0				$80,000
6.	**TOTAL VENDOR BUDGET**	**$0**	**$80,000**	**$1,263,022**	**$8,335,971**	**$0**	**$0**	**$9,678,993**

(Applies to SPR only)

PRIMARY VENDOR HISTORY SPECIFIC TO THIS PROJECT

7.	**Primary Vendor**	
8.	**Contract Start Date**	
9.	**Contract End Date (projected)**	
10.	**Amount**	$

PRIMARY VENDOR CONTACTS

	Vendor	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-Mail
11.									
12.									
13.									

INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION F: RISK ASSESSMENT INFORMATION

Project #	
PCAS	**DOF**
Doc. Type	FSR

RISK ASSESSMENT

	Yes	No
Has a Risk Management Plan been developed for this project?	X	

General Comment(s)
The risk management plan is contained in Section 7 of this document.

3. Business Case

3.1. Program Background

One of the Department of Motor Vehicles' (DMV) primary responsibilities is to grant driving privileges to California residents by issuing a California driver license (DL) card to individuals who demonstrate the ability to safely operate a motor vehicle. DMV is also responsible for issuing personal identification (ID) cards, monitoring driving privileges, and taking sanctions against drivers for traffic safety related incidents, such as driving under the influence or failure to provide proof of insurance at the time of an accident. The Department also issues the salesperson (SP) license following a similar but slightly different process from the DL and ID cards.

The production of the DL/ID/SP card is an integral component of the driver licensing program. Although the original intent of DL is to grant driving privileges, the DL/ID card is also considered an individual's primary identification document. As such, the State must ensure the accuracy and integrity of the card, the issuance process, and the related database systems. More than eight million DL/ID cards are produced annually[1] and currently there are about 22.8 million DL and 3.6 million ID cards in use in California.[2] In addition, approximately 62,000 SP cards are produced annually.[3]

3.1.1. DMV Overview

The DMV is part of the Business, Transportation and Housing Agency, and has over 8,200 employees, under seven executive offices and nine divisions reporting to the Directorate. The executive offices provide support to the Directorate as well as oversight and assistance to programs across divisions. Multiple divisions have responsibilities for various aspects of the DL/ID/SP processes. These divisions as well as the offices with key DL/ID/SP oversight responsibilities are highlighted (and appear lighter) in the figure that follows. The responsibilities of each office and division are described in the text that follows the diagram.

[1] 2006/07 Workload Indicators for Budget Estimates, Part 1, Table 2, September 14, 2005, p. 14.

[2] DMV Instant Speechmaker No. 3a, California DMV Statistics, January 1, 2005. These numbers include nearly 2 million people who hold both a DL and an ID card.

[3] Ad Hoc OL Workload Data Report FY 2004-05, September 2005.

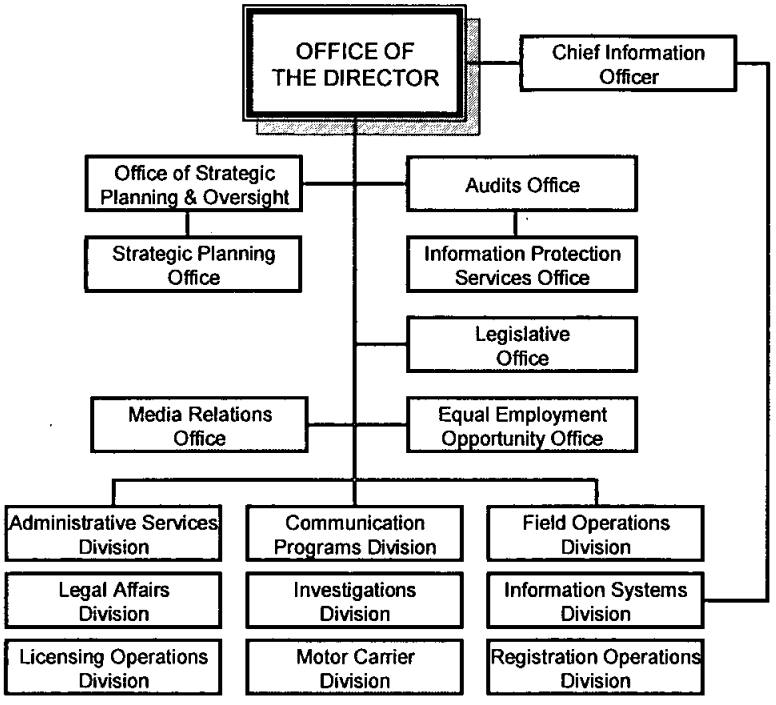


Figure 3-1. DMV Organization Chart

Information Protection Services Office

- Ensures that proper technology and administrative security measures are used to protect the integrity, confidentiality, and availability of DMV's information assets, whether they are electronically stored or hard copy documents.

Strategic Planning Office

- Serves as enterprise planning advisor to the Directorate and deputy directors.
- Provides support for project management, business process improvement, and organizational effectiveness.

Administrative Services Division

- Pays the vendor for the production of the DL/ID/SP cards.
- Prepares DL/ID cards for mailing.
- Provides training.
- Coordinates facility modifications such as power and cabling.

Communication Programs Division

- Provides retrieved image of applicant's record to authorized requestors.
- Develops appropriate memos for field office.

- Provides card issuance information and record status to authorized law enforcement representatives.

Field Operations Division

- Acts as liaison with all field offices.
- Ensures ongoing training needs are met.
- Operates the vendor Video Capture Station (VCS) equipment and reports any problems.
  - Collects applicant's photo, fingerprint, and signature.
- Processes all original DL/ID/SP card applications.
  - Reviews applicant's documents for authenticity.
  - Enters applicant data into DMV system.
- Collects fees.
- Tests drivers.
- Issues temporary and interim driver licenses.

Investigations Division

- Reviews requirements to ensure security needs for the card production site, and transport and storage of card materials are met.
- Provides expert assistance regarding security features relating to the DL/ID Card.
- Investigates possible fraudulent applications and counterfeit licenses.

Information Systems Division

- Provides information technology assistance for the DMV systems, including secure network communications with the vendor system.

Licensing Operations Division

- Administers the DL/ID/SP card contract including any amendments or upgrades during the life of the contract.
- Prepares programming service change requests for the DMV system to interface with changes in the vendor system.
- Implements new legislation that impacts the production of the DL/ID/SP card.
- Reviews applications and determines eligibility for all salesperson licenses.
- Performs quality check before daily mailing of the DL/ID/SP cards.
- Combines or separates records, as the case may be, to ensure accuracy.
- Administers the DL/ID renewal by mail and Internet programs.

Registration Operations Division

- Processes the DL Renewals by Mail through its Remittance Processing System.
- Interfaces with field offices, courts, other State agencies, financial institutions, dealers, and the public about issues relating to the vehicle or vessel programs.

3.1.2. The Current DL/ID/SP Contract

3.1.2.1 Procurement History

In May 1994, DMV released a Request for Proposal (RFP) to identify vendors interested in providing DL/ID/SP cards for the State of California. During the RFP process, vendors were required to submit bids which were analyzed by an evaluation and selection team. In May of 1995, following a thorough and complete evaluation of all proposals received, the Department of General Services (DGS) issued an "Intent to Award" notice to the Polaroid Corporation. The incumbent vendor immediately submitted a challenge to the Board of Control, which heard arguments from all involved parties. Ultimately, the Board of Control rendered its decision, which resulted in the signing of a six-year contract with the Polaroid Corporation in October 1995.

Displeased with the Board of Control's decision, an appeal to the Sacramento Superior Court was filed by the incumbent vendor. In June 1996, the decision from the Sacramento Superior Court found there was disqualifying conflict of interest in the bid process and entered a court injunction against the State from continuing to work on the DL/ID/SP project with Polaroid. The State appealed the Superior Court's decision, and on December 23, 1997, the Third District Court of Appeals issued a decision reversing the Sacramento Superior Court's decision by finding there was no disqualifying conflict of interest. However, this decision was again appealed, yet ultimately rejected by the California Supreme Court.

On March 23, 1998, the Superior Court entered into the record an order denying the writ and preliminary injunction, allowing the State to initiate DL/ID/SP project implementation with Polaroid. In July 1999, the DL/ID/SP project was implemented statewide. On December 3, 2001, Digimarc Corporation purchased Polaroid's ID Systems division and assumed all responsibilities of the Polaroid contract. Digimarc Corporation is the current DL/ID/SP card contractor.

The delayed implementation of the DL/ID/SP project necessitated an extension of the contract until July 15, 2004. The exercise of two optional one-year extensions moved the contract end date to June 30, 2006. An additional extension has been granted through

June 30, 2008 to allow sufficient time for control agency approvals, procurement of a new contract, and implementation.

3.1.2.2 Services Under the Contract

At a high level, Digimarc provides the following services under the current contract:

- Interfaces with DMV systems to receive requests for photo, fingerprint, signature, and card issuance.
- Provides workstation and video capture station equipment (camera, personal computer, signature collection, and fingerprint collection device) at all DMV field offices and headquarters.
- Maintains all current and historical digital images (fingerprint, photo, and signature).
- Maintains data at a backup hot site where the images can also be retrieved by law enforcement.
- Produces DL/ID/SP cards.
- Delivers cards to DMV HQ for quality assurance.
- Reproduces cards that fail the quality assurance process.
- Produces operational reports.

The Card Image Database System (CIDS) is managed and maintained by Digimarc and contains more than 100 million image records (photographs, fingerprints, and signatures). The image database is kept separate from DMV's DL/ID card record database. For the purpose of database management, DL/ID data is purged five years after the license or identification expires and there is no activity for the record. Salesperson records are purged three years following expiration and there is no activity for the record. Although the data in the CIDS belongs to DMV, the system hardware and software used to capture and store image records, beginning with the DL/ID application and continuing through to the actual card production, are owned by Digimarc. Consequently, once the current DL/ID card contract expires, existing equipment will no longer be available to the DMV for the production of DL/ID/SP cards.

Under the current contract which expires June 2008, the DL/ID/SP card contractor charges the Department $0.65 plus 7.75 percent tax for each DL/ID/SP card produced.

3.1.3. DL/ID/SP Program

There are 168 field offices, located throughout California, where DMV employees verify the identity of DL and ID card applicants, test and issue licenses to qualified drivers, and issue identification cards. The "life-cycle" of the DL/ID process includes:

- Issuing driver licenses and personal ID cards;
- Monitoring driving privileges; and,
- Taking sanctions against drivers for traffic safety related incidents, such as driving under the influence or failure to provide proof of insurance at the time of an accident.

During Fiscal Year (FY) 2004-05 approximately 8.5 million DL/ID/SP cards were issued in response to the 8.6 million applications received. The applications processed by headquarters (HQ) and field office staff for FY 2004-05 are detailed in Table 3-1 below.

Table 3-1. DMV DL/ID/SP Application Activity for FY 2004-05

DL/ID Applications Completed	Volume[4]
DL Applications	
Original	818,671
Renewal	2,355,543
Renewal by Mail	2,328,173
Duplicate (Replacement)	1,025,189
Corrections	68,079
Name Change	375,777
Renewal by Internet	312,833[5]
Totals	**7,284,265**
ID Applications	
Original	632,357
Renewal	667,831
Correction	28,577
Totals	**1,328,765**
Total for all DL/ID Cards	**8,613,030**

To legally operate a motor vehicle in the state, all California drivers must obtain a DL card or an instruction permit. DL cards are now renewed every five years. ID cards are issued to California residents needing an identification card. Identification card holders under 62 renew their cards every six years; those 62 years and older renew their ID card every 10 years. All vehicle salespeople in California are required to obtain an SP card. A vehicle salesperson is any person selling vehicles or contracts regarding vehicles or supervising the sale of vehicles or contracts for a dealer. The SP card must be renewed every three years.

[4] 2006/07 Workload Indicators for Budget Estimates, Part I, Table 2, September 14, 2005, pp. 9-13.

[5] This number is broken out from Renewal by Mail.

Because nearly every Californian interacts with the DMV during the course of a year, the efficiency and effectiveness with which the DMV performs its duties have a significant influence on citizens' perceptions of State government. One of those duties is ensuring the integrity of the DMV-issued cards as a form of identification. The California DL is recognized as a primary form of identification. Besides conveying evidence of one's driving privilege, the California DL is commonly used to cash checks, secure credit, obtain social services, register to vote, and perform various other financial, governmental, and legal transactions that require evidence of one's identity. It is therefore essential that the integrity of the license as a positive form of identification be protected. The DMV must ensure the accuracy and integrity of its data and documents.

3.1.3.1 Legal Requirements

DMV is legally charged with safeguarding DL/ID cards against fraudulent activities. Various sections of the California Vehicle Code (CVC) speak of true full name, address, social security number, legal presence and other information aimed at verifying the identity of an applicant for a DL/ID Card. CVC section 12511 requires that "No person shall have in his or her possession or otherwise under his or her control more than one driver's license." Various other CVC sections (e.g., 12805g/h, 12807, 12809, and 13000.1a) mandate that a DL or ID Card not be issued or renewed if a situation negates entitlement. Additional CVC sections require the surrender (13362) or refusal to issue or renew (13369a) if a card has been erroneously issued or falsely obtained.

The federal legislation known as the REAL ID Act (HR 1268), which became public law on May 11, 2005, was enacted to bolster the integrity of the driver license as a form of valid identification. It requires that by May 2008 states comply with minimum standards for issuing DL and ID cards if they are to be recognized as a legal form of identification for federal purposes, such as boarding an airplane. Otherwise, the card must clearly state "on its face that it may not be acceptable by any Federal agency for federal identification or any other official purpose; and" use "a unique design or color indicator to alert Federal agency or law enforcement personnel that it may not be accepted...."[6] This bill is not a federal mandate for the states, but does impact the states' cardholders who depend on the DL/ID card for federal identification purposes. States are anticipating clarifying federal regulations before they can implement all of the legislation's provisions. The legislation has many requirements beyond the scope of this report. California is compliant with many of the provisions of the Act. The following are excerpts of those requirements:

[6] Title II, Section 202 of HR 1268 (enrolled) found at: http://thomas.loc.gov/cgi-bin/query/F?c109:9:./temp/~c109nDZ6Z8:e238497:

> ...a State shall include, at a minimum, the following information and features on each driver's license and identification card issued to a person by the State:
>
> ...(5) A digital photograph of the person....
> (7) The person's signature.
> (8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes.
> (9) A common machine-readable technology, with defined minimum data elements.
>
> ...a State shall adopt the following practices in the issuance of drivers' licenses and identification cards:
>
> (1) Employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format....
> (3) Subject each person applying for a driver's license or identification card to mandatory facial image capture.
> (4) Establish an effective procedure to confirm or verify a renewing applicant's information....

3.1.3.2 Driver License Agreement

The mobility of the driving population and the commitment to strengthen the DL's role for identity verification led California to join most of the other 49 states and Canada to cooperatively develop a DL agreement known as the DL Compact (DLC). Since 1963, California has been a member of the Compact which is recognized legally under the California Vehicle Code Division 6, Chapter 6, Sections 15000, et seq. The DLC provides an arrangement between participating states for compliance with laws, ordinances, and administrative rules and regulations relating to the operation of motor vehicles in each jurisdiction. Specifically, the DLC allows record sharing among states, facilitates reciprocity, and promotes uniformity.

A contributing member of the DLC is the American Association of Motor Vehicle Administrators (AAMVA). "Founded in 1933, AAMVA is a voluntary, non-profit, tax exempt educational organization" which "represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws." AAMVA's programs are intended to encourage uniformity and reciprocity among the states and provinces. The association believes DL/ID security will help increase national security, increase highway safety, reduce fraud and system abuse, increase effectiveness, and achieve uniformity of processes and practices.[7] The implementation of the U.S. Commercial Motor Vehicle Safety Act of 1986 required minimum national

[7] http://www.aamva.org/Documents/std2005DL-IDCardSpecV2FINAL.pdf.

standards for the testing and licensing of commercial motor vehicle drivers. It also made it illegal for an individual to obtain more than one commercial driver license. Prior to the Act, individuals were readily able to obtain driving privileges in multiple jurisdictions. Since then (particularly given the events of September 11, 2001) and with considerable help from DLC members, law enforcement agencies, and stakeholder communities, AAMVA has developed a DL/ID security framework, which serves as a guide for achieving a common security protocol (one identity, one license, one driver control record) among motor vehicle agencies.

In June 2005 the Driver License Agreement was adopted by the states and it referenced several specifications, including the Personal Identification—AAMVA International Specification—DL/ID Card Design, Version 2, March 2005.[8] These standards encourage consistency in adherence to specifications, many already followed by California. They also provide guidance on minimum security features, recommending both overt and covert card security features. With these standards, AAMVA recognized the need for flexibility and a targeted approach by state authorities in selecting card security features most appropriate to the needs of the individual state. To help states select security features, the 2005 standards include an index or list to be used as a guideline for discussions about security feature selection. This index can be found in Appendix B.

3.1.3.3 State Efforts to Address DL/ID Card Integrity

To meet the State's responsibility of ensuring a strong identity verification system, efforts have been made to evaluate current programs and the potential for leveraging technology. The DMV is committed to effective identity verification through its role as issuer of DL/ID cards. The Department recognizes the need to address security issues in order to protect the public, prevent fraud, and guard against identity theft. Solutions to security issues include the reduction of risk through use of technological advances to verify identity, validate the integrity of source documents, and create audit trails of internal processes to prevent employee malfeasance.

In October 2004, the Business, Transportation and Housing Agency hosted a Biometrics Policy Review Committee at which industry leaders, federal and state officials, members of the academic community, and other stakeholders met to discuss using biometric technology to strengthen identification and verification in California's driver licensing program. Biometrics are defined as automated methods of recognizing a person based

[8] AAMVA Uniform ID Subcommittee, Personal Identification—AAMVA International Specification—DL/ID Card Design, March 2005.

on physiological or behavioral characteristics. The characteristics include facial, fingerprint, handwriting, iris, retinal, vein, and voice.[9]

In February 2005, a Steering Committee and Task Force were established to further explore and make recommendations on the critical policy issues surrounding identity and privacy protection. The Steering Committee and Task Force members identified the issues in securing personal identity and protecting privacy, researched various biometric technologies, held discussions with stakeholders, and determined the practical uses and feasibility of a biometrics identification solution for the State of California. As a result, the following primary recommendations were made:

- Establish an electronic verification process for breeder documents. Breeder documents are existing identity documents used for creating new identity documents. This recommendation will be fully addressed outside the scope of this FSR.
- Implement a robust biometric identity system that will be built on proven technology and best practices, including fingerprint and facial recognition biometrics.
- Issue state-of-the-art driver licenses and identification cards to meet the challenge of providing Californians with a secure identity document.

3.2. Business Problem or Opportunity

The DMV is responsible for providing the 35.9 million[10] residents of California with secure, accurate and valid DL/ID/SP cards. Currently, more than eight million cards per year[11] (with a total 22.8 million DL and 3.6 million ID cards in circulation) are issued by Digimarc Corporation. After multiple extensions, the contract with Digimarc is due to expire by June 30, 2008. As a result, the following problems must be addressed:

1. **DL/ID/SP card contract expiration.** The expiration of the contract means that DMV must plan a method by which cards will be issued after June 30, 2008.
2. **Fingerprint and photo comparisons are made manually.** Although DMV currently captures digital fingerprint and facial photos, comparisons to existing records are an entirely manual process.
3. **Current contract does not comply with recently issued AAMVA standards.** Since the AAMVA standards have now been finalized and issued, a new DL/ID card should meet or exceed the minimum security features established by AAMVA.

---

[9] Biometrics Consortium found at www.biometrics.org/html/introduction.html.

[10] U.S. Census Bureau 2004 estimate found at http://quickfacts.census.gov/qfd/states/06000.html.

[11] 2006/07 Workload Indicators for Budget Estimates, Part 1, Table 2, September 14, 2005, p. 14.

4. **Digital images of identity source documents are not captured.** The REAL ID Act requires that DMV capture and store digital images of identity source documents for all new and renewing DL/ID card holders starting in May 2008. An infrastructure must be established to comply with this requirement.

The following sections describe and discuss these issues in further detail.

3.2.1. Driver License/Identification/Salesperson Card Contract Expiration

The contract to produce California's DL/ID/SP cards was scheduled to expire June 30, 2006. Due to the amount of time required to install a system, this deadline would have required that a new contract be in place by June 30, 2005. Since it was impossible to accomplish this, the DMV obtained approval to extend the existing contract for two years through June 30, 2008. This allows just enough time to gain approval for the project, procure the new contract, and install the solution.

As stipulated in the current DL/ID/SP contract, all necessary equipment including computer hardware and software were purchased and installed by the contractor in conformance with the business requirements developed in 1994. The equipment currently used has outlived its useful life and is quickly approaching obsolescence. Since DMV does not own any of the equipment to produce DL/ID/SP cards, Digimarc will retain the equipment upon contract expiration, leaving DMV with no mechanism to continue producing the DL/ID/SP cards. As a result, the DMV must establish another contract or method to produce the DL/ID/SP cards. The new contract must be awarded a minimum of one year prior to the extended contract expiration date in order to:

- Facilitate the conversion of the DMV database records to a new Card Image Database System (CIDS);
- Develop a card format that meets requirements;
- Establish a platform for digitizing identity source documents; and,
- Ensure a seamless transition upon conclusion of the current contract.

The expiration of the current contract provides DMV the opportunity to utilize up-to-date technology in order to produce a secure DL/ID/SP card with all required features.

3.2.2. Manual Fingerprint and Photo Image Comparisons

3.2.2.1 DMV's Responsibilities Under the California Vehicle Code

The DMV is responsible for protecting the public interest and promoting public safety on California's roads and highways by issuing driver licenses. Additionally, the Department licenses and regulates vehicle-related businesses such as automobile dealers and

salespeople. The driver license is now the identification document of choice throughout the State and North America. With a photo, signature, and physical description, the driver license assumes a role beyond its original purpose of identifying a licensed driver. The DL/ID is now readily accepted as an official identification document for both licensed drivers, and, in most jurisdictions, for non-drivers.

The California Vehicle Code (CVC) requires that for every application to obtain an original or a renewed driver license, DMV obtain the following:

(a) The applicant's true full name, age, sex, mailing address, residence address, and social security account number.

(b) A brief description of the applicant for the purpose of identification.

(c) A legible print of the thumb or finger of the applicant.

(d) The type of motor vehicle or combination of vehicles the applicant desires to operate.

(e) Whether the applicant has ever previously been licensed as a driver and, if so, when and in what state or country and whether or not the license has been suspended or revoked and, if so, the date of and reason for the suspension or revocation.

(f) Whether the applicant has ever previously been refused a driver's license in this state and, if so, the date of and the reason for the refusal.

For ID cards, the CVC also requires the DMV to obtain the information in bullets a, b, and c, cited above for driver licenses. In addition, several code sections require that a DL not be issued to an individual under certain conditions, such as those outlined in Sections 12800.7 and 12805 through 12809. To verify those conditions, DMV must be able to verify the identity of the applicant. The following Sections relate to verification of an applicant's identity:

12800.7. Upon application for an original or duplicate license the department may require the applicant to produce any identification that it determines is necessary in order to ensure that the name of the applicant stated in the application is his or her true, full name....

13000.1. (a) The department may refuse to issue or renew an identification card to any person for any of the following reasons:

(1) The department determines that the person has knowingly used a false or fictitious name in any application.

(2) The department determines that the person has impersonated another in making an application.

(3) The department determines that the person has knowingly made a false statement, knowingly concealed a material fact, or otherwise committed any fraud on any application.

Under the CVC, DMV's goal is to ensure an individual has only one license, one identity, and one record. The DMV must take appropriate action to safeguard Californians from fraud and identity theft while maintaining the highest security standards to protect its information systems. However, DMV has no automated means to enable full compliance with its responsibility to verify that an applicant is who they claim to be based on DMV records. Photo comparisons are conducted manually by field office technicians comparing the photo image on the database to the applicant in the field office. Image comparisons are also performed by the Investigations staff when fraud is suspected.

3.2.2.2 Identity Theft Fraud in California

The incidence of identity theft continues to rise in California. In 2004, the Federal Trade Commission (FTC) reported that there were 43,839 identity theft victims in California. This represents a 42 percent increase in two years from the 30,738 cases documented in 2002. Also, the rate of fraud and identity theft using a DL/ID in California was slightly higher than in other states.[12] Of the total number of victims in California, 1,052 incidents were related to DL fraud or forgery. As an example, in a recent case, Canoga Park investigators arrested a man who had in his possession driver licenses with his photo and various names and dates of birth. He was obtaining credit using a victim's identity.[13]

how attributable to this + new card should reduce or eliminate

Another example of this kind of fraud was reported on July 1, 2003 by a local television station in Palm Springs, California.[14] A counterfeit operation was discovered where computers, scanners, a laminator, copy machines and countless fake identification cards, including driver licenses, passports, and birth certificates were found. San Bernardino sheriff's deputies also found a list of identification numbers and addresses for use from stolen checkbooks. The driver licenses were being scanned, the buyer's picture taken, and someone else's stolen identification information placed in the name and address fields.

Driver license fraud is a significant problem for law enforcement because it makes it harder to detect and deter crimes. False identification provides opportunity for other criminal activity such as bank, credit card, and welfare fraud. Innocent victims whose identities were stolen can be falsely arrested while a criminal has concealed his or her identity. Driver license fraud has a significant impact on citizens because it increases the cost of consumer products and services and can destroy an innocent victim's credit.

---

[12] Federal Trade Commission, Identity Theft Victim Complaint Data, Figures and Trends in California, January 1–December 31, 2004.

[13] Media Relations Office, Department of Motor Vehicles, The Spirit, September 2005, p. 5.

[14] KESQ News Channel 3, Palm Springs, Counterfeit driver's license operation busted in Morongo Valley, July 1, 2003. Article found at http://www.kesq.com/Global/story.asp?S=1384496.

The DMV opened 67 cases in 2000 related to counterfeit licenses. This number dramatically increased to 230 in 2003. This is in large part due to the fact that fraud increases as criminals become familiar with the security features and processes followed to verify identity and issue a DL/ID. The DMV expects a new license format to help deter identity theft.

Unfortunately, the value and importance of the California DL have made it a popular target for fraud. California's workload, with 24 million residents holding a DL or ID card,[15] along with the pressure to provide better and quicker customer service make it quite challenging to verify identity using a manual image comparison process. The process is inefficient and impractical, making it difficult to deter fraud.

A major weakness in the DMV's ability to crack down on identity fraud is that it cannot use the fingerprint images it collects to verify the identity of DL/ID applicants at the time they are in the field offices. Additionally, DMV does not have a system to perform comparisons of an applicant's photo to other photos on file to ensure applicants are who they claim to be.

An additional weakness in the DMV's ability to prevent fraud is a restricted ability to create effective audit trails for employee feedback, training and fraud prevention purposes. For example, employees using the Video Capture Station to take a photo sign in to the system using a generic rather than individual system user identification. This makes it difficult to provide constructive feedback when errors are made or to mitigate the risk of employee fraud.

3.2.3. American Association of Motor Vehicle Administrators Security Standards[16]

The AAMVA strives to develop model programs in motor vehicle administration, police traffic services and highway safety. The association serves as an information clearinghouse for these same disciplines, and acts as the international spokesman for these interests.

The proliferation in domestic and international crime, coupled with identity fraud, have led to increasing concerns over the security of driver licenses as well as all other kinds of personal identification documents and what may be done to help safeguard them from

[15] Net total persons issued a DL or ID card as of January 1, 2005, as shown in the DMV Instant Speechmaker No. 3a. This number excludes nearly two million cards for holders of both a DL and an ID card.

[16] http://www.aamva.org/Documents/std2005DL-IDCardSpecV2FINAL.pdf.

misuse. The DL/ID is one of the most commonly used forms of identification in North America and therefore a target for counterfeiting.

The AAMVA International Specification - DL/ID Card Design (Version 2, March 2005) was developed as one part of an extensive program to improve the security of the DL/ID card. AAMVA encourages uniformity and reciprocity among the states and provinces, and works collaboratively with other levels of government and the private sector. Its program development and research activities provide guidelines for more effective public service. Additionally, AAMVA believes ID security helps increase national security, increase highway safety, reduce fraud and system abuse, increase efficiency and effectiveness, and achieve uniformity of processes and practices. Although the AAMVA specification was developed for the production and use of government-issued DL/ID card documents, private institutions and other organizations also benefit from DL/ID uniformity established by the association.

The intent of AAMVA standards is to establish uniformity of features and guidelines for card security while taking advantage of the most recent advances in DL/ID card security technology. The specification provides a comprehensive set of guidelines for security features in the DL/ID card. Jurisdictions that follow this specification will have a common format for the DL/ID card that reduces interstate differences. Additionally, jurisdictions are encouraged to select security features that best address their needs.

A DL/ID is in conformance with the AAMVA International Specification - DL/ID Card Design (Version 2, March 2005) if it meets all specified requirements. Historically, the DMV has typically exceeded AAMVA requirements in all categories such as card design, physical security, DL/ID security device index, card durability, and optional magnetic stripe. Nonetheless, to further ensure protection against fraud, all specifications within each of the five annexes (sections) should be reviewed and determination made for their inclusion in the DL/ID card design. The five annexes in the AAMVA 2005 Standard are:

A – Card Design

B – Physical Security

C – DL/ID Security Device Index

D – Mandatory PDF417 Bar Code

E – Card Durability Test Methods

Presently, the DL/ID card contains various levels of security features, including the State flag in ultra violet ink, a ghost photo, and magnetic stripe. Annex C will be used to identify specific security features to be included in the new DL/ID card. The Annex C

Security Device Index can be found in Appendix B. The solution must include updated overt and covert security features in conformance with AAMVA specifications.

3.2.4. Digital Capture of Identity Source Document

The REAL ID Act (Act) was signed into law on May 11, 2005, and is intended to strengthen the integrity of the driver license and identification card as a form of valid personal identification. The Act attempts to achieve this goal by requiring states to meet certain minimum card issuance standards. In order for a state's driver licenses and personal identification cards to be accepted for federal purposes, such as entering a federal facility or boarding a commercial aircraft, after May 11, 2008, all the standards described in the Act must be fully met.

Implementation of the REAL ID Act presents significant challenges to all states. It will have a major impact on driver licensing and identification card processes. Many of the clarifying details of the provisions have not yet been defined in federal regulations. However, one of the certain requirements under the law is that DMV will be required to capture and store digital images of identity source documents.

The DMV does not currently capture identity source documents as digital images. In fact, the document images the Department does retain (e.g., applications) are captured on microfilm rather than digitally. Compliance with the requirement to capture digital images of identity documents will increase workload and transaction times and should be implemented in such a manner to minimize the impact on customer service. This is especially important in the first five years after May 11, 2008 since federal regulations will likely preclude applicants from renewing by mail or by Internet.

In order for the Department to capture digital images and support the redesigned processes, the DMV must analyze and plan necessary upgrades to its technical environment. Failure to plan for the digital imaging solution in a timely manner significantly increases the risk of California failing to comply with REAL ID regulations by the May 2008 deadline.

3.3. Business Objectives

The following objectives relate to the problem statements outlined above.

3.3.1. Implement a New DL/ID/SP Card Solution

To fully implement a new system to produce DL/ID/SP cards and store and retrieve images and demographics by May 11, 2008:

- Begin development of the new solution by July 2007;
- To reduce implementation risk, begin a phased field office implementation by February 2008;
- Obtain the hardware, software, and materials for a complete system to produce DL/ID/SP cards with information specified in CVC Sections 11802, 12811, and 13005; and,
- Address the need for production of the DL/ID/SP cards, including the capture, storage, use and retrieval of images. (Note: The DMV application processing and support activities are not being changed.)

3.3.2. Improve Ability to Verify Identity of All Applicants

Improving the ability to verify the identity of all applicants, the solution must achieve the following:

- Implement immediate verification that the newly captured fingerprint matches or does not match the existing print on the DL/ID card image database (one to one comparison);
- Implement an efficient objective photo match process whereby an applicant's photo is compared to all photos on file to identify potential identity theft;
- Provide an effective audit trail for internal DMV DL issuance processes; and,
- Reduce the percentage of DL/ID related fraud or identity theft cases.

3.3.3. Comply with AAMVA Standards

To reasonably comply with AAMVA Standards, the solution must:

- Implement tamper-proof cards that reasonably comply with AAMVA card standards;
- As is the case with existing cards, include both overt and covert security features;
- Update security features in order to deter counterfeiting; and,
- Provide at least the same number of security features presently included in the DL/ID/SP cards.

3.3.4. Digitally Capture Identity Source Documents

To comply with the REAL ID Act, the solution must:

- Provide the ability to digitally capture images of identity source documents for all California DL/ID cardholders.
- Capture and store digital images as required by the REAL ID Act and related clarifying federal regulations.
- Minimize service level delays so that the average time to process a transaction in the field office does not exceed 10 minutes for an original application and 8.5 minutes for a renewal.

3.4. Business Functional Requirements

This section presents the key business functional requirements needed to achieve the objectives defined in Section 3.3 above. The following table is a compilation of requirements that satisfy one or more of the project objectives. For purposes of the functional requirements, "Card Image Database System" and "System" are synonymous.

Table 3-2. DL/ID Functional Requirements

Functional Requirements
CHARACTERISTICS
1. Obtain the hardware, software, materials, and resources for a complete system to produce tamper-resistant Driver License, Identification, and Salesperson cards.
2. Provide an intuitive, repeatable, and consistent capture process for field office staff and customers.
3. Capture images in less than 90 seconds at the VCS.
4. Continuously meet all hardware and software requirements throughout the useful life of the solution (or term of a contract). Should equipment fail to meet any requirement, repairs or replacement must be completed as appropriate, within the specified time, and at no extra cost.
5. All field office video capture stations must electronically capture and store images and demographics and transmit them to a DL/ID/SP Card Image Database System, on a real time basis, without affecting the primary function of capturing the applicant's image record.
6. All equipment must meet State ergonomic standards as applicable.
7. The system must comply with Section 508 of the Federal Rehabilitation Act and be accessible by the physically challenged.
8. All field offices must be capable of digitally capturing images of identity source documents.
9. Every VCS must provide the ability to scan and verify identity source documents.
10. Allow for biometric logon for the verifier in order to provide an audit trail.
11. Allow displaying the digitized image at the time of capture in order to assess image quality, adjust, and re-image as needed.
12. Capture and display identity documents in less than 10 seconds.
13. Display requested digitized images within one second.

Functional Requirements
14. Store digitized images at the field office until they are ready to be uploaded to the image repository.
15. Assign a unique identity to each digitized document.
16. Document capture device must fit within or between existing standard workspaces of 24" x 48".
17. Devices must be capable of digitizing documents up to 11" x 17" in size and of varying print qualities.
18. System must be scalable to provide for additional scanners as needed.
CARD PRODUCTION, IMAGE STORAGE & RETRIEVAL
19. Based on expected workload, provide the capability to process at least the following image retrieval requests on a daily basis: a. From Primary Site ▪ 50,000 from the 168 field offices ▪ 5,000 from DMV headquarters b. From Back Up Hot Site ▪ 85,000 from an estimated 5,000 external users such as law enforcement agencies ▪ 10,000 in batch mode
20. Manufacture at least 50,000 cards daily in various Driver License, Identification, or Salesperson combinations.
21. Maintain a secondary database of image records for access by external users.
22. Provide a comprehensive system that includes disaster prevention and recovery which is evaluated and updated at least annually.
23. Conform with regulations pursuant to the REAL ID Act (HR 1268) pertaining to DL/ID/SP card issuance specifications.
24. Maintain storage capacity for at least 35 million Driver License, Identification, and Salesperson records including their associated 200 million-plus images.
25. Produce DL/ID/SP cards with information specified by CVC Sections 11802, 12811 and 13005.
26. Remanufacture previously issued DL/ID/SP cards when necessary.
27. Include at least the number of existing security features (eight overt and covert).
28. Fully archive and maintain throughout the term of the contract all photos, prints, and signatures.
29. Digitized documents must conform to industry standard and federally prescribed image file formats.
STANDARDS
30. Conform to the latest AAMVA, American National Standards Institute (ANSI) and National Institute of Standards and Technology (NIST) standards for the quality, capture, compression, decompression, transmission, storage, and retrieval of images. At the State's discretion, implement any subsequent standards throughout the contract period.

Functional Requirements
31. In the absence of ANSI or NIST standards, proprietary algorithms and software may be used for an automated comparison process.
32. Produce DL/ID cards conforming to AAMVA specifications. Current reference - Personal Identification—AAMVA International Specification—DL/ID Card Design, March 2005.
33. Adhere to Federal Information Security Management Act (FISMA) guidelines for analysis, design, development, and implementation of systems that may exchange protected information with federal systems.
34. Conform to the latest NIST standards for security, encryption, testing, and management as defined by the NIST-Computer Security Division.
35. Adhere to Information Technology Code of Practice for information security management and best practices as defined by the International Standards Organization (ISO) publication 17,799.
DATABASE FUNCTIONALITY
36. System must be fully operational 99.98% of the time between 7 AM to 7 PM.
37. System must be fully operational 99.6% of the time 24 hours per day, 7 days per week, 52 weeks a year (24/7/52) operation.
38. System maintenance must be done during non-working hours (e.g., 12:00 a.m. - 4:00 a.m.).
39. Store all DL/ID/SP card records (images and corresponding demographic data including customer information) for the life of the solution. This includes transferring all records from the existing Card Image Database System to the new database.
40. To authorize release of the image, retrievals from internal and external DMV requesters must use the existing inquiry program to query the DL Master File Record.
41. System must be capable of annotating or flagging a DL/ID Card Image Database record as requested by the Department.
42. System must return confirmation to the VCS upon receipt of the customer's information (images and demographics) and, in turn, the VCS must send confirmation to the DMV application server upon receipt or non-receipt of same information.
43. System must electronically receive card request data from the DMV system before a card is produced.
44. System must merge the card request data with the corresponding images.
45. Digitized documents must be linked to a unique identifier and be selectable for validation at the field office prior to permanent storage.
46. Prevent digitized images from being altered, manipulated, or degraded from their captured form.
47. Provide a means for updating DMV records upon successful digitizing of the identity source documents.
48. Unusable image files must be removed from the production system.
REPORTS
49. Generate production statistical reports on a regular basis and as specified by DMV.
50. Provide reports by individual video capture station as necessary and upon request.

Functional Requirements
51. Generate detailed reports that provide an audit trail of trends and anomalies. These reports will aid DMV investigators to address employee and customer fraud.
SECURITY
52. Provide guaranteed effective data and image access control to protect the privacy of customer information.
53. Allow assignment of users to roles (e.g., administrator, manager, user).
54. Allow assignment of users to user groups (e.g., field office representative, Investigators, management).
55. Meet or exceed security policies and requirements as defined in the DMV Information Security Manual and Security requirements for e-Government.
56. Provide state-of-the-art features to protect against alterations, substitutions, and cannibalization by counterfeiters.
57. Include overt and covert security features, as specified by AAMVA standards.
58. Include at least the number of overt and covert security features included in the current DL/ID card (no less than eight).
59. Provide security measures to protect the card production site as well as the transport and storage of card materials.
60. All equipment must comply with DMV, Federal, and ISO guidelines to ensure confidentiality of data.
61. Comply with all security provisions prescribed by the REAL ID Act and related clarifying regulations..
TRAINING
62. Provide training and manuals to Departmental staff involved with image capture, automated comparison, and retrieval processes.
63. Provide training instruction and manuals for any subsequent hardware or software updates.
64. Provide advanced technical support, troubleshooting, and general training including all manuals and updates for DMV's Help Desk staff.
AUTOMATED COMPARISON
65. Provide the hardware and software to receive and compare print images from the Card Image Database System. (Note: current print images are in standardized formats and should not require reformatting to interface with a print comparison process.).
66. Within one second, the system must automatically verify whether the newly captured print matches the most recent image on the database (one to one comparison).
67. Perform system searches based on the applicant's date of birth, height, weight, or other appropriate data.
68. Include image enhancement capability allowing image details to be drawn out or cleaned up.
69. Allow adjustment of match/non-match confidence thresholds for fingerprint and facial recognition comparisons.
70. Provide a "match" or "no match" response to the technician for each print comparison.

Functional Requirements	
	71. "No match" results for one-to-one print comparisons must be reported in a specified timeframe and format.
	72. "No match" results for one-to-one print comparisons must result in a flag for investigation.
	73. "Match" results for one-to-many facial comparisons must result in a flag for investigation.
	74. For applications processed in field offices, one to many matches must be completed within 24 hours of the business day's work; for investigative purposes, they must be completed within 60 seconds.

4. Baseline Analysis

4.1. Current Methods

This section provides an overview of the existing business and technical environment and infrastructure that currently support DMV's issuance and administration of DL/ID/SP cards. Review of existing methods will provide a better context for understanding the problems and opportunities presented previously, supporting the need to implement the proposed solution described in Section 5.

Over the years, DMV has improved systems to manage and administer the DL/ID/SP process beginning with receipt of the customer's application and ending with issuance of a new card. Field office employees serve as the public's primary point of contact with the DMV and, as such, become the conduit for information collection, review, and assurance of data accuracy.

As identified in Table 3-1, in FY 2004-05, the DMV processed and issued over 8.5 million DL/ID/SP cards including:

- Original issuances processed in field offices;
- Renewals in field offices;
- Renewals by mail;
- Renewals by Internet;
- Replacements;
- ID Cards;
- Senior ID Cards; and,
- Corrections and name changes.

The majority of these applications are currently processed at local field offices. The following subsections describe the user interfaces, DL/ID/SP field office issuance/renewal process, the renewal by mail or Internet process, and the systems and services that support these processes.

4.1.1. User Interfaces

The DMV user interfaces for purposes of DL/ID/SP issuance and renewal primarily consist of:

- The Department of Motor Vehicles Automation;

- The Transaction Inventory System;
- Internet;
- Card Image Database System;
- Video Capture Station; and,
- DMV programs that interface with the above.

Department of Motor Vehicles Automation (DMVA) – DMVA is the name given to the application that runs on IBM RS/6000 computers at the DMV. Specifically, it refers to a set of programs written in Event Driven Language (EDL), for the IBM Series/1 computer environment. These EDL programs now operate under emulation on the RS/6000 using the UNIX AIX operating system. DMVA is the application used primarily by DMV field offices to communicate with DMV databases and to obtain data from external entities. DMVA is more than just a user interface or simple application server because much of the business logic for processing DL/ID/SP issuance is maintained within DMVA. The DMVA is installed at 215 sites throughout the State (field offices, satellite offices, business partner locations, and headquarters). There are 325 RS/6000 processors at DMV with a total of 5,775 Neoware terminals, 24 personal computers, and 2,990 printers connected to them.

Transaction Inventory System (TIS) – The TIS is a database that tracks the status of the DL/ID/SP cards after they have been manufactured. Following each batch set of cards produced, the card vendor sends an electronic file (referred to as a TIS file) to DMV headquarters to update the TIS. TIS tracks each card by batch number, card type, and DL/ID/SP number. When cards are sent to DMV headquarters for quality assurance (QA), they are reconciled with TIS. Any cards not passing QA are noted in TIS for remanufacture or retake. Once cards are mailed, the "date mailed" field is updated in the TIS as well as the driver record master (DRM).

The Internet – This user interface is for DMV customers to access general information, print required forms, and initiate selected DMV processes, such as renewing a driver license. The Internet interface allows use of credit cards to pay some DMV fees.

Card Image Database System (CIDS) – Digimarc's CIDS exchanges files and messages with DMV, and houses over 100 million image records (photographs, fingerprints, and signatures). Although the data in the CIDS belongs to DMV, the system hardware/software used to capture and store all image records is owned by the contractor. A web application now allows field office technicians to retrieve applicant photos at their terminal by toggling to a browser.

Video Capture Station – The VCS application software is a disk operating-based system or more commonly known as a DOS-based system. The VCS is connected to DMV's network via RS422 communications and Registered Jack (RJ) 45 Ethernet cables. The Ethernet connection transmits images from the VCS to the DL/ID/SP Card Image Database System and communicates with the DMVA. The VCS is comprised of the following components at each field office:

- Personal computer, keyboard and color monitor;
- Fingerprint capture device;
- Photo capture device (camera);
- Photo receipt printer; and,
- Signature capture device.

DMV Programs – DMV programs process information captured during the application process. The data collected by the field office is processed by DMV systems which determine eligibility and update the driver record. Only after all requirements are met is the remainder of the card demographic information sent to the DL/ID/SP card vendor's system to manufacture the cards. The DMV receives a file from the card vendor indicating the cards have been produced, and updates the Transaction Inventory System. A file is also generated by the vendor for card requests that could not be processed and are returned as "unconfirmed." DMV interfaces with the vendor system to retrieve photos. Photos can be released based on the identity of the requester.

4.1.2. DL/ID Issuance Process

The average system transaction time for an original issuance in the field office is currently seven minutes.[17] A high-level business process flow diagram of the DL/ID field office issuance process is illustrated.

[17] Based on the Production Statistics Detail Report, FY 2004-05. Estimated time added for original issuance to account for visual verification of identity documents.

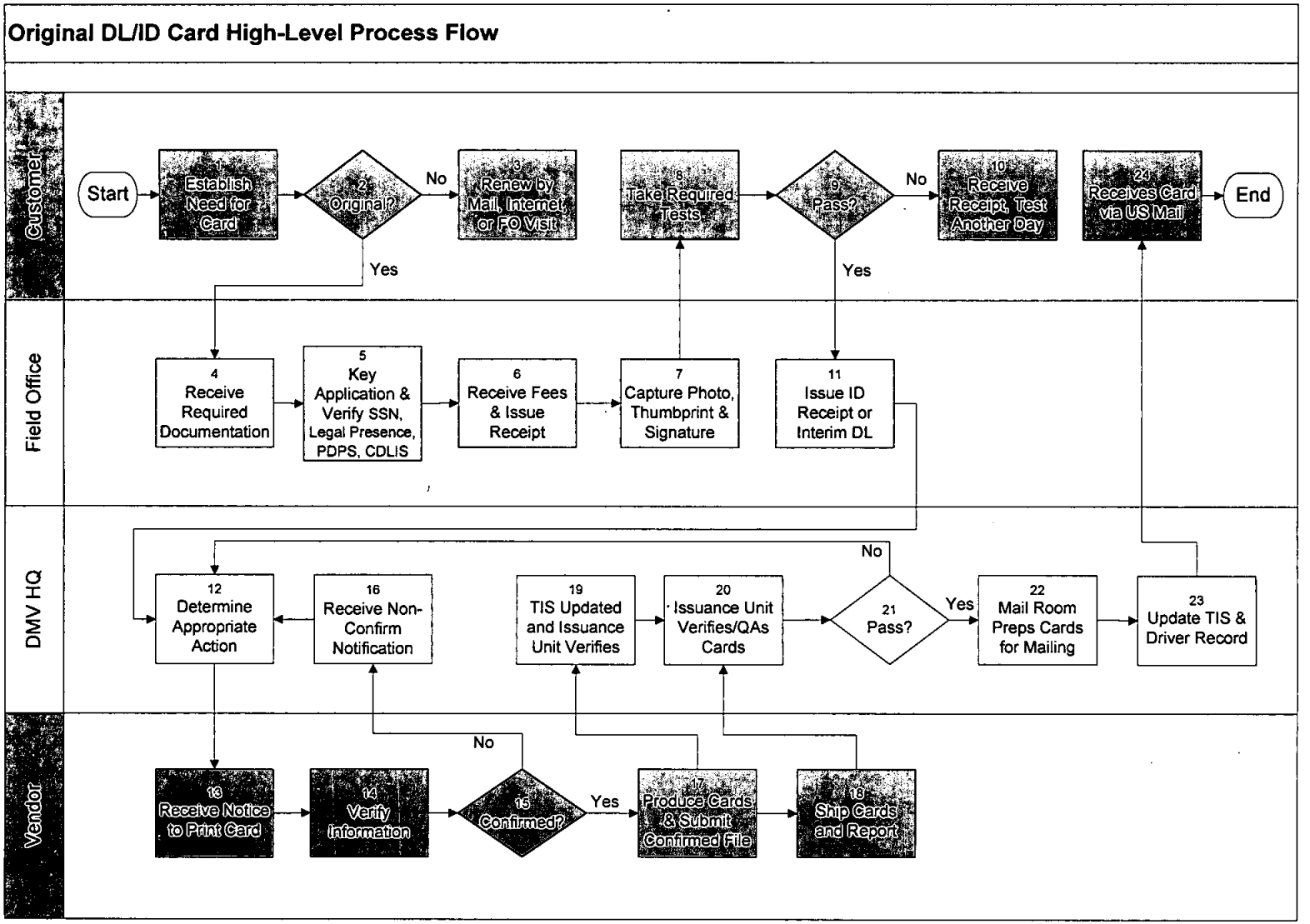


Figure 4-1. Original DL/ID Field Office Issuance Process

The following steps are generally followed to issue a DL/ID card:

1. Customer determines the need for a DL/ID card.
2. If the DL/ID card is an original, (i.e., first issuance) the customer must visit a field office to apply.
3. If the DL/ID card is a renewal and eligibility criteria are met, the customer may renew either by mail, the Internet, or visit a field office (FO).
4. Original DL/ID card customers are required to provide a Birth Date/Legal Presence (BD/LP) document, a Social Security Number, a Driver Training Certificate of Completion or Enrollment, if applicable, an Out of State Driver License, if applicable, and a completed Application for Driver License/Identification Card (DL 44). A commercial driver license applicant must also provide proof of a Social Security Number Card. The FO representative visually verifies the BD/LP documentation. A second, specially trained FO employee also verifies the document. After inspection of the document, both FO employees initial the DL 44 as proof of verification. The DL 44 is sent to DMV HQ to be microfilmed, but an image of the identity source document is not currently captured by DMV. Once assured the DL 44 form is completed correctly, including the True Full Name on the BD/LP document, the customer signs the form and the information is entered into the DMVA system.

   If the document appears to be fraudulent, the FO employee marks the record "FA" (possible fraudulent application) during the key entry of information into the DMVA system. The headquarters Driver License Fraud Analysis Unit investigates the possible fraudulent application when received from the field office. When a question arises about an applicant's identity, headquarters technicians spend time retrieving and comparing photos and thumbprints. There are an average of four image sets per record. It takes headquarters technicians approximately eight minutes to compare two photos or prints visually.

5. During the keying of application information in step 4, a number of electronic verifications are conducted with external systems. The Social Security Number (SSN) submitted by the applicant is electronically verified with the Social Security Administration (SSA). If the record indicates the SSN was previously verified or is a generic substitute, the SSN is not sent for verification. If the SSN is not verified, the applicant is informed to resolve with SSA. If the SSN verification is conducted when the applicant is not in the field office, a letter is generated and sent to the applicant who may then respond by mail, telephone, or visit to a field office to correct the previously submitted information or inform DMV the applicant's SSA record has been updated.

   When applicable, the Problem Driver Pointer System (PDPS) is also accessed to identify a record in another state. If the applicant is applying for a commercial driver license, the Commercial Driver License Information System (CDLIS) is also checked. If a CDLIS response indicates the applicant is not qualified to receive a commercial driver license, the representative cancels the transaction and provides the applicant any relevant information as to why the application cannot be processed. If there is a PDPS response, the customer can continue through the testing phase; however, the licensing document cannot be issued.

6. The representative completes the initial application, collects the fee and issues a receipt to the applicant.
7. The applicant is then sent to the Video Capture Station. Here, the FO representative selects the correct record on the system by using the Daily Application File (DAF) number from the money receipt. The digital signature, thumbprint and photo of the applicant are taken. If any further tests are required, such as a written or driving test, a photo receipt is generated by the VCS and provided to the applicant.
8. The applicant takes applicable tests as required.
9. A FO representative grades the test to determine whether the applicant passed or failed.
10. If the applicant fails the test, the applicant is instructed to return at a later date to retake the test.
11. If the applicant passes the test, they are issued a temporary license or, in the case of an ID card, a receipt only as there is no means of issuing a temporary ID card.
12. DMV headquarters determines the appropriate action to take before a card can be issued. When all updates to the driver record master are successful, a card request is sent electronically to the card production vendor. This data transmission includes the demographic information necessary to produce the card.
13. The card production vendor receives the electronic card request.
14. The card production vendor verifies the request to issue the card.
15. The verification process results in the request being categorized as confirmed or unconfirmed. Confirmed cards can be produced. An unconfirmed request indicates the card could not be produced due to an error condition, not meeting the workload threshold, or a photo not being available. Depending on the condition that resulted in the unconfirmed status, unconfirmed records may continue to cycle for up to 15 days, until confirmed.
16. The vendor notifies DMV headquarters when requests to print cards are unconfirmed. DMV staff determine appropriate action, which may result in customer notification that a photo retake is required.
17. If the request to produce a card is confirmed, the vendor produces the card and electronically submits the confirmed file. The most current image is placed on magnetic storage media and the historical images are written onto optical disks, for future retrieval. Additionally, the card production vendor electronically sends a file of all confirmed cards produced to DMV.
18. The DL/ID cards and a report are delivered to the Issuance Unit (located at DMV headquarters) at 7:15 a.m. daily.
19. The TIS is updated and the Issuance Unit verifies the data for accuracy.
20. The Issuance Unit verifies receipt of the cards and inspects the cards for quality. Any cards with special handling requirements are removed from the batch and processed separately.

21. The Issuance Unit determines whether the cards meet defined quality standards. Cards that do not meet standards are reviewed by DMV staff to determine appropriate action. Acceptable cards are sent to Mail Operations for processing.
22. Mail operations prepares the cards for mailing. By reading the magnetic stripe on the back of the DL/ID card, a machine addresses and attaches a card carrier to the card which is then inserted in an envelope.
23. The TIS and DL record are updated with the status and mailing date.
24. The customer receives the DL/ID card, concluding the process.

4.1.3. DL Renewal by Mail and Internet Processes

The average system transaction time for a renewal in the field office currently approximates 5.5 minutes.[18] DL renewals by mail and the Internet are handled by DMV headquarters. Of the five million driver license renewals, approximately half are processed by mail or Internet. The renewal by Internet program is new and its use is expected to increase, unless restricted by the REAL ID Act and clarifying regulations. Figure 4-2 provides a high-level flow diagram of the DL renewal by mail and Internet processes.

[18] Production Statistics Detail Report, FY 2004-05.

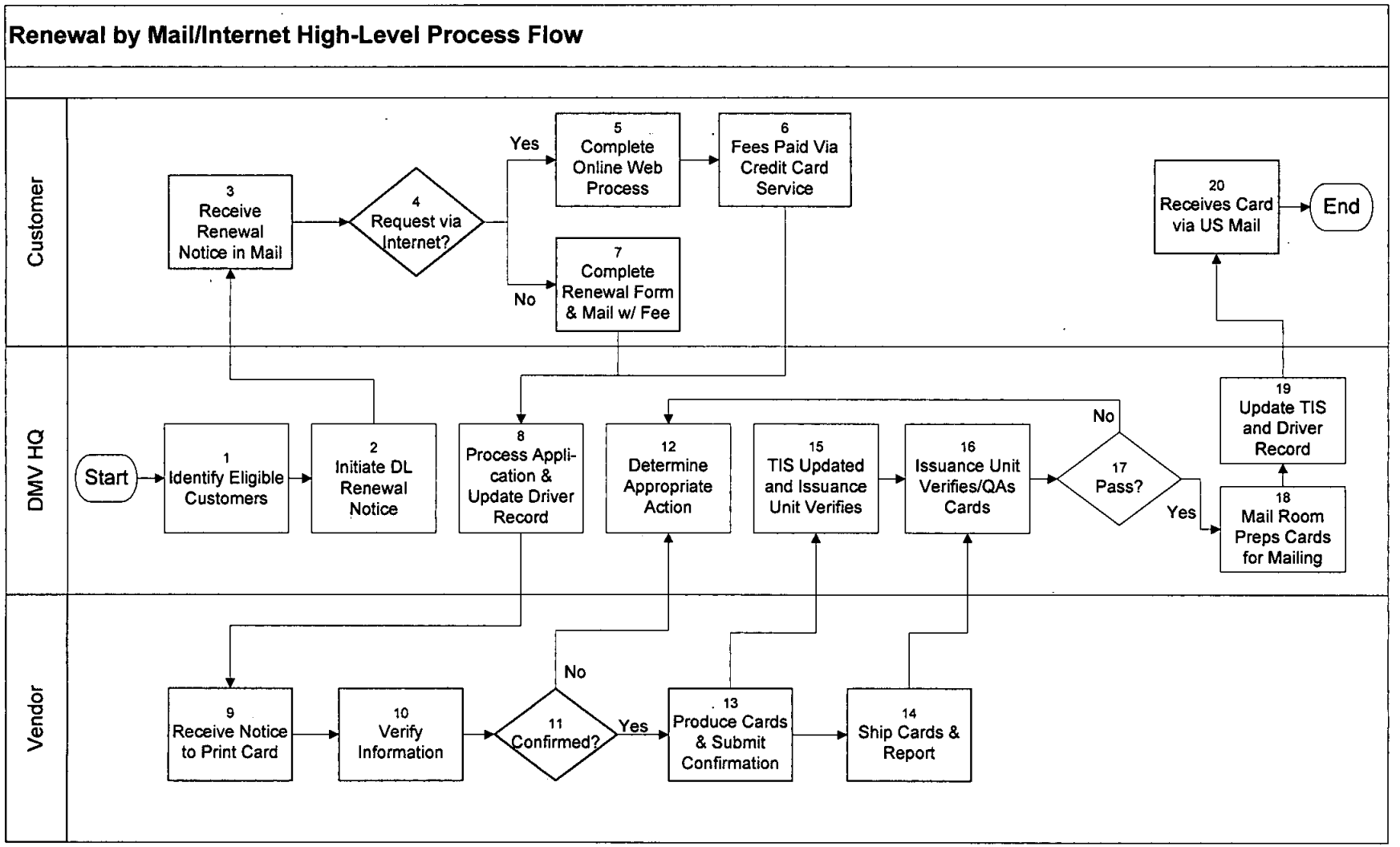


Figure 4-2. DL Renewal By Mail/Internet Process

The following steps are followed to renew DL cards by Internet or by mail:

1. DMV identifies customers who qualify for the DL renewal by mail/Internet process.
2. DMV initiates and mails DL renewal by mail/Internet notifications.
3. Customer receives the DL renewal by mail/Internet notification in the mail.
4. Customer decides whether to renew the DL by visiting the DMV website (www.dmv.ca.gov) or by mail, or by visiting a field office.
5. If renewing by Internet, the customer logs onto the DMV website and completes the renewal application process.
6. During the online DL renewal process, the customer pays the renewal fee by credit card, processed by the credit card service provider.
7. If renewing by mail, the customer completes the renewal form and mails it to DMV HQ along with the appropriate fees.
8. For renewals by mail, a DMV HQ representative processes the application through the Remittance Processing System, which updates the DMV headquarters programs. For renewals by Internet, the headquarters programs are automatically updated. Money is cashiered and balanced, and the driver record master is updated. In addition, an automated notice to print the card is sent electronically to the card production vendor.
9. The vendor receives the electronic notice to produce the cards.
10. The card production vendor verifies the information.
11. The vendor determines whether the request meets the confirmation criteria. A confirmed request indicates the record will be produced into a card. An unconfirmed request generally indicates damaged or missing image data. The unconfirmed record will continue to cycle for up to 15 days, until a match is made.
12. The vendor notifies DMV headquarters when requests to print cards are unconfirmed. DMV staff determine appropriate action, which may result in customer notification that a retake is required.
13. If the request to produce a card is confirmed, the vendor produces the card and electronically submits the confirmed file.
14. The DL/ID cards and a report are delivered to the Issuance Unit (located at DMV headquarters) at 7:15 a.m. daily.
15. The TIS is updated and the Issuance Unit verifies the data for accuracy.
16. The Issuance Unit verifies receipt of the cards and inspects the cards for quality. Any cards with special handling requirements are removed from the batch and processed separately.
17. The Issuance Unit determines whether the cards meet defined quality standards. Cards that do not meet standards are reviewed by DMV staff to determine appropriate action. Acceptable cards are sent to Mail Operations for processing.

18. Mail operations prepares the cards for mailing. By reading the magnetic stripe on the back of the DL/ID card, a machine addresses and attaches a card carrier to the card which is then inserted in an envelope.
19. The TIS and the DL record are updated with the status and mailing date.
20. The customer receives the DL card, concluding the process.

4.1.4. Salesperson License Issuance Process

The SP application process varies somewhat from the DL/ID application process. Figure 4-3 depicts a high-level flow diagram of the SP issuance process.

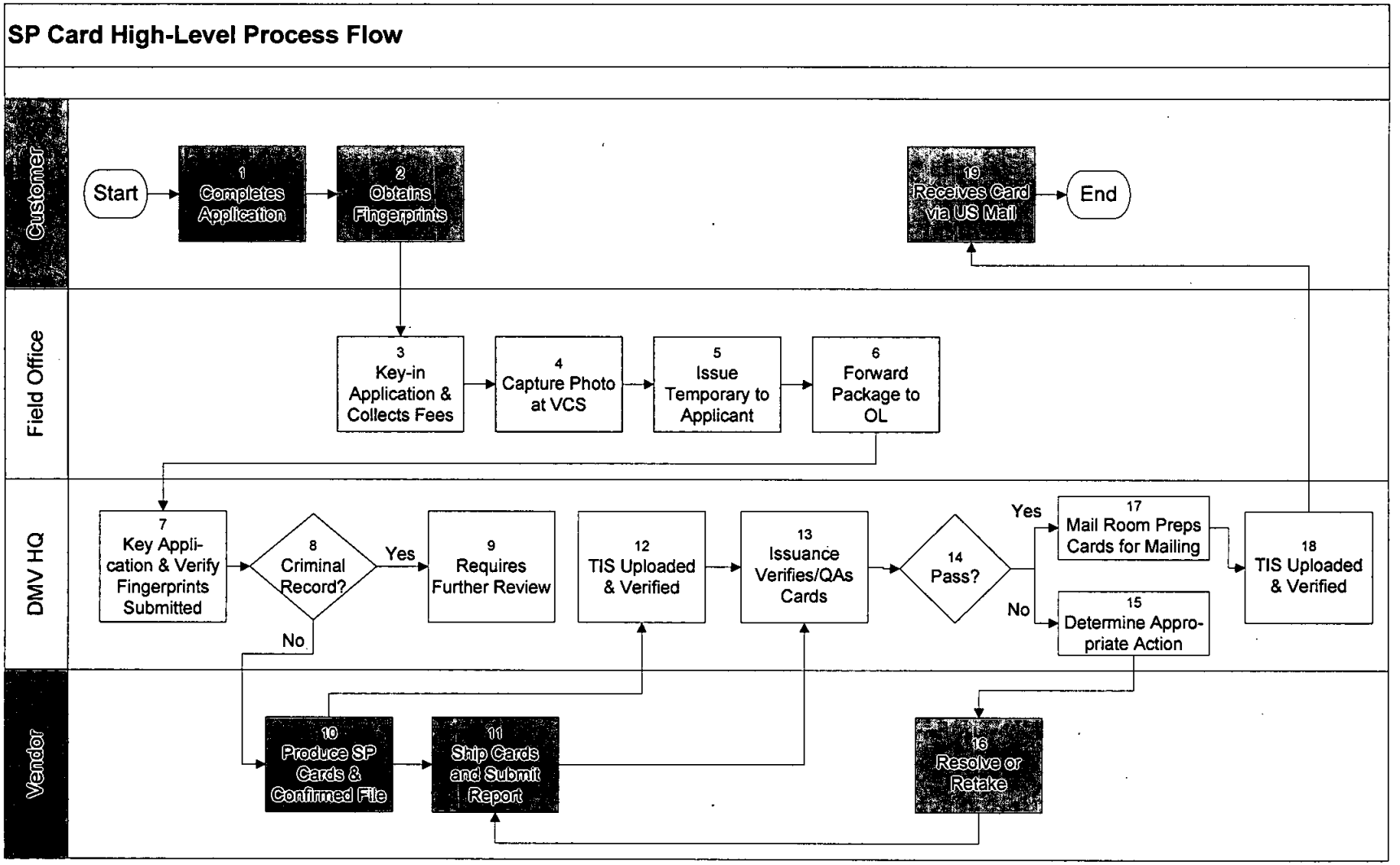


Figure 4-3. SP Issuance Process

The following steps are followed to issue an SP card:

1. Customer obtains the application including the fingerprint live-scan triplicate form (BCII 8016) from the dealership where they work or from a local field office. The live-scan form is necessary in order for obtaining the required 10 fingerprints.
2. The applicant obtains the required 10 fingerprints by going to any local jurisdiction such as a sheriff's office, police department, school district office, etc. The live-scan operator at the local jurisdiction takes the applicant's fingerprints and retains the original or first copy. This initiates a criminal history background check through the California Department of Justice. Results are electronically communicated to DMV. The applicant submits the completed application in person.
3. The applicant brings the second copy of the live-scan form along with the application to a local field office. Upon receiving the completed application, a FO representative enters into DMVA the necessary application data, collects the appropriate fees, and returns a copy of the live-scan form to the applicant.
4. The applicant is then sent to the VCS. Here, the FO representative selects the correct record on the system by using the Daily Application File number from the money receipt. Both the applicant's photo and signature are captured by the VCS.
5. The FO representative issues a temporary SP Card to the applicant if all criteria have been met.
6. Following the issuance of a temporary, the FO representative compiles the application and live-scan information into a package which is forwarded to the Occupational Licensing (OL) Unit at DMV headquarters.
7. Here, an OL employee re-enters the application data into the OL database. The employee also verifies the live-scan fingerprint results once they are received from the California Department of Justice.
8. A determination is made as to whether the applicant has a criminal record.
9. If the applicant has a criminal record, Occupational Licensing conducts further reviews to determine whether a license can be issued.
10. If the applicant does not have a criminal record, the vendor is notified to produce the SP card, verifies the request, confirms the data, and produces the card. The most current image is placed on magnetic storage and the historical images are written onto optical disks, for future retrieval. A confirmed file is submitted to DMV.
11. The vendor ships the SP cards and report to DMV HQ.
12. The TIS is updated and the Issuance Unit verifies the data for accuracy.
13. The Issuance Unit verifies receipt of the cards and inspects the cards for quality.
14. Cards must meet defined quality standards. Any cards with special handling requirements are removed from the batch and processed separately.
15. Cards that do not meet standards are reviewed by DMV staff to determine appropriate action.

16. Staff then resolves the unacceptable card issue or requires a photo retake.
17. Acceptable cards are sent to Mail Operations for processing. Mail operations prepares the cards for mailing. By reading the magnetic stripe on the back of the DL/ID card, a machine addresses and attaches a card carrier to the card which is then inserted in an envelope.
18. The TIS and the SP record are updated with the status and mailing date.
19. The customer receives the SP card, concluding the process.

4.1.5. DL System Interfaces

DMVA interfaces with other systems which provide useful information for determining DL/ID eligibility. The systems used include:

- Social Security On-Line Verification system;
- Verification Information System ;
- Commercial Driver License Information System; and,
- Problem Driver Pointer System.

Social Security On-Line Verification (SSOLV) System – Social security number verification occurs online at the initiation of application processing which involves verification of name, date of birth, and social security number against the Social Security Administration master database. If records cannot be verified, DL or ID cards will not be issued. This verification request occurs through DMVA.

Verification Information System (VIS) – The Systematic Alien Verification for Entitlements (SAVE) program administers programs involving access to information contained in VIS, an online legal presence document verification database owned and maintained by the Bureau of Citizenship and Immigration Services (part of the U.S. Department of Homeland Security). The VIS database contains information on immigrants in the U.S. DMV personnel access VIS records electronically through DMVA DL/ID to verify all immigration birth and legal presence documents.

Commercial Driver License Information System (CDLIS) – The Commercial Motor Vehicle Safety Act of 1986 mandated that "each driver, nationwide, have only one driver license and one record." CDLIS assists all 51 jurisdictions (50 states and the District of Columbia) in meeting this goal when issuing commercial driver licenses. This system interfaces with DMVA.

CDLIS consists of a central site, managed by Electronic Data Systems, located in Plano, Texas. The system maintains data on each commercial driver registered, which includes:

- Name
- Date of birth
- Social security number
- State driver license number
- AKA (also known as) or alias information

When a jurisdiction queries CDLIS to obtain information about an applicant prior to issuing a commercial DL, the CDLIS central site compares data provided by the state of inquiry against all records in its system. If one or more matches are returned, CDLIS informs the state making the inquiry of the existence of records on file from other states. More detailed information about the driver's commercial driving history is available from the state of record should the inquiring state want to research further.

Problem Driver Pointer System (PDPS) – The Problem Driver Pointer System (PDPS) is used to search the National Driver Register (NDR). This is a repository of information on problem drivers provided by all 51 jurisdictions in the U.S. (50 states and the District of Columbia). Through DMVA, a PDPS inquiry is initiated on all original non-commercial driver license customers who are 17 years of age or older. A PDPS inquiry is also done on all commercial driver license applicants. Based upon the information received, PDPS will "point" the inquiry jurisdiction to the state of record, where the applicant's driving status and history information are stored. If the applicant's driving privilege is withheld in another state, the DMV will not issue a permit or license until all actions or violations are cleared.

4.1.6. Document Imaging

As described in Section 4.1.1., the digital images of an applicant's signature, thumbprint, and facial photo are captured by the VCS and transmitted to the card vendor for storage. The VCS does not require a user-specific identification and password. A generic identification and password are used instead. In addition to the digital images, the DMV captures specific document images on microfilm through a centralized micrographics unit located at DMV headquarters. Document images captured on microfilm include applications (such as DL 44s) and legal documents related to license reinstatement.

DMV currently receives, prepares, films, and indexes 72 million registration and driver license documents per fiscal year.[19] These documents are sent from all of the field offices and units at headquarters, as well as some auto clubs located throughout the State. Of the documents filmed, this department retrieves and prints 600,000 documents

[19] Data obtained from the Unit Daily Inventory Report.

annually for law enforcement agencies, courts and customers.[20] DMV currently utilizes 12 Kodak ImageLink 70 microfilming cameras that were purchased in 1993. The storage media is 16mm film.

Each camera has a customized sorter. These sorters separate the bar-coded documents into groups based on whether the bar code for each document was successfully read. Those not read are physically separated and manually worked. The customized sorters mitigate the need for extensive manual sorting and indexing of microfilming bar-coded documents. The customized components are used to process 84% of the 72 million documents processed. As the equipment has aged, it has become increasingly difficult to obtain parts for the customized components.

4.1.7. System Security

The card production facility stores the materials used to create the DL/ID cards in locked secured areas. Any materials that do not meet specifications are destroyed. The production facility also maintains complete audit records of materials received, used, destroyed, and stored. The facility is available for planned and unplanned State inspection. The system includes the CIDS, redundant hot site, and card production equipment. The hot site is maintained in Southern California for operational recovery and access by authorized external users, and is updated within seconds of the primary site.

System security is maintained at the user level through secure sign-ins requiring user IDs and passwords. The exception to this are the VCS in the Field Offices which require a non-user-specific sign-in.

4.1.8. Card Security

The card security features protect against alterations, substitutions, and cannibalization. The California DL/ID card currently has at least eight overt and covert security features. Some of these features include:

- Two-color, optical variable, ink coated on the inside of the face of the laminate, in the configuration of the "California State Seal" and "DMV" logo. Depending on the angle of the card, the images will appear either green or gold.
- Ultraviolet technology that can only be seen through the use of a "black-light". The image of the California State Flag prominently displays the California State bear across the bottom of the card.

[20] Data obtained from the Micro-Retrieval Inventory Report.

- A fine line security printing, known as Guilloche, uses a series of colored concentric circles that are placed throughout the face of the card.
- A secondary 'ghost' photo that is a smaller, less dense, version of the primary photo is located on the front of the card. The location of the "ghost" photo depends on the type of card being issued.

Typically, the life expectancy of high-end security features is less than two years, depending on the skill level of the forger. The existing DL/ID security features are outdated and must be updated to reduce the opportunity for counterfeiting. Additional details relating to recommended security features are included in Appendix B.

4.1.9. Personnel Requirements

The existing contract is supported by the following:

Table 4-1. Current Personnel Requirements

Activity and Position	PY
Contract Management Activities (One Staff Services Manager I)	1.00
Change Coordinator (DMV Manager III)	0.30
Card Request Holding File Extract Processing (Information Systems Technician Specialist I)	0.34
Daily Statistical Report Preparation (Management Services Technician)	0.14
File Extract Problem Resolution (Staff Information Systems Analyst – Specialist)	0.11
File Extract Problem Resolution (Senior Information Systems Analyst – Supervisor)	0.04
Network Installations and Problem Resolution (Staff Information Systems Analyst – Specialist)	0.04
Problem Resolution for Information Transfers Between VCS & RS6000 (Systems Software Specialist I –Technical)	0.04
Total	**2.01**

4.2. Technical Environment

The contractor's Video Capture Station (VCS) interacts with DMV systems by receiving demographic information through DMVA. The images are captured at the VCS and transmitted, along with the demographics, to the Digimarc's Card Image Database System (CIDS). Upon successful completion of the DL/ID/SP application process, CIDS receives notification and demographic information from DMV systems necessary to produce the card.

The VCS performs two primary functions. First, it captures the print, photo, and signature for transmission to the card production facility. Second, it retrieves the photo from CIDS for manual comparison of the photo to the applicant in the field office (FO). Currently, there is not a technical solution for conducting automated image comparisons.

4.2.1. Existing Infrastructure

4.2.1.1 Network Infrastructure

The field offices utilize the State's Frame Relay Network that is managed by the Department of Technology Services (DTS) for data traffic. Each DMV FO has a Trunk Level 1 (T-1) frame relay circuit connected to the frame relay network. Interlata (long distance service) transport is carried via the State's frame relay network and delivered through three (3) separate permanent virtual circuits (PVCs) with data link connection identifiers. These circuits connect to:

- DMV headquarters for connectivity to the local area network (LAN);
- DTS for systems network architecture traffic to DMV databases, and,
- The card production facility for image and demographic data from the VCS.

The PVC for the image data has a committed information rate of 112 kilobytes per second. The data is delivered directly to the card production facility over T-1 circuits and a digital signal level 3 (DS-3) circuit in the frame relay network. There is also a direct T-1 circuit from the card production facility to its backup site in southern California. The following diagram illustrates the infrastructure that supports the DL/ID/SP infrastructure:

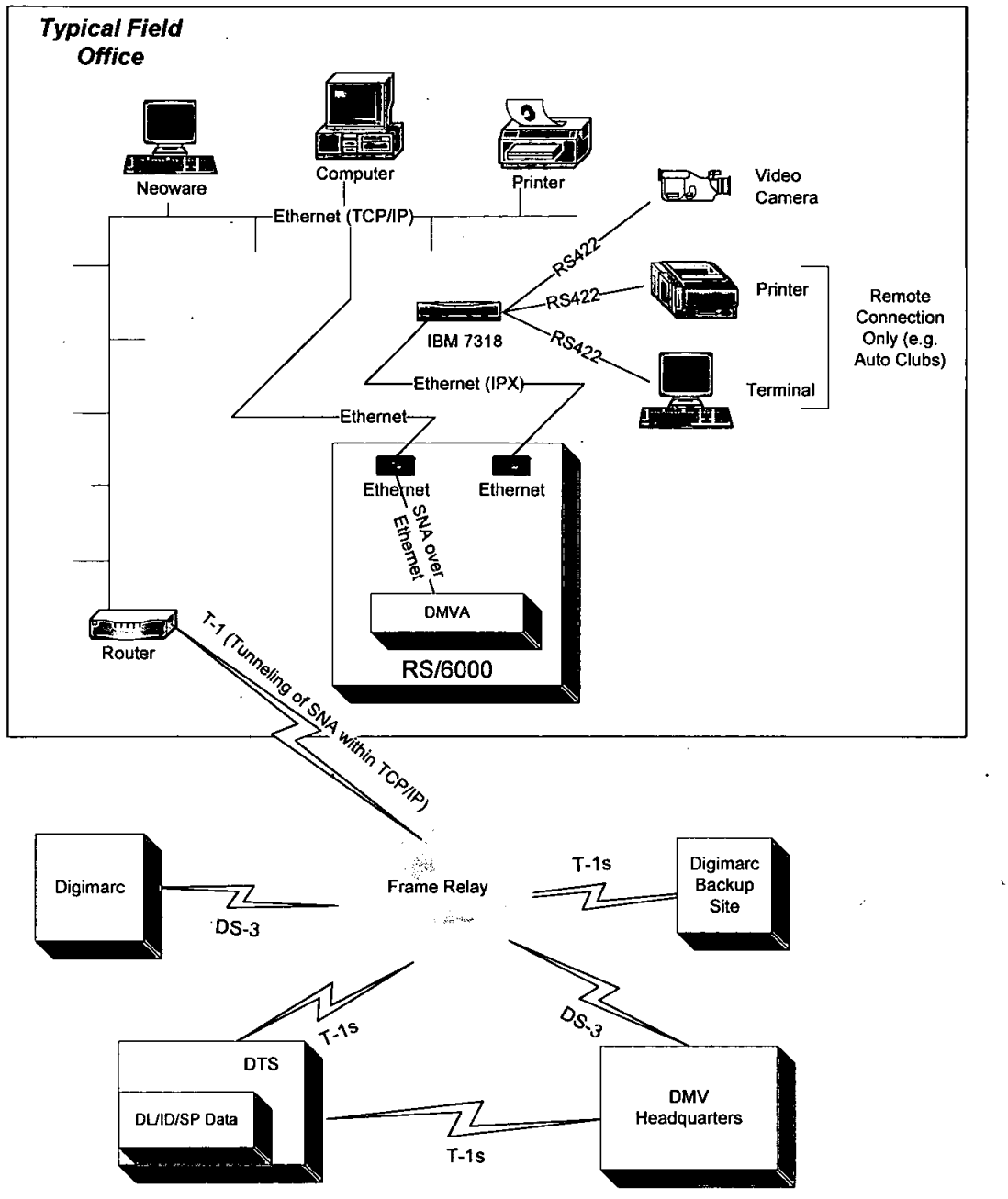


Figure 4-4. DL/ID/SP Infrastructure

VCS application software is disk operating system (DOS)-based. The VCS is connected to the Department's network via both an RS422 connection and a Registered Jack (RJ) 45 Ethernet cable. The Ethernet connection transmits images from the VCS to the CIDS and communicates with DMVA.

The CIDS is comprised of a hard drive that stores the most recent image. Prior images are stored on Write-Once-Read-Many (WORM) optical disks as well as backed up onto magnetic media. These storage devices are connected to a server that communicates

with DTS, DMV headquarters, field offices, and CIDS. DMV retrieval of these images is through the same communication lines. Authorized law enforcement entities retrieve images from the southern California backup site. A typical size of the image file is approximately 15 KB.

After the image and demographics are merged and printed on card material, the card goes through a lamination and die cutting system and finally through a magnetic stripe encoder and sorter. Automated quality control and production software help produce the DL/ID/SP cards to the required specifications.

4.2.2. Anticipated Changes in Equipment, Software, and Operating Environment

The DMV anticipates transitioning to a new document imaging solution at DMV headquarters by September 2007 as described in the Document Imaging and Storage Replacement FSR which was approved in March 2006. The document imaging and storage replacement initiative will replace 12 aging microfilm cameras at DMV headquarters purchased in 1993 with high-speed digital scanners. The documents currently imaged to microfilm are forms received by the Department at field offices and headquarters. Updating the imaging and storage capability of the Department provides increased capacity for storing images of source documents. There are no other relevant anticipated changes for DMV in equipment, software, and operating environment by the implementation date for the new DL/ID/SP solution.

4.2.3. Policy Constraints

There are numerous strategies and policies that provide parameters and constraints for the DMV programs. The following list identifies some of the policy considerations.

Federal laws and standards – The DMV is required to comply with all relevant federal laws and standards, including but not limited to:

- The Commercial Motor Vehicle Safety Act of 1986;
- The Motor Carrier Safety Improvement Act of 1999;
- Federal Information Security Management Act of 2002 (FISMA);
- The US PATRIOT Act of 2001; and,
- The REAL ID Act.

California Vehicle Code – The DMV is legally required to comply with and enforce the California Vehicle Code.

California Code of Regulations – The DMV is legally required to comply with and enforce the California Code of Regulations regarding activities related to driving and motor vehicles.

DMV-Related Executive Orders – The DMV is required to comply with all Executive Orders relating to the Department, including policies regarding budget, exchange of data with other agencies, reporting, and compliance with the California Information Technology Strategic Plan of 2005.

California Public Records Act – The DMV follows the guidelines, which state that all public records, except those protected by privacy considerations, are open for inspection by the public, and that copies are to be made available upon request.

California State Information Technology Strategic Plan – The DMV supports the direction of the State IT strategic plan published in November 2004 and updated in 2005.

e-Government – For any proposed solution, DMV follows the e-Government initiative that directs state agencies and departments to implement electronic technologies that allow the people of California to receive government services and interact with State government.

State Administrative Manual (SAM) – The DMV follows all SAM policies and guidelines in the development of new information systems, specifically SAM sections 4800-5180 (IT General), 5200-5953 (IT Procurement), and 6700-6780 (IT Fiscal).

Statewide Information Management Manual (SIMM) – The DMV follows all SIMM policies and guidelines in the development of new information systems, specifically SIMM Sections 10 through 80 (as required) and Sections 110 through 200 (as recommended).

Information Technology Oversight – DMV follows State policy regarding the establishment of an information technology project management, oversight, and procurement roles and responsibilities within any proposed solution.

AAMVA Standards – DMV attempts to adhere to AAMVA DL/ID card design specification standards. The AAMVA specifications serve as a guideline for achieving the common objective of one identity, one license, and one driver record per individual across states and Canadian provinces.

4.2.4. Project Management Methodology

The DMV enterprise project management methodology serves as a guideline for managing all DMV projects. It is a blend of business and IT project management methodologies and best practices. The methodology is based on and consistent with the Project Management Institute's best practices and the Project Management Body of Knowledge (PMBOK). The project methodology incorporates the concepts of project lifecycle and project management processes, as shown in the illustration below.

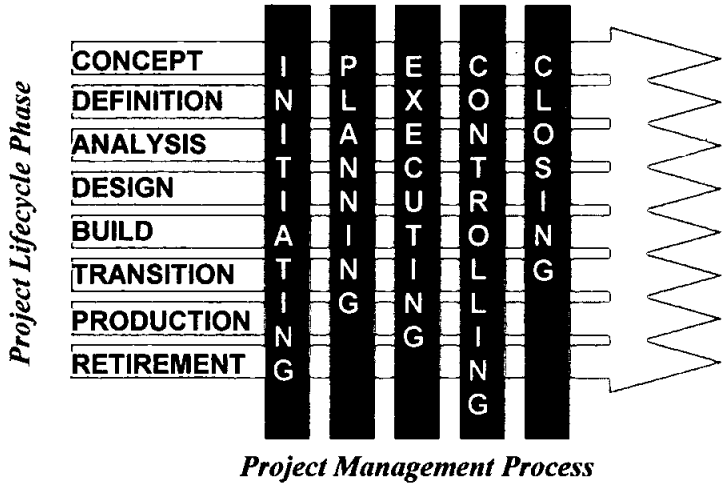


Figure 4-5. DMV's IT Project Management

5. Proposed Solution

The proposed solution will transition support of the current DL/ID/SP card production to a new contract. This solution will include replacement of vendor equipment currently provided by the contractor at the field offices and at the card production facility. The solution will also include technology to capture digital images of identity source documents in a transferable format. Through this business-based procurement, DMV will seek the solution that best meets the objectives and requirements outlined in this report.

Alternatives for the DL/ID/SP card issuance program were evaluated based on the business objectives and functional requirements presented in Section 3, which were compiled through discussions with subject matter experts and stakeholders. Based on these discussions, research, and state surveys, the following alternatives were identified and evaluated:

- Implement a contractor-owned system with centralized issuance;
- Implement a contractor-owned system with an instant or over-the-counter issuance system;
- Implement a DMV-owned system with over-the-counter card issuance; and,
- Implement a DMV-owned system with a centralized card production system.

In this section, the alternative that best satisfies those objectives and functional requirements is described.

5.1. Solution Description

The DMV will implement a contractor-owned solution with centralized issuance which meets all business and functional requirements and includes the following:

- A system, including hardware and software to capture, store, and retrieve, images and demographics;
- A system that verifies the newly captured print and photo images match or do not match images on file;
- A database at a centralized location with a redundant system and a backup at a separate site;
- A card production facility to produce durable DL/ID/SP cards that sufficiently meet AAMVA security standards;
- A system, including hardware and software to digitize, store and display identity source documents;
- A system to track the validation of digitized documents;

- A system that will allow secure storage and transmission of data;
- A system that includes secure, robust audit and tracking capabilities at the individual user level; and,
- A system compatible with DMV's Enterprise Architecture Standards.

The selected contractor's card production facility will store all materials required to create the DL/ID/SP cards in locked secured areas and destroy any off-specification materials. The vendor will maintain thorough and comprehensive records of materials received, used, destroyed, and stored; and make its facilities available for planned and unplanned State inspections or audits.

5.1.1. Hardware

The DL/ID/SP card contractor will supply, install, and maintain new hardware to provide the following:

- **VCS** – Each field office will have at least one video capture station. Larger field offices (grade four and above) will have a minimum of two stations. Each VCS will include at a minimum a laser printer, personal computer, keyboard, color monitor, electronic fingerprint scanner and signature pad, digital scanner, camera with strobe, and backdrop. In addition, VCS capability will be required in headquarters for testing and other purposes.
- **Image Retrieval** – DMV staff at field offices will have the ability to retrieve, view, and print images using a web browser. There will also be at least seven retrieval workstations in headquarters. Each workstation at headquarters will include at a minimum, a personal computer, keyboard, color monitor, and color laser printer.
- **Identity Source Document Capture** – Field offices will be equipped with document scanners and software capable of digitizing all identity source documents. The number of scanners provided will be proportional to the number of workstations in each field office. The solution will include a method to capture the identity of the field office staff performing the second validation (Existing procedures require a second person to visually verify the validity of the identity source document.).

5.1.2. Software

The contractor will provide custom software or commercial off the shelf (COTS) software for the following processes:

- Secure image capture, storage, and retrieval;
- DL/ID/SP card production; and,
- Automated image comparison of images.

5.1.3. Technical Platform

The contractor's system may utilize multiple platforms. However, the technical platform must meet industry standards and be compatible and interface with DMV systems.

5.1.4. Development Approach

Although the contractor will be primarily responsible for solution development efforts, the approach calls for a collaborative design and development approach as outlined Section 6, following a standard system development lifecycle approach. Implementation will also require some DMV in-house application development to interface between the contractor's system and DMV systems to access DL master file records.

The deployment of the new DL/ID/ SP card solution will include a period of parallel operation of the old and new system. During this period, groups of field offices will be phased in, processing applications and issuing cards under the new contract. This approach will allow applications started under the old contract to be processed without interruption and will mitigate against risks associated with full Statewide deployment all at once.

5.1.5. Integration Issues

The contractor's systems must interoperate with the DMV systems. The hardware and software must be capable of utilizing the print images from the existing image record database maintained by the current DL/ID/SP card contractor. Since information from the DMV system will be sent to the contractor's system, both the contractor and DMV will be responsible for ensuring successful integration.

The contractor's document imaging solution must allow digitized images to be viewed at each workstation during scanning (including the VCS) for validation. This should be possible without the need for additional keyboards, monitors, and computers. Digitized image files will be stored such that they are accessible to the field office until the application process has been completed. Once completed, the images will be uploaded to a central repository for future access.

5.1.6. Procurement Approach

The Request For Proposal (RFP) is the most appropriate procurement vehicle for the DL/ID/SP solution. Other procurement methods cannot be used. The cost of the proposed solution will far exceed the authority to procure through the California Multiple

Award Schedule (CMAS), and a Master Service Agreement (MSA) for DL/ID/SP card production is not available.

The equipment used to produce DL/ID/SP cards or capture and verify the identity source documents is not limited to one or two specific makes or models and is not solely based on lowest costs. Other factors, such as a proven history of effectiveness and experience in performing the required services, must be considered when selecting a DL/ID/SP card vendor. Therefore, an Invitation for Bid (IFB) would not be an appropriate procurement approach.

An RFP will be prepared and released to prospective contractors for a new DL/ID/SP card contract. The RFP will specify that the contract is for a system with all the hardware and software necessary to capture and automatically compare photo and fingerprint images, produce the DL/ID/SP cards, capture identity source documents, as well as securely store and provide access to the images as required. During the RFP evaluation process, any proposed DL/ID/SP card will be thoroughly tested by an independent laboratory for durability and security. Durability testing includes bending/folding, friction/abrasion, temperature, laundering, chemical/liquids, and fading. Key elements of the security testing are to ensure the various security features do not compromise one security feature over another and that the combined use of all security features offers more protection against various threat types. Security testing includes:

- Alteration/Cannibalization/Substitution
  - Ease with which alpha numeric data and/or photo/signature may be altered without detection;
  - Ease with which security features, laminate, photo or signature may be transferred from one document to another;
  - Ease with which the magnetic stripe or any other security feature may be removed, replaced, or substituted;
  - Attempts to destroy/alter the data on the magnetic stripe or any feature containing data; and,
  - Ease with which chemicals/water/heat may be used to remove and/or release the laminate or other security feature within the document.
- Counterfeiting
  - Degree to which color copies can be distinguished from the original cards and whether the security features offer resistance to color photocopying and scanning;
  - Degree to which photographic reproductions can be distinguished from original cards and security features offer resistance to photographic reproduction; and,

- Ease with which a security feature/laminate may be counterfeited; including the availability of materials on the open market, technical skills needed, equipment, and costs to successfully counterfeit a feature and deceive an unskilled examiner.

5.1.7. Technical Interfaces

The contractor's systems must interface with the DMV systems so that DL/ID/SP cards can be produced with demographic information from DMV databases. During the roll-out period, DMV must maintain interfaces with both the current and new contractor systems. The document scanning component of the solution must also interface with existing systems such that the documents being captured can be viewed at existing DMV workstation devices and at the VCS. Also, the capture of an identity document will result in an update to the DL master file. Once full deployment is achieved, interfaces to the current contractor system will be decommissioned.

5.1.8. Testing Plan

The contractor will be responsible for developing a test plan, which must be submitted to and approved by DMV. As outlined in the Project Management Plan in Section 6, thorough testing of the proposed solution will be conducted prior to production. Testing will be done without interruption to ongoing operations and will include:

- Unit Testing
- Interface and Integration Testing
- System and Performance Testing
- Parallel Testing
- User Acceptance Testing
- Security Compliance Testing

DMV staff, including subject matter experts and members of the integration team will help develop test scripts and participate in all aspects of testing that impact the interface with DMV systems. The contractor will test its own system.

5.1.9. Resource Requirements

Both DMV and vendor resources will be required during the DL/ID/SP project design, development, testing, implementation, and training phases. Vendor resources will include a contracted independent verification and validation (IV&V) consultant and an Independent Project Oversight Consultant (IPOC). These personnel will participate in the capacities listed below.

Table 5-1. Project Resource Requirements

DMV Resources	Vendor Resources	Other Resources
• Project Sponsor • Project Manager • Steering Committee • DL/ID/SP Workgroup • Procurement and Contract Management • Design Team • Integration Team • Change Management Team • Project Management Office (PMO)	• IV&V/IPOC Consultants • Design Team • Integration Team • Change Management Team	• DGS • DOF • AAMVA • Other States

Section 6 provides detail regarding the specific responsibilities of each of these resources. Under direction of the project manager, the DL/ID/SP card vendor will perform the majority of the required development and implementation tasks, with significant oversight from the IPOC consultant and the PMO. In addition, successful implementation of this project will require DMV and other staff participation during all phases. Assumptions relating to resource requirements are presented in Section 8 of this FSR.

5.1.10. Training

The contractor will develop a training plan with anticipated timing and duration of required training. The DMV assumes the selected vendor will provide core training. The implementation of a new DL/ID/SP card issuance system will require training for system users. Core training will be provided by the vendor and any subsequent training provided by the DMV. The contractor will work with the change management team to plan the details of the training plan.

The DMV plans to disseminate information about the project to the field offices often throughout the DL/ID/SP project, from the procurement phase through implementation. Continuous outreach and communication with the field offices will help ensure successful and timely project implementation.

5.1.11. Ongoing Maintenance and Operation

Because the proposed solution is provided, owned, and maintained by the vendor, ongoing maintenance is the responsibility of the vendor. In the event that vendor equipment fails to meet any requirement, DMV will require that steps be taken by the contractor to repair or replace failing hardware/software as appropriate and within the time specified by the Department at no additional charge. The ongoing costs of the solution are based on the volume of cards issued as projected and shown in Section 8. DMV IT staff will continue to provide ongoing maintenance for the interface between DMV and contractor systems.

5.1.12. Information Security

The system must adhere to the Department of Motor Vehicles information security standards. The vendors and the Department will comply with the information security provisions of the State Administration Manual Sections 4840 and 4841. The proposed system will be evaluated with the assistance of the Department's Information Protection Services Office (IPSO) to ensure that data traveling across the DL/ID/SP network remains secure. IPSO staff will be involved as subject matter experts in the project to assure compliance with DMV's security policies and standards. The Department will ensure that software licenses are acquired and kept current.

Images and demographics will be captured in a secure environment that includes simple biometric identification of the system user to provide a robust audit trail and minimize risk of employee malfeasance. The images and demographics will be transmitted through the frame relay network and the information must remain secure during transit. Security at the card production facility will be verified by the Department by making announced and unannounced site inspections. The Department will require that all production materials be in a locked storage area and any materials not meeting specifications be destroyed by the vendor's facility staff. The card production facility will be required to maintain complete audit records of materials received, used, destroyed, and stored.

5.1.13. Confidentiality

Employees of the DMV are required to maintain the integrity of the processes they perform and the confidentiality of the information they collect. The same basic fingerprint-matching technology used to verify the identity of a DL or ID applicant will be used at sign in to verify the identify of DMV employees involved with the most sensitive aspects of the issuance process.

The DMV employee confidentiality requirements also apply to the DL/ID/SP card contractor. The contractor staff must sign the "Information Security Disclosure Statement Annual Certification." This informs contractor staff of the laws and regulations governing access and disclosure of confidential information, precautions to protect it, and federal and State penalties for non-compliance. It also acknowledges the recipient has read and understood the security policies.

The DL/ID/SP card contractor is required to adhere to the DMV's confidentiality protocols. Subject matter experts from IPSO will support the project team regarding concerns related to confidentiality. The vendor and the Department will comply with the State Administrative Manual Sections 4840 and 4841.

5.1.14. Impact on End Users

Implementation of the new contract is expected to have a significant impact on end users due to addition of the federally required component to capture digital images of identity source documents. Digitizing source documents will result in a process change and increased transaction times in the field office. The increased transaction time is a result of the time required to handle the document, scan it, and verify that the image quality is good. End users will further be impacted because under the REAL ID Act, for the first five years after May 11, 2008, all existing DL/ID holders will likely be required to renew their cards by visiting a field office so that DMV can capture an image of their identity source document. As a result, field office workload will increase dramatically. This impact will be addressed in the REAL ID FSR when reasonably quantifiable. However, because of the expected impact on end-users, the DL/ID/SP card vendor solution must minimize the impact on field office staff while also minimizing the impact to customers. Other than the scanning of the identity source documents, the transition from the old to the new system should be transparent to customers. DMV will be processing cards through both vendors during the phased transition period. An incremental roll-out will have to be planned and coordinated carefully in order to minimize impact on field office staff while making the transition transparent to customers.

Automated print and photo comparisons along with digitized source documents will be new to DMV headquarters and field office staff, eliminating subjectivity from the identification process. If the applicant is a true "no-match", field office staff will not issue a temporary DL license. Headquarters staff would conduct follow-up activities related to an automated listing of applications forwarded for review. The impact of implementation of automated comparisons is unknown at this time. However, DMV expects a short-term increase in record reviews caused by exception items resulting from automated comparisons. This increase is expected to be temporary because the process will

eventually result in deterrence of DL/ID/SP fraud. In addition, end users will use the same print comparison technology to provide a more secure processing environment by using a fingerprint as a biometric logon. Any changes to the system will be communicated to field office staff according to the project training plan.

5.1.15. Impact on Existing System

There will be minimal impact on existing systems. All card data will be transitioned to the new contractor's database; therefore, there will be no loss of data. During the transition period, images captured by the old card production system must be transferred to the new card production system, including the new backup hot site. Images captured under the new card production system will not be transferred to the old card production system.

Digitized document images will be transmitted over a secure line to a secure image repository.

5.1.16. Consistency with Overall Strategies

The proposed solution is consistent with the Department's Strategic Business Plan to enhance consumer protection and employee/public safety. It is also consistent with the Strategic Information Technology Plan goal to transform systems and expand and enhance services. The solution is also consistent with overarching goals established by the Commercial Motor Vehicle Safety Act, the REAL ID Act, DLC, and AAMVA to enhance the integrity of the DL/ID card as a form of identification.

5.1.17. Impact on Current Infrastructure

The proposed solution is not expected to impact the current information technology infrastructure. There may be an increase in bandwidth utilization resulting from automated match requests and responses. An impact on costs would be reflected in the cost per DL/ID/SP card. The solution may impact facilities and result in telecommunications and other facilities costs. Those impacts will not affect the vendor contract but will impact DMV. The Department will be better positioned to ascertain and document those impacts in the REAL ID FSR/Special Project Report (SPR) once federal regulations are promulgated. The solution seeks a scanning solution that will result in the least impact to facilities.

5.1.18. Impact on Department of Technology Services (DTS)

The DMV currently has systems hosted at the DTS. The proposed solution will interface with DMV systems housed at DTS and will require that connectivity be established with the new contractor.

5.1.19. Backup and Operational Recovery

The contractor system must maintain a redundant disaster recovery database and card production system. If the primary facility is unavailable, card production requests will be routed to a backup production site. If the primary image database is unavailable, image retrieval requests from internal DMV requesters will be routed to the backup hot site. Regular operational recovery testing will be conducted in coordination with DMV and the DTS. Results of the testing will be submitted to DMV. Furthermore, the proposed solution must be designed so that the hardware will have ample backup and operational recovery in the event of a hardware failure or natural disaster. The vendor and DMV subject matter experts will develop a backup and operational recovery plan. The system must be able to recover in a secure, systematic, and timely fashion from any planned or unplanned interruptions, with minimal impact to the Department and its customers.

5.1.20. Public Access

The DL/ID/SP card contractor system cannot provide public access by private sector organizations or individuals. However, information will be shared or released on an as needed basis and in accordance with applicable sections of the California Vehicle Code.

5.1.21. Costs and Benefits

DMV will procure a complete system with payment made on a per card basis. There will not be incremental or separate costs for document imaging, print and photo comparison or security features.

As detailed in the Economic Analysis Worksheets in Section 8 of this FSR, DMV estimates one-time costs associated with the proposed solution will be approximately $1,889,087 over a two year period for the following:

Table 5-2. One-Time Costs for Proposed Solution

Cost Category	Cost
DMV Staff Assistance (Salaries & Benefits)	$1,465,857
Telecommunications	$15,000

IPOC Services	147,054
IV&V Services	73,971
Other - DGS Service Fees	$80,000
Agency Facilities	32,500
Training	$74,705
Total	**$1,889,087**

Due to its size, California has historically had the lowest DL/ID/SP per card cost among the states. The DMV expects these economies of scale will continue to be achieved with the proposed solution. Through extensive market research, using information provided by other states, DMV has determined that expected DL/ID/SP card cost will increase from approximately $0.65 to $0.90 per card. This estimate includes costs related to document image capture, automated print comparison (including biometric logon) and updated security features. The ongoing vendor costs are expected to be approximately $8,335,971 (including tax) per year based on a card production volume of 8,596,000.

The proposed solution provides the following benefits over the term of the new contract:

- Allows uninterrupted continued issuance of consistently high quality, secure DL/ID/SP cards.
- Improves the ability of other agencies (e.g., law enforcement, courts) to rely on the cards for identification purposes. Presently, one of the courts and only 80 percent of law enforcement use DL/ID cards for identification purposes. Without absolute confirmation of an individual's identity, citations are often dismissed or assigned a generic substitute DL number. Presently, there are more than 2.5 million such records, with a five year purge criterion. Subsequently, the potential revenue from court fines, license penalties, reissue, and other fees is lost. This loss is substantial. For example, if each citation results in $100 in fines and fees and if only 10 percent of these cases could be properly identified to the offending individual, approximately $5 million in lost revenue could be recovered (2.5 million records x 1/5 x 10 percent x $100).
- Updated card security features will make it more difficult to create counterfeit DL/ID cards.
- Provides 99 percent accuracy in validating whether cardholders are who they say they are by comparing the latest print image on file with the print being captured. Whether or not a customer presents a DL/ID at the time of the field office visit, 100 percent of non-original applicants will be verified via the print comparison process.
- Provides immediate (one second or less) and ongoing print comparisons in order to verify applicants' identification.
- Using standard automated verifications, the process will no longer be subjective and prone to error. By using automation to perform the image comparison, verification will not be subject to personal bias.

- Requires minimal field office employee training because changes to the video capture process are not anticipated to be significant.
- Provides a solution that meets the latest AAMVA, ANSI and NIST standards, presenting an opportunity to improve data exchange with other states and jurisdictions.
- Improves DMV's ability to meet its responsibilities under the CVC. As discussed in Section 3, certain CVC sections preclude issuance or possession of a DL/ID card if circumstances negate entitlement. The image comparison process will verify an individual's identity which, in turn, virtually eliminates the possibility of multiple individuals having a DL/ID tied to a single record. As a result, it is estimated that at least 28 records per year will no longer be issued in error.
- Prevents employee misuse of the VCS and establishes an audit trail for all DL/ID card transactions. Currently one employee identification number is used at the VCS. The proposed solution requires each employee to be biometrically identified when capturing the image data to create a card. This will bring to light necessary training issues. The increased field office training is anticipated to reduce employee audit cases by 10 per year and reduce card remakes due to employee error by approximately 200 per year.
- Provides an identity document imaging solution as required by the REAL ID Act.

5.1.22. Sources of Funding

DL/ID/SP card production costs will be paid on a per card basis and funded through budget augmentation starting in April of fiscal year 2007-08, as reflected in Section 8 of this report. DGS procurement services for fiscal year 2006-2007 are funded through budget augmentation. Other one-time project costs shown in Section 8 will be funded through redirections. Ongoing funding for the DL/ID/SP card production costs will be from the Motor Vehicle Account.

5.2. Rationale for Selection

The proposed solution satisfies all of the objectives and functional requirements set forth in this feasibility study report. In addition to the benefits enumerated in Section 5.1.21., the proposed solution will:

- **Allow DMV to provide uninterrupted high-quality DL/ID/SP card production to customers in the most cost-effective, expert, and efficient manner.** The existing process has proven to be effective in handling a high volume of cards in a timely and effective way. Centralized card production provides for better control, security, and accountability than decentralized production. Also, this solution allows DMV to avoid having to create and maintain an infrastructure for DL/ID/SP card production including a production facility, imaging equipment, and a back-up site. Since there are companies that provide expert and cost-effective card production equipment and services, it is in DMV's best interest to leverage those resources.

- **Improve DMV's ability to verify the identity of applicants.** In order for DMV to more effectively meet its goal of ensuring an individual has only one identity, one license, and one driver record, an automated image comparison process is necessary to identify and deter potential fraud. An automated one-to-one comparison of newly captured images to verify the identity of an applicant at the field office, provides technicians an immediate and objective tool for verification of the applicant's identity and eligibility for a DL/ID/SP card. Current imaging technology allows a highly accurate electronic comparison of the person at the counter with others in a database system. Automated print comparison is the most accurate and cost effective way of identifying individuals.[21] In a recent assessment by the International Biometric Group, 90 percent of DMV's print images were found to be of good quality and useable to support an automated comparison process. Auto-comparing current print images will, without major risk and cost to the DMV, allow staff to determine whether subsequent action is necessary in identifying multiple individuals on the same DL/ID record. Print auto-comparison technology also provides a simple biometric logon capability.
- **Provide an opportunity to adhere to AAMVA standards.** The expiration of the DL/ID/SP contract coincides with the promulgation of the AAMVA standards published in March 2005. A new contract provides the opportunity to update the card security features in order to deter counterfeiting in a manner that complies with AAMVA standards.
- **Enable DMV to capture digital images of identity source documents.** To be compliant with the REAL ID Act, all DL/ID card applicants must provide an identity source document which DMV is required to capture as a digitized image. The expiration of the DL/ID/SP card contract nearly coincides with the effective date of the REAL ID Act. The new contract provides an opportunity for DMV to obtain the imaging solution from the new vendor.

The following table summarizes the advantages and disadvantages of the proposed solution.

Table 5-3. Advantages and Disadvantages of the Proposed Solution

Advantages	Disadvantages
• Leverages contractor expertise. • Because it is similar to the existing process and DMV has experience with this type of procurement, it is the alternative with the highest probability of success and lowest risk of failure. • Many states have conducted recent procurements for similar solutions and California could benefit from their input. • Does not require that DMV own	• Requires a procurement which could be a lengthy process. • Continues DMV's dependence on a vendor to provide services.

[21] International Biometric Group, DMV Biometric Assessment, June 7, 2002; Federal Commercial Driver's License Biometrics Demonstration Test, November 13, 2002; and the Federal Fingerprint Vendor Technology Evaluation, 2003.

Advantages	Disadvantages
production and imaging technology. • Requires minimal training because the solution is much like the existing process. • Provides the opportunity to update security features. • Adheres to recent AAMVA standards. • Centralized card production provides for better control, security, and accountability. • Automated comparison of images reduces opportunities for fraud and errors (e.g., twin on wrong record). • Provides a pool of vendors with specialized expertise to offer the best solution. • Provides a means to capture digital images of identity source documents.	

5.3. Other Alternatives Considered

Along with the proposed solution for the DL/ID/SP card issuance program, the following alternative solutions were considered:[22]

- Contractor-owned system and instant over-the-counter card issuance.
- DMV-owned system and instant over-the-counter card issuance.
- DMV-owned centralized card production system.

In summary, only the proposed solution satisfies all the program requirements and objectives set forth in this FSR using the most cost-effective approach. Instant over-the-counter card issuance is simply not cost effective and a DMV-owned, operated, and maintained DL/ID/SP card production system is impractical and an inefficient use of State funds.

5.3.1. Alternative 1: Contractor-owned System and Instant Over-the-Counter Card Issuance

This alternative requires the contractor to own the CIDS and provide the ability to create cards in a field office. Upon meeting all application requirements, the applicant would receive a card at the conclusion of the field office visit and not have to wait to receive the

[22] Costing for all alternatives was derived from other states' recently awarded DL/ID card contracts for cost comparison purposes.

card by mail. Based on the experience of states that create instant, over-the-counter issuance of more than one million cards annually by a contractor, the average cost per card is $1.50 for this alternative. The detail associated with this solution is shown in Section 8.

The advantages and disadvantages associated with this alternative are summarized below.

Table 5-4. Alternative 1 Advantages and Disadvantages

Advantages	Disadvantages
• For those who met all application requirements, the DL/ID Card would be issued at the time of the field office visit. • Reduced mailing costs. • A contractor would provide the equipment and a backup site. • Poor quality cards would be identified immediately, images re-taken, and card remade before the customer leaves the field office. • Provides a means to capture digital images of identity source documents.	• Security, control, and accountability of the card material would be at greater risk with a distributed process in 170 field offices. • Greater effort would be required to supply and distribute card material. • Card production costs would increase approximately $0.78 over California's current cost. • Non-uniform card appearance may result making verification more difficult for law enforcement, retail merchants, and others who depend on the card as a form of identification. • Increases applicant transaction and wait time in the field offices. • Overcrowded field offices may result because of individuals waiting for a DL/ID card to be produced. • Since SP card applications require additional processing in headquarters, SP cards would also need to be produced centrally. • Would require a centralized process anyway for card issuance related to DL renewal by mail and Internet (this is approximately 31 percent of the annual card production) and cards issued through exception processing.

Recommendation: Over the counter card issuance is not a good solution for California due to the volume of transactions. Given the number of field offices and the challenges of minimizing wait times, creating DL/ID cards in the field office would present unnecessary risks that cannot be justified. An over-the-counter solution would still require a centralized component to address renewal by mail, renewal by Internet, and SP license issuance processes. This alternative would result in:

- Increased customer transaction and wait times in field offices;
- Increased security risk due to the distribution and storage of card materials;
- Increased risk of equipment theft at more than 170 locations;
- Potentially non-uniform card appearance; and,
- Increased opportunities for fraud.

5.3.2. Alternative 2: DMV-Owned System and Instant, Over-the-Counter Card Production

This alternative requires DMV to develop and maintain a system to provide for instant, over-the-counter issuance of the cards in field offices.

For comparison purposes, the State of Arizona has over-the-counter issuance in 46 of its 66 field offices and centralized issuance in the remaining 20 field offices. Arizona's cost to produce DL/ID Cards is $1.78 per card, which includes the image capture and database as well as support staff to maintain the equipment. The Arizona cost does not include automated image comparison. This alternative has all of the drawbacks of Alternative 1, plus the added disadvantage of requiring DMV to purchase equipment and software for imaging, production, retrieval, and comparison of images. The costs associated with this solution are shown in Section 8.

The advantages and disadvantages associated with this alternative are as summarized below.

Table 5-5. Alternative 2 Advantages and Disadvantages

Advantages	Disadvantages
• DMV would have complete control over card production and database creation and maintenance. • For those who met all application requirements, the DL/ID Card would be issued at the time of the field office visit. • Reduced mailing costs. • A poor quality card could be identified, images re-taken, and the card remade before the customer leaves the field office. • Provides a means to capture digital images of identity source documents.	• Any changes or enhancements to the system would be subject to Departmental IT priorities (resources may not be available when needed). • The DMV would have to incur the cost to create and maintain the DL/ID Card database and backup site. • The DMV would have to procure and maintain its own card materials and VCS, card production, and database hardware and software. • The DMV would be solely responsible for an interface between the image capture equipment, image databases, and the DMV systems. • May result in field office overcrowding, as

Advantages	Disadvantages
	long lines could result from individuals waiting for a DL/ID card to be produced. • The State would not have the benefit of vendor expertise in developing and maintaining the solution. Ongoing staff training needs could jeopardize card production. • Security, control, and accountability of the card material would be at greater risk with a distributed process in 170 field offices. • Greater effort would be required to supply and distribute card materials. • The average card production cost is approximately three times higher than California's current cost. • Non-uniform card appearance may result making verification more difficult for law enforcement, retail merchants, and others who depend on the card as a form of identification. • Would require a centralized process anyway for card issuance related to DL renewal by mail and Internet (this is approximately 31 percent of the annual card production). • Since SP card applications require additional processing in headquarters, SP cards would also need to be produced centrally.

Recommendation: As is the case with the previous alternative, this alternative is not a good solution for California because it requires over-the-counter card issuance. This alternative has the added disadvantage of requiring DMV to develop internal expertise in photo and print imaging, image comparison, card security, and card production. This alternative would result in :

- Increased customer transaction and wait times in field offices;
- Increased security risk due to the distribution and storage of card materials;
- Potentially non-uniform card appearance;
- Increased opportunities for fraud; and,
- Increased costs associated with purchase, installation, and maintenance of equipment.

5.3.3. Alternative 3: DMV-Owned Centralized DL/ID Card Production System

This alternative requires DMV to develop and maintain a CIDS and produce DL/ID/SP cards in a centralized location. Unfortunately, there are no cost comparisons available, as no other states have this type of implementation. Similar to Alternative 2, this option would require that DMV develop internal expertise in various aspects of card production and security and purchase and maintain equipment and materials currently handled by the contractor.

The advantages and disadvantages associated with this alternative are summarized below.

Table 5-6. Alternative 3 Advantages and Disadvantages

Advantages	Disadvantages
• DMV would have complete control over card imaging, production and database creation and maintenance. • Although it requires DMV responsibility of the card production material, it reduces the effort required to secure, control, and account for the card production materials compared to the other two alternatives. • Reduces the opportunity for employee fraud since the card production material is not housed in any of the 170 field offices. • All DL/ID/SP cards would be created using consistent standards, controlled centrally. • Applicant transaction and wait times would not be increased in the field offices because the applicant is not waiting for the DL/ID Card to be produced.	• It would be difficult for DMV to keep up with the latest technology. • The DL/ID card system would require internal IT expertise subject to competing priorities. • Mailing costs for the DL/ID/SP Cards would continue to be incurred. • The DMV would assume responsibility for administering multiple contracts for hardware and software purchase and maintenance, as well as for materials. • A secure production facility would be needed. • If commercial off-the-shelf software could not be obtained, DMV would have to develop a custom solution. • A poor quality card could not be identified, images re-taken, and the card remade before a customer leaves a field office. • The State would require industry experts in developing, maintaining, and enhancing the system. • Would require many more resources to support. • Ongoing staff training needs could jeopardize card production.

Recommendation: In addition to other disadvantages, this alternative requires expertise the DMV lacks. With many vendors available to provide the services, it would not be

wise for DMV to take on the production of DL/ID/SP cards internally at this time. Such an undertaking would require the purchase of imaging and card production equipment, development or purchase of required software, maintenance of an additional database with a backup site, and expertise in card security features and image comparison technology. Therefore, this alternative is not recommended.

6. Project Management Plan

DMV recognizes that a structured approach to managing the DL/ID project is critical to ensuring its success. To this end, DMV has developed the Project Management Plan outlined in this section of the FSR. This plan complies with Department of Finance's Information Technology Project Management Methodology.

6.1. Project Manager Qualifications

The project manager, Wesley Goo, is a 20 year employee of DMV with extensive knowledge and experience in multiple aspects of DMV operations. Mr. Goo has been Manager of the Systems Development Unit in Licensing Operations Division since 1999. He has provided project management services to a number of projects designed to strengthen the driver license program and safeguard it from fraudulent activities. His recent project experience includes:

- Implementation of image retrieval at field office workstations;
- Provision of forms related to driving under the influence over the Internet; and,
- Development of the proof of concept for automating the driver license knowledge test.

Additionally, Mr. Goo was the project lead for the last driver license contract replacement that occurred during state fiscal year 1998-99. This directly relevant experience will contribute to the project's success.

6.2. Project Management Methodology

The DMV Enterprise Project Management Methodology serves as a guideline for managing all DMV projects. It is based on the Department of Finance's Information Technology Project Management Methodology as outlined in the Statewide Information Management Manual (SIMM), Section 200. The DMV methodology is a blend of business and IT project management methodologies and best practices. It is consistent with the Project Management Institute's Project Management Body of Knowledge (PMBOK) best practices. The project methodology incorporates the concepts of project lifecycle and project management processes. The DL/ID/SP project manager will use Microsoft Project to develop a detailed project plan and schedule, and will provide written status reports on a regular basis.

6.3. Project Organization

The proposed DL/ID/SP organization is illustrated in Figure 6-1. Information about the roles and responsibilities of the project team is provided in Section 6.5.4.

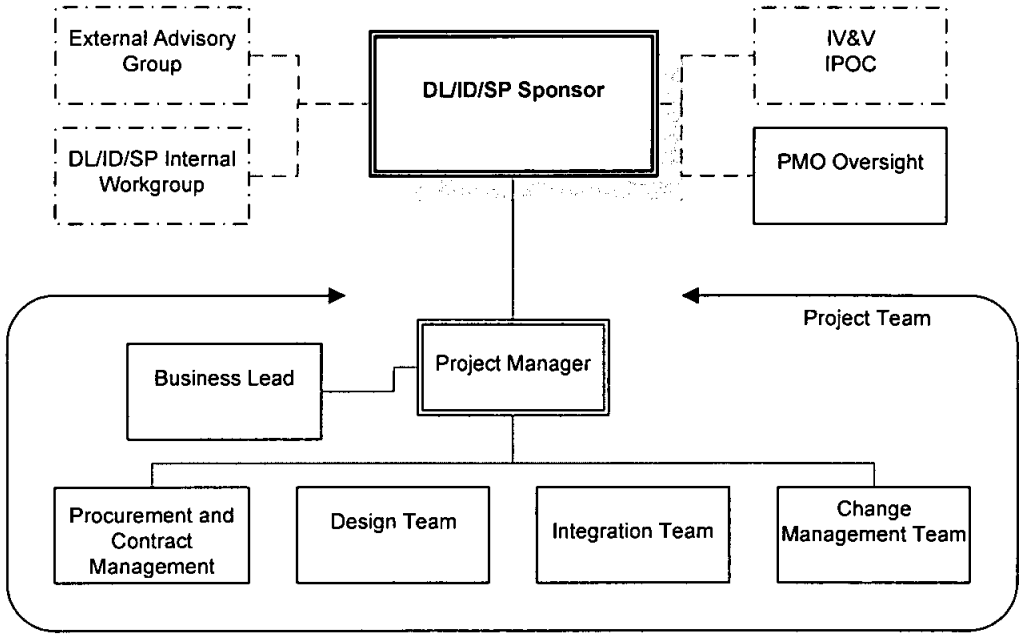


Figure 6-1. DL/ID/SP Project Team Organization

6.4. Project Priorities

All projects have three core components that must be managed:

- Schedule
- Scope
- Resources

Each of these is interrelated – a change in any one factor will almost certainly impact the others. Prior to beginning the project, it is important to determine the relative importance and flexibility of each. For the DL/ID Project, this is documented in the matrix that follows.

Table 6-1. DL/ID Project Trade-Off Matrix

Schedule	Scope	Resources
Constrained *(Cannot be changed)*	**Improved** *(Can be adjusted)*	**Accepted** (Are somewhat flexible)

6.5. Project Plan

Project planning defines:

- Project goals and objectives;
- The activities required to accomplish them;
- How to perform these activities, and,
- The resources required to accomplish them.

The project plan defines each major task, estimates the time and resources required to accomplish it, and provides a framework for management review and control. Project planning activities include defining the project scope, assumptions, phasing, team roles and responsibilities, and schedule. The following sections briefly define and discuss each of these components.

6.5.1. Project Scope

The DL/ID Project will implement a new DL/ID/SP card contract to issue new cards statewide by May 11, 2008. This contract will include hardware and software to capture, store, and retrieve images and demographics.

In addition to the new card contract, the project will automate the fingerprint and photo comparison processes in order to verify identity. Updated security features will be provided that reasonably adhere to AAMVA standards to reduce fraud and counterfeiting. The scope of specific DL/ID system requirements is documented in Section 3 of this FSR (Business Functional Requirements).

6.5.2. Project Assumptions

The following assumptions are made for the DL/ID Project:

- Automated identification components can be added to the CIDS;
- Funding will be provided by the Motor Vehicle Account;
- DMV will coordinate with the Department of General Services (DGS) to ensure that DGS can review and approve the proposed procurement approach defined in the ITPP for the DL/ID/SP project according to the plan outlined in Table 6-4;
- Functional requirements will not change substantially during project implementation;
- Higher priority issues will not impact the schedule or resource needs;

- Executive sponsorship will continue through project completion;
- The Department of Finance (DOF) will review and approve this FSR as planned (see Table 6-4);
- There is COTS software that can meet the critical functional requirements of DL/ID/SP;
- Qualified DMV program and technical staff will be available to participate, as needed, in design, development, testing, training, and implementation of the selected DL/ID/SP solution;
- Suppliers, vendors, consultants, and State staff will perform their assignments related to the DL/ID/SP project in a competent and timely manner;
- Issues will be resolved and risks mitigated on a timely basis; and,
- All equipment and software provided will comply with DMV standards.

6.5.3. Project Phasing

In order to reduce project risk and stay within resource constraints, the DL/ID project will be implemented in a phased approach, as described below.

Phase 1.0 FSR Development and Approval

This phase consists of the pre-work and analysis done to identify the need and appropriate scope for the DL/ID/SP project as well as the preparation of this FSR for the project. Upon completion of this phase, DMV will have developed a good assessment of impacted program areas and business functions, and defined and documented major project execution activities.

Phase 2.0 RFP Development and Vendor Procurements

In this phase, detailed requirements will be gathered and documented and a Request for Proposal (RFP) will be prepared. The RFP will be made available to potential DL/ID system vendors, their responses evaluated, and a system vendor selected. DMV will work closely with DGS during all phases of procurement. Prior to issuance of the contract, DMV will submit a Special Project Report to Department of Finance to report updated costs, as required for business-based procurements.

The IV&V and IPOC consultant(s) will also be selected during this phase. Based on the Department of Finance Technology Oversight Framework, DL/ID/SP is a medium criticality project and requires control agency oversight as shown in Table 6-2. Funding for IV&V and IPOC services have been included in the EAWs.

Table 6-2. DL/ID Rating for Oversight

Factor	DL/ID Rating
1) Size	High (3)
2) Project Manager	Low (1)
3) Project Team (DMV)	Low (1)
4) Type	High (3)
Total Score	**8**
Average Score	**2**

Phase 3.0 System Development

Following a standard development life cycle methodology, this phase will include project initiation and planning, requirements gathering and design, development, testing, and training.

Initiation and Planning

The project initiation formally authorizes the project. It will involve preparing a project charter, developing an updated project management plan, and coordinating project team and subject matter experts' participation. The project leadership will conduct a kick-off meeting with the project team to mark the official start of the project.

Requirements and Design

The project team reviews the business requirements and defines what the solution must do to meet the functional requirements. Some of the major activities are to analyze the current system and functions; identify the gaps in processing and functionality; conduct a logical data analysis; and, define and document the findings into detailed business requirements. Problems, opportunities, and functional requirements are broken down into detailed business requirements.

Working closely with the project team, the contractor will develop the business and technical design. In business and technical design, the project requirements are used to develop specifications that guide the building of the finished product during the development and unit testing phase. Business design and technical design are conducted as separate sub-phases, but will be run concurrently.

During business design activities the project team will identify card features, card design, and business processes. During technical design activities the team will select the application software, prepare the architecture, design the application's technical

functions, design the CIDS database, design the interfaces, and prepare conversion plans.

Development and Unit Testing

During development and unit testing, the contractor and Information Systems Division (ISD) create the development environment, build the solution, and perform unit testing of components in their respective systems to verify they work according to specifications.

Conversion of Images

All images will be converted to the new CIDS. Tests must be conducted to ensure that these images can be retrieved and utilized as needed by the new solution.

System, Integration, and User Testing

The contractor will be primarily responsible for developing a testing plan and conducting system testing to verify that all components of the solution work according to the business and technical design. Any problems that are identified will be prioritized and corrected, and then re-tested. This process will be repeated until all problems have been resolved. Regression testing will also be conducted during this phase to ensure that changes made during problem resolution did not negatively affect other areas of the system.

Concurrent with system testing, performance tests will be conducted to ensure that there is sufficient bandwidth to meet the system's demand. Performance testing will verify that a large number of concurrent users or a large number of simultaneous inquiries do not cause system failure or delayed response.

After the successful conclusion of system testing, DMV and contractor staff will conduct parallel testing. During parallel testing data will be entered into both the current and new systems in a test environment. The data, cards, other outputs, and reports will then be compared to identify any discrepancies. Although the parallel test will increase the work effort, it will be an important simulation of production before the system is actually implemented.

After parallel testing, but prior to implementation, the project team's subject matter experts and a select group of staff will conduct acceptance testing to verify the solution works according to the business requirements, including appropriate field office environment response times. When acceptance testing has been completed successfully, the new DL/ID/SP card solution will be signed-off as ready for production.

Training Development and Delivery

The contractor will be responsible for developing a training plan and training content. Before implementation all users will be trained in how to use the new equipment and software. The change management team will work with the contractor to develop a detailed plan including a schedule for delivering training to field offices as they prepare to implement the new system. The team will prepare user training documents and materials, conduct communications and outreach to other stakeholders within DMV, and prepare policies and procedures for the new system, as needed.

Phase 4.0 Phased Solution Implementation

This will be the period when DL/ID/SP is rolled out to the field offices in phases over a 2.5 month period to allow staff to address last-minute problems without impacting every field office. This approach will also provide an opportunity for technical staff to monitor network usage as offices are methodically brought online. After implementation, testers will conduct post-implementation verification to ensure the system is meeting requirements in the production environment.

The decision on which offices are included in each implementation phase will depend on the size of the office, its location in the state, staff's availability for training, and the office's business needs.

Phase 5.0 Closeout and Post Implementation Evaluation and Review

The Closeout and Post Implementation Evaluation and Review phase will signal the end of the DL/ID project. There will be final sign-off of the new system and formal closure of the prior contract. Six months after formal sign-off, a Post Implementation Evaluation Report (PIER) will be initiated to evaluate the project. Any lessons learned for future projects will also be included.

For additional information on each of these phases, please see *Table 6-4 DL/ID Project Phases and Tasks*.

6.5.4. Roles and Responsibilities

As illustrated in the Project Organization Chart in Section 6.3, the key leaders and decision-makers related to the DL/ID project will be the project sponsor and project manager. Other members of the project team will also be critical to its success. The roles and responsibilities of the various individuals and groups that make up the DL/ID project team are described below.

Table 6-3. DL/ID Project Team Roles and Responsibilities

Responsibilities	Resource
1. DL/ID Project Sponsor	
• Approves project scope and objectives. • Serves as key business decision-maker on the DL/ID project. • Resolves significant project issues. • Attends Steering Committee meetings. • Communicates project status and outstanding issues to the Steering Committee, executive staff, and other stakeholders. • Ensues adequate staffing and funding for the project. • Communicates project status to internal and external stakeholders. • Manages communications and relationships with external organizations.	DMV
2. DL/ID Project Manager	
• Helps coordinate work efforts that impact the project. • Approves project deliverables throughout the DL/ID project. • Attends DL/ID project status briefings. • Facilitates the Steering Committee meetings. • Facilitate Internal Workgroup and project meetings. • Coordinates and oversees project activities. • Reviews project deliverables. • Schedules and attends project team meetings. • Finalizes, monitors, and oversees the Risk Management Plan. • Develops project management-related deliverables (e.g., weekly project status reports and project plan updates). • Serves as liaison between vendors and stakeholders. • Tracks and resolves project issues. • Maintains the project work plan. • Ensures that issues and changes are documented. • Institutes controls to determine adherence to the project work plan and schedule. • Facilitates active and timely participation of program and technical staff for the duration of the project.	DMV
3. DL/ID Business Lead	
• Maintains a resource management plan and schedules business resources throughout the project. • Ensures adherence to business requirements.	DMV

Responsibilities	Resource
• Develops project management-related deliverables (e.g., weekly project status reports and project plan updates). • Assists the project manager in tracking and resolving issues. • Coordinates active and timely participation of program staff for the duration of the project.	
4. DL/ID Steering Committee	
• Confirms project goals and scope. • Resolves significant issues and makes scope change decisions that cannot be resolved by the DL/ID Project Management Team. • Participates in Steering Committee meetings. • Communicates project status to stakeholders as needed. • Addresses cross-divisional policy issues. • Addresses barriers to project success.	DMV
5. DL/ID Internal Oversight (PMO)	
• Serves as an internal expert to provide project management assistance to the project manager in activities that are critical to the project's success. • Provides consultative services to project leadership to ensure the project approach makes use of established DMV best practices. • Provides analyses as needed on DL/ID/SP solutions.	DMV
6. Independent Verification and Validation Consultant	
• Serves as an independent expert that provides oversight of project activities that are critical to the project's success. • Evaluates the project to ensure that it is following a structured and defined approach. • Reviews deliverables to ensure that they are aligned with defined standards, DMV's needs, and contractual requirements. • Prepares periodic project assessments and develops DOF/OTROS progress reports in coordination with DL/ID Project Management.	IV&V Vendor
7. Independent Project Oversight Consultant	
• Serves as an independent expert to provide project management oversight and assistance to the project manager in activities that are critical to the project's success. • Provides consultative services to project leadership to ensure the project approach makes use of established best practices and mitigates project risks. • Provides analyses as needed on DL/ID/SP solutions.	**Vendor**

Responsibilities	Resource
• Reviews deliverables to ensure that they are aligned with defined standards, DMV's needs, and contractual requirements. • Assists in the preparation of periodic project assessments.	
8, External Advisory Group	
• Provides expertise to DMV that would address areas of concern. • Advocates for and supports the project.	DOF BT&H DGS
9. Internal Project Workgroup	
• Assists with the evaluation of proposals. • Provides input on DL/ID communications and training. • Provides resources for testing.	DMV
10. Procurement and Contract Management	
• Participates in the procurement processes to secure a DL/ID/SP card and IV&V contractor. • Tracks the vendor project budget and reviews vendor invoices. • Maintains information on contracted costs vs. actual costs. • Manages contract change requests and addendums.	DMV
11. Design Team (Includes Subject Matter Experts [SMEs] and IPSO)	
• Participates in project initiation, design, and testing sessions. • Resolves DMV card design and specification issues. • Defines business processes and business rules. • Defines privacy and information security requirements and rules to ensure protection of constituent privacy. • Participates in joint application design sessions. • Assures adherence to privacy and information security standards such as FISMA. • Participates in user acceptance testing.	DMV Vendor
12. Integration Team (Includes SMEs)	
• Installs the DL/ID application and all related hardware and software according to agreed upon requirements and specifications. • Participates in initiation, design, development, and testing. • Conducts prototyping sessions with stakeholders. • Leads in testing the DL/ID system. • Conducts unit, system, integration, performance, regression, and parallel tests. • Develops test scripts for user acceptance testing.	DMV Vendor

Responsibilities	Resource
• Facilitates user acceptance testing. • Conducts risk analyses and recommends acceptable level of risks to the project management team. • Performs information security reviews to ensure applicable safeguards are in place and operational. • Conducts Post-Implementation Verification of the system. • Prepares system documentation. • Provides ongoing support for the DL/ID system. • Works with the change management team to develop user manuals, address user questions and issues (e.g., help desk), develop training manuals, and conduct training sessions.	
13. Change Management Team (Includes SMEs)	
• Participates in project activities. • Develops project deliverables, especially the change management plan and the communication management plan. • Develops and manages, along with the project manager, project change management processes, including requests for changes to project scope, budget, and schedule. • Develops training content, and trains the DMV personnel who will administer the DL/ID system. • Maintains version control over project deliverable documents. • Executes project-related organizational change management and communication initiatives. • Conducts organizational change readiness assessments as needed for the duration of the project. • Assists the vendor with development of the employee training plan.	DMV Vendor

6.5.5. Project Schedule

The proposed DL/ID project schedule is outlined in the table below.

Table 6-4. DL/ID Project Phases and Tasks

Phase	Task	Start	Finish	Deliverables
1	**Phase 1.0 FSR Development and Approval**			
1.1	Prepare and Submit FSR	01/16/06	05/17/06	• FSR submitted and approved • ITPP Report • BCP completed and submitted
1.2	Prepare and Submit ITPP	02/28/06	04/19/06	
1.3	Control Agency Review and Approval	04/13/06	06/07/06	
1.4	Prepare and Submit the BCP	05/18/06	09/18/06	
2	**Phase 2.0 RFP Development and Procurement**			

Phase	Task	Start	Finish	Deliverables
2.1	Develop RFP document	01/16/06	06/02/06	• DL/ID RFP completed and approved • RFP Released • Vendor selected
2.2	DGS Review and Approval	06/05/06	06/28/06	
2.3	Release RFP	06/29/06	06/29/06	
2.4	Vendor Selection	07/14/06	07/02/07	
2.5	Contract Award			
2.5.1	Prepare & Submit SPR	05/11/07	05/31/07	• SPR submitted and approved • DL/ID vendor contracted
2.5.2	DOF Review and Approval of SPR	06/01/07	07/02/07	
2.5.3	Issue "Notice of Intent to Award"	06/12/07	06/13/07	
2.5.4	Alternative Protest Period	06/14/07	07/30/07	
2.5.5	Award Contract	07/02/07	07/02/07	
3	**Phase 3.0 System Development and Implementation**			
3.1	Initiate Project	07/03/07	07/09/07	• Project Kick-Off meeting held • Project, issue, and risk management plans • Communications management plan • Business requirements & rules document • Design document completed • Development & test environments installed • Application developed and unit
3.2	Gather Requirements	07/10/07	08/06/07	
3.3	Design the System	08/07/07	10/02/07	
3.4	Develop the System	10/03/07	12/11/07	
3.5	Test the System			
3.5.1	Conduct Unit Testing	10/10/07	12/13/07	• System test plans and scripts • System test results • Integration test results • Performance test results • Parallel & security compliance test results • User acceptance
3.5.2	Conduct Integration Testing	12/14/07	01/02/08	
3.5.3	Conduct System & Regression Testing	01/03/08	01/23/08	
3.5.4	Conduct Performance Testing	01/03/08	01/22/08	
3.5.5	Conduct Parallel Testing	01/24/08	01/30/08	
3.5.6	Conduct User Acceptance Testing	01/31/08	02/14/08	
3.5.7	User Acceptance Sign-Off	02/14/08	02/14/08	
3.6	System Training			
3.6.1	Develop Policies and Procedures	12/14/07	01/16/08	• Policies and procedure documents • Training plan, curriculum, & materials
3.6.2	Develop Training Material	12/14/07	02/19/08	

4	**Phase 4.0 Implement the Solution**			
4.1	Install, Train, and Implement Group One Offices	02/20/08	03/03/08	• All offices trained • Group 1 offices implemented • Group 2 offices implemented • Group 3 offices implemented • Group 4 offices implemented • Issue new cards Statewide
4.2	Assess Group One Implementation	03/04/08	03/10/08	
4.3	Install, Train, and Implement Group Two Offices	03/11/08	03/24/08	
4.4	Assess Group Two Implementation	03/25/08	03/27/08	
4.5	Install, Train, and Implement Group Three Offices	03/28/08	04/15/08	
4.6	Assess Group Three Implementation	04/16/08	04/17/08	
4.7	Install, Train, and Implement Group Four Offices	04/18/08	05/07/08	
4.8	Assess Group Four Implementation	05/08/08	05/08/08	
4.9	Go Live all offices	05/08/08	05/08/08	
5	**Closeout and Post Implementation Review**			
5.1	Project Sign-off	06/30/08	06/30/08	• Final sign-off obtained • Contract closed • PIER completed
5.2	Close out Prior Contract	06/30/08	06/30/08	
5.3	Conduct PIER	10/15/08	04/13/09	

6.6. Project Monitoring

The DL/ID Project Management Team will monitor project progress. Key components of this monitoring include:

- **Weekly Project Team Meetings** and **Monthly Project Management Meetings**. These will include discussions of the project schedule, deliverable status, upcoming meetings, risks, and issues.
- **Weekly Project Status Reports**. These will be distributed to the project manager. It will report on the activities performed by all project team members during the previous week, including accomplishments, activities in progress, upcoming activities, issues, and deliverable status.
- **Independent Project Oversight** will be provided by an independent project oversight consultant, and compliant with DOF IT Project oversight recommendations.
- **Independent Verification and Validation** will be provided by an independent verification and validation consultant, and compliant with DOF IT Project oversight recommendations.

6.7. Project Quality

A structured approach is necessary to ensure that the DL/ID/SP Project is successful in meeting DMV's goals and objectives for quality assurance. The first step in ensuring project quality is developing clearly defined functional and technical requirements. They provide the benchmarks against which quality can be evaluated. Through assessment, validation, and testing, project results will then be measured against these requirements in order to ensure quality.

The DMV requires that project work products and deliverables satisfy project requirements and objectives with minimal errors and defects. In order to minimize the risk of receiving an unsatisfactory deliverable, a Deliverable Expectations Document (DED) will be prepared prior to the start of any major deliverable. The DED will ensure that all parties have a clear understanding of what is expected from the deliverable before work commences on it. The DED will contain the following information about the deliverable:

- Contract Number
- Deliverable Title
- Start and End Dates
- Description of Tasks and Deliverable
- Description of Acceptance Criteria
- Reviewers Sign-off

Additionally, internal DMV processes will continue to be tracked through the existing change control process. Upon completion of each deliverable, the DL/ID project manager will conduct a walkthrough with appropriate members of the project team and DMV management. Designated members of DMV management will be allowed a reasonable time to review each deliverable and either request changes or sign-off on them indicating that they are acceptable.

ISD will assist the DL/ID project team during the planning, analysis, and development activities in order to ensure that DL/ID collects and stores data according to DMV's standards. Additionally, ISD will coordinate and implement DMV system software changes, including those required for interfaces with the vendor's system.

DMV has published information technology standards for computers, infrastructure, web content, and system development methodology. The DL/ID project team will adhere to these standards wherever they are applicable.

6.8. Change Management

The DL/ID Project Management Team will identify and manage proposed changes to the project's scope, schedule, or resource requirements. This will be accomplished through a change management process that includes the following activities:

- The initiator submits a change request to the Change Management Team. This documents the scope, reason, budget impact, and schedule impact of the change. It must also identify the impact of not incorporating the change.
- The Change Management Team logs all change requests. The project manager evaluates them, and reviews them with impacted DMV and vendor personnel.
- The project manager then incorporates the change into the plan, rejects it, or submits it to the project sponsor or appropriate DMV management for a decision.
- As implementation nears, the Change Management Team develops an organizational change management and communication plan for review by the project sponsor. The project sponsor will coordinate with the steering committee to implement the plan and ensure effective communication and change management with the rest of the organization.

6.9. Authorization Required

The DL/ID Project requires the approval of the FSR by the DMV Project sponsor, the DMV executive management, and the Business Transportation & Housing Agency. The project also requires approval of the technical approach and expenditures from the California Department of Finance. In addition, approval of the procurement approach must be obtained from the California Department of General Services.

7. Risk Management Plan

Project risks are factors that jeopardize the successful accomplishment of project goals. Risk management is the systematic process of identifying, analyzing, and responding to project risks. This Risk Management Plan helps minimize the risks associated with the DL/IDSP project. It is presented in the following sections:

- Risk Management Approach
- Risk Management Worksheet
- Risk Tracking and Control

7.1. Risk Management Approach

The DMV's approach to risk management on the DL/ID/SP project includes:

- Identification of potential project issues and risks by the DL/ID/SP project team, the DL/ID/SP Internal and External Advisory Groups, DMV management, and vendors;
- Development of preventative risk mitigation strategies and contingency measures to avoid or minimize the impact of these potential issues and risks; and,
- Continuous monitoring of identified issues and risks through ongoing communications and reporting mechanisms.

DMV's risk management processes will comply with the Department of Finance's Information Technology Project Management Methodology. The DMV's approach is based on early detection, swift response, close monitoring, impact minimization, and thorough recovery. The costs of managing risks on the DL/ID/SP project are included in the Economic Analysis Worksheets presented in Section 8 of this report.

The DL/ID/SP project manager has the overall responsibility for risk management on the project, and will be supported in this responsibility by the DL/ID Project Management Team. The project manager and team members will have experience with the various DMV programs, and will receive assistance and advice from the DMV Project Management Office (PMO). The independent nature of the DMV PMO gives it the ability to work with the project team to identify, monitor, mitigate, and report project risk without conflicting interests. The DL/ID/SP Project Management Team will include the following key individuals:

- **Project Sponsor** – Has overall responsibility for the DL/ID Project. The project sponsor helps identify project risks, review and approve the risk management plan, regularly review the project issues log, and meet regularly with the project manager.

- **Project Manager** – Develops and maintains the Risk Management Plan and the issues log. The project manager has primary responsibility for monitoring project risks, developing risk mitigation strategies and contingency plans, and ensuring that these are implemented appropriately.
- **Independent Project Oversight Consultant** – Responsible for providing project oversight. The IPOC meets with the project sponsor, PMO and project manager on a regular basis to discuss the status of the project, including project risks. The IPOC may assist the project sponsor, PMO and project manager in identifying project risks and developing risk mitigation strategies and contingency plans.
- **Independent Verification and Validation Consultant** – Responsible for providing project independent verification and validation. The IV&V consultant meets with the project sponsor and project manager at least every month for proactive discussions regarding observed project risks and possible mitigation strategies.

7.1.1. Risk Assessment

The DL/ID project manager, with support from the project management team and subject matter experts, will be responsible for risk assessment. This consists of identifying, analyzing, quantifying, and prioritizing project and security risks. The project manager will determine the probability that specific risks will occur, and evaluate their potential impact. This will be an ongoing process throughout the life of the project. The three steps in Risk Assessment are: (1) Risk Identification, (2) Risk Analysis and Confirmation, and (3) Risk Prioritization. Each of these is briefly discussed below.

7.1.1.1 Risk Identification

Risk identification is the first step in risk assessment. It is the responsibility of all members of the DL/ID Project team, and consists of foreseeing potential risks as early as possible in the project. Initially, this is based on an understanding and analysis of project requirements and challenges in light of previous experience with similar projects. As the project progresses, and more specific experience is gained with the people, organizations, technologies, and the business environment associated with DL/ID/SP, additional risks will be identified, and the probability estimates of others may be adjusted.

Crucial to risk identification is the input of the project team and other stakeholders who will be encouraged to recognize and report risks as soon as possible. This will occur through formal means, such as status reports and meetings, as well as by less formal communications such as telephone calls and email messages. The DL/ID/SP project manager will document and evaluate risks identified by team members and stakeholders.

7.1.1.2 Risk Analysis and Quantification

Once a risk is identified, the DL/ID/SP project manager, in consultation with the project team, will evaluate the likelihood of the risk event occurring, and the probable outcomes associated with the risk event, in order to determine its probable impact on the success of the project.

7.1.1.3 Risk Prioritization

Risk prioritization is the final step in risk assessment. Based on the analysis of risk event likelihood and impact, the DL/ID/SP project manager will prioritize the risks so that attention and resources are applied to reducing the likelihood and/or minimizing the impact of the highest priority risks. Risks that are less likely to occur and/or will have relatively low impact if they do occur, will be assigned a lower priority. They will be monitored, but fewer resources will be applied to addressing them unless circumstances change their likelihood of occurrence or probable impact.

Some risks may cease to require attention because one or more of the following occur:

- Their likelihood of occurrence drops to zero percent;
- Their impact is determined to be negligible; or,
- They have already occurred, successful contingency measures have been implemented, and there is little risk of recurrence.

These are the lowest priority risks. They will be removed from the list of open risk issues and will no longer be actively managed by the project manager or DL/ID Project team. Nevertheless, a record will be maintained of these items, their impact (if any), and how they were addressed.

A Risk Priority Matrix like the one shown in Table 7-1, in conjunction with the Impact and Probability estimates documented in the Risk Management Worksheet (Table 7 2), will be used to prioritize risks.

Table 7-1. Risk Priority Matrix

Impact on Project Goals and Objectives	Probability of Occurrence	Risk Priority
High	80%-100%	**High**
	20%-79%	
	0%-19%	**Medium**
Medium	80%-100%	
	20%-79%	
	0%-19%	**Low**
Low	80%-100%	
	20%-79%	
	0%-19%	

7.1.2. Risk Response

This refers to the actions taken to manage risks. They include risk avoidance, acceptance, mitigation, and sharing. Each of these is discussed briefly below. In general, risk mitigation actions are undertaken for all high impact/high probability risks that cannot reasonably be avoided. When risk events do occur, DMV will have contingency plans in place to address them and minimize their negative impact on the project.

7.1.2.1 Risk Avoidance

This refers to eliminating the cause of the risk by modifying or selecting an alternate approach, technology, vendor, timeframe, or method that does not include the risk. Risk avoidance is often a key factor in initially selecting the proposed solution, but once a solution is selected, the risks inherent in it cannot usually be avoided without sacrificing important benefits. When planning the DL/ID implementation, the project manager and DL/ID project team will weigh the risks associated with all key project decisions (vendor, technology, schedule, etc.) in order to avoid or minimize risks whenever possible.

7.1.2.2 Risk Acceptance

Risk acceptance involves an organizational decision to accept a certain degree of risk, usually for technical or cost reasons. The DL/ID project manager and project team will evaluate the costs and benefits associated with all key project decisions in order to determine which risks should reasonably be accepted. For example, in addressing a particular risk they may have to weigh the probable impact of a particular risk event occurring against the cost of shifting some portion of the risk to a vendor, in order to determine how much of the risk DMV should accept.

7.1.2.3 Risk Mitigation

In the context of this DL/ID Risk Management Plan, *risk mitigation* refers to actions taken to minimize the probability of a risk event occurring (in contrast to *contingency plans*, which attempt to minimize the negative impact of risk events that do occur). For example, in addressing the risk that a vendor may not deliver needed equipment on time, a risk mitigation action may be to order the equipment ahead of schedule. A contingency plan may be to have an alternate source of the equipment if the primary vendor still fails to deliver on time. The Risk Management Worksheet (Table 7-2) lists both risk mitigation actions and contingency plans.

7.1.2.4 Risk Sharing

Risk sharing involves shifting some of the risk to other stakeholders (such as vendors). This is often possible, but can result in increasing the project cost. For example, a risk may be that ISD's help desk will be overwhelmed with calls when the new DL/ID component goes on line. DMV may elect to accept this risk (and perhaps shift additional internal resources to the help line at that time), or to share this risk by contracting with the vendor to handle some or all of these calls.

7.2. Risk Management Worksheet

The Risk Management Worksheet that follows (Table 7-2) is a key tool in tracking, managing, and reporting on project risks. It lists the major risks associated with the DL/ID project, and groups them into the following risk categories:

- Resources
- Schedule
- Scope
- Product/Technology
- Organization

It also includes an estimate of the likely impact on project success of each risk event, the estimated probability of occurrence, and a priority rating based on the Risk Priority Matrix *(Table 7-1)*. In addition, the areas impacted are identified (schedule, cost, functionality, and/or operations). Finally, specific strategies to reduce the likelihood or impact of each risk event are identified. Within each category, risks are sorted according to their priority. The content of this table will be updated regularly throughout the project.

Table 7-2. Risk Management Worksheet

ID	Risk Category or Event	Impact & Probability	Affected Areas	Preventive Strategies & Contingency Measures
1.0 Resources				
1.1	Pulling together the resources needed for DL/ID implementation may be difficult.	Impact: High Prob: 40% *Priority: High*	Cost Operations	▪ Obtain support from senior DMV management in order to ensure appropriate allocation of resources for DL/ID. ▪ Consider a shared-ownership model for DL/ID development and administration, in which various DL/ID stakeholders (across DMV branches and divisions) assign support resources to a central DL/ID team – while retaining control of those resources. ▪ Develop a resource management plan, obtain executive approval of the plan, and communicate the plan early, making sure to address staff concerns about their careers. The implementation of DL/ID may change the nature of their work, but will not result in job loss. ▪ Identify DL/ID team members early and plan for resources to temporarily backfill their work while they work on DL/ID. ▪ Minimize fluctuations in existing workload during DL/ID.
1.2	Departure, retirement or reassignment of DL/ID project staff, management, technical, and/or subject matter experts could delay project implementation.	Impact: Med. Prob: 25% *Priority: Med.*	Schedule	▪ Define roles and responsibilities for team members and identify backups for them. ▪ Ensure knowledge transfer between team members, subject matter experts, and their backups. ▪ Document key project and system information.

ID	Risk Category or Event	Impact & Probability	Affected Areas	Preventive Strategies & Contingency Measures
1.3	Vendor technical personnel may lack the skills required to implement the new system.	Impact: High Prob: 5% *Priority: Med.*	Operations Cost	▪ Require minimum skill sets of technical staff in the Request For Proposal. Vendor must submit resumes of all key personnel. ▪ Require that the vendor promptly replace personnel on DMV demand, allowing vendor personnel to be quickly moved off the project if necessary. ▪ Vendor must submit resumes of any replacement staff to DMV for review and approval.
1.4	The DL/ID vendor might go out of business, or otherwise be unable to provide ongoing support for DL/ID.	Impact: Med. Prob: 5% *Priority: Low*	Operations Cost	▪ Select a base product that is in use in other states (enhancing the probability that some vendor will continue to provide support). ▪ Obtain and train DMV technical personnel in order to develop the skills and knowledge needed to support the system. ▪ Contractually provide the means to obtain the source code and full system documentation in the event the vendor is unable to perform. ▪ Require vendor to submit financial statements, stakeholder reports, and bond. ▪ Ensure the Department of General Services and the Legal team review and approve the Qualifications Checklist that is required in the Request For Proposal.
2.0 Schedule				
2.1	There is a protest of the contract award.	Impact: High Prob: 90% *Priority: High*	Schedule Contract	▪ Ensure all procurement rules are followed. ▪ Specify clear, non-proprietary requirements. ▪ Conduct bidder conferences. ▪ Send RFP and contract to DMV and DGS legal counsel for review and approval. ▪ Utilize alternative protest procedures.

ID	Risk Category or Event	Impact & Probability	Affected Areas	Preventive Strategies & Contingency Measures
2.2	The project is not approved on time.	Impact: High Prob: 70% *Priority: High*	Schedule	▪ Establish early communication with the control agencies. ▪ Set up regular meetings with DMV Sponsor and Steering Committee to address urgent approval needs. ▪ Work with DGS prior to DOF approval of FSR.
2.3	The DL/ID vendor might fail to complete DMV-required customization and enhancements on schedule.	Impact: High Prob: 40% *Priority: High*	Schedule Functionality	▪ Provide the vendor with very clear, complete, and specific functional requirements. ▪ Incorporate financial penalties into the contract for failure of the vendor to perform as agreed. ▪ Ensure the vendor has timely and appropriate access to all required DMV systems, personnel, and information.
2.4	Contractor cannot meet the schedule.	Impact: High Prob: 30% *Priority: High*	Schedule Contract	▪ Allow sufficient time for the implementation process. ▪ Check vendor references thoroughly. ▪ Obtain contractual agreement to the project schedule. ▪ Include substantial penalties in the contract for late performance.
2.5	Installation of vendor hardware may be delayed.	Impact: High Prob: 20% *Priority: High*	Schedule Cost	▪ Ensure vendor installs required equipment timely. ▪ Develop project plan delineating detailed timeline. ▪ Communicate project deadlines regularly.
2.6	Contract not awarded on schedule.	Impact: High Prob: 20% *Priority: High*	Schedule Contract Resources	▪ Allow sufficient time for the procurement process. ▪ Establish an experienced evaluation team to review schedule options. ▪ Work with DGS early in the process.

ID	Risk Category or Event	Impact & Probability	Affected Areas	Preventive Strategies & Contingency Measures
2.7	The DMV design review process may take longer than anticipated. The time required to complete reviews, agree on system characteristics, and approve design decisions may increase due to the many DMV units impacted by DL/ID.	Impact: Med. Prob: 20% *Priority: Med.*	Schedule	▪ Establish review procedures that include clear timeframes for review completion. ▪ Establish issue resolution processes to quickly resolve disagreements on DL/ID functionality or other project characteristics. ▪ Plan for the vendor to proceed with selected components of the project if DMV takes longer than agreed to review the design or other documentation.
2.8	DMV personnel with the required business and technical expertise may not have sufficient time available to support the DL/ID implementation, thereby causing delays.	Impact: Med. Prob: 15% *Priority: Low*	Schedule Functionality	▪ Identify key resources and backups early in the process and obtain commitments from them and their management. ▪ Provide realistic estimates of the time required on DL/ID, and remind staff in advance as the need for their services approaches. ▪ When developing the DL/ID implementation schedule, consider other Department priorities and resource demands.

ID	Risk Category or Event	Impact & Probability	Affected Areas	Preventive Strategies & Contingency Measures
2.9	The number of organizational units and systems impacted by DL/ID may result in project planning, scheduling, and coordinating issues that delay project completion.	Impact: Low Prob: 25% *Priority: Low*	Schedule	▪ Develop and share an approved project charter. ▪ Develop a detailed and realistic project plan and ensure that all participants know and accept their responsibilities. ▪ Establish clear project phases and milestones and carefully monitor their timely completion. ▪ Ensure that DMV management and DL/ID project team members are committed to the project and work together. ▪ Ensure that the selected vendor dedicates appropriate resources to the project and plans sufficient time on-site at DMV. ▪ Communicate the approved issue resolution process. ▪ Rely on a steering committee to resolve escalated issues quickly. ▪ Communicate regularly with all key parties.
3.0 Scope				
3.1	Changing requirements may delay project implementation.	Impact: High Prob: 60% *Priority: High*	Schedule Cost	▪ Clearly identify, document, and communicate the functionality DL/ID will (and will not) provide. ▪ Agree on and incorporate a structured change management process.
3.2	Different expectations for DL/ID among various stakeholders may cause frustration with the capabilities of the system as implemented.	Impact: Med. Prob: 30% *Priority: Med*	Functionality Operations	▪ Clearly identify, document, and communicate the functionality DL/ID will (and will not) provide. ▪ Obtain buy-off from stakeholders early on in the project to avoid conflicting expectations.
3.3	Contractor does not meet quality, security or production requirements.	Impact: High Prob: 10% *Impact: Med.*	Functionality Schedule	▪ Check vendor references thoroughly. ▪ Include RFP and contract provisions that are clear as to these standards. ▪ Include penalty provisions in the contract.

ID	Risk Category or Event	Impact & Probability	Affected Areas	Preventive Strategies & Contingency Measures
4.0 Product/Technical				
4.1	Developing interfaces between DL/ID and other systems may present unforeseen technical difficulties.	Impact: High Prob: 25% *Priority: High*	Schedule Functionality	▪ Work early and closely with ISD. ▪ Include personnel responsible for systems with which DL/ID must interface in the DL/ID project team. ▪ Clearly document the DL/ID interface requirements.
4.2	Less than thorough and complete documentation of requirements may result in DL/ID lacking required functionality.	Impact: High Prob: 20% *Priority: High*	Functionality Schedule Cost	▪ Thoroughly document functional requirements in the Request for Proposal (RFP). ▪ Select a vendor experienced with card issuance (and therefore, less likely to omit or misunderstand a core requirement). ▪ Involve DMV subject matter experts throughout the process. Provide opportunities for them to review the system design, in detail, early on, in order to verify that required functionality is included.
4.3	A DL/ID vendor and/or product may be selected that fails to meet DMV's requirements in one or more key areas.	Impact: High Prob: 20% *Priority: High*	Functionality Cost Operations	▪ Gather as much information as possible from other states regarding their experiences with the vendors under consideration. ▪ Obtain demonstrations and hands-on experience, if possible, with the systems under consideration. ▪ Ensure that key DMV technical and business personnel have the opportunity to meet with and question vendors. Obtain and carefully consider their concerns and impressions. ▪ Ensure that vendor compensation is clearly tied to delivering a functioning and usable system that meets documented requirements.
4.4	DL/ID may be unable to adequately support future State or federal programs or new program requirements.	Impact: High Prob: 15% *Priority: Med.*	Functionality Operations	▪ Include contract terms which allow the DL/ID solution to be flexible and expandable.

ID	Risk Category or Event	Impact & Probability	Affected Areas	Preventive Strategies & Contingency Measures
4.5	Card production systems malfunction.	Impact: High Prob: 10% *Priority: High*	Functionality	▪ Perform thorough system testing. ▪ Carefully review vendor qualifications. ▪ Check vendor references thoroughly. ▪ Identify specific quality, security and production requirements in the RFP. ▪ Operate dual system until new system is performing as required. ▪ Have maintenance agreement in place.
5.0 Organization				
5.1	Critical DMV business processes may be disrupted due to unforeseen problems experienced during the transition to the new DL/ID contract.	Impact: High Prob: 30% *Priority: High*	Operations	▪ Where practical, conduct parallel system testing prior to DL/ID implementation. ▪ Cut over to DL/ID in phases to limit the impact of any problems.

7.3. Risk Tracking and Control

This involves maintaining up-to-date risk status information. It is continuous throughout the project. The DL/ID project manager will track and control project risk using the Risk Management Worksheet, which may be expanded to include:

- Date the risk was identified
- Person/organization that identified the risk
- Timeframe (Short/Medium/Long)
- Priority
- Mitigation actions taken
- Contingency plans implemented
- Current status

7.3.1. Risk Tracking

Risk tracking involves monitoring risks and the progress toward risk event resolution. It includes providing accurate and timely information to the Project Management Team, and keeping the Risk Management Worksheet updated as new risk-related information becomes available and risks are addressed. Risks will be discussed in project staff meetings in order to identify new risks, plan mitigation strategies and contingency plans, and monitor the impact of risk events that have occurred. The project manager and Project Management Office track this information. Risk tracking and control information will be included in project status reports.

7.3.2. Risk Control

Risk control is necessary to ensure that the risk management plan is executed and risk events are addressed in a timely manner. The focus is on risk response actions. As risk events occur, the DL/ID project team will implement the appropriate contingency plans as outlined in the Risk Management Worksheet, which is, in turn, updated with the results of these actions and other relevant information. While the project manager will take the lead in this, the IV&V Consultant and the Independent Project Oversight Consultant have important roles in providing timely support and oversight of the risk control function.

8. Economic Analysis Worksheets

The worksheets included in this section provide a comprehensive analysis of the costs associated with the proposed solution for DL/ID/SP card production. Instructions for the Economic Analysis Worksheets require full analysis of those alternatives that "satisfactorily meet the objectives and functional requirements." As a result cost worksheets associated with Alternatives 1 and 2 are included.

The EAWs present estimated personnel years (PYs) and costs for Fiscal Years (FYs) 2005-06 through 2008-09, representing the one-time project costs and the first full year of maintenance and operations (M&O) for DL/ID/SP card production.

This section presents the assumptions made to prepare the cost sheets pursuant to the EAW Package Guidelines. The EAW Worksheets are presented as follows:

1. Existing System/Baseline Cost Worksheet
2. Proposed Alternative: Procure Contractor-Provided Solution for Centralized Issuance
3. Alternative 1: Contractor-Provided Over-The-Counter Issuance
4. Alternative 2: DMV-Owned Over-The-Counter Issuance
5. Economic Analysis Summary
6. Project Funding Plan

8.1. Existing System Cost Worksheet

All existing costs are based on estimated staffing allocations and dollars budgeted in support of DL/ID/SP card production.

8.1.1. Existing Information Technology Costs

The costs in this category include salaries and benefits for 0.7 IT staff, as follows:

Table 8-1. Existing IT Staff

IT Staff (Class Title & Duties)	PY
Information Systems Technician Specialist I - Processes card request holding file extract	0.34
Management Services Technician - Prepares daily statistical reports	0.14
Staff Information Systems Analyst, Specialist - Performs problem resolution for file extract	0.11

IT Staff (Class Title & Duties)	PY
Senior Information Systems Analyst (Supervisor) - Performs problem resolution for file extract	0.04
Staff Information Systems Analyst, Specialist - Performs network installs & resolves problems	0.04
Systems Software Specialist I (Technical) - Resolves data transfer problems between VCS & RS6000	0.04
Total Continuing IT Staff Costs	**0.7**

This category also includes costs associated with card production. The costs are based on $0.65 per card plus sales tax of 7.75 percent at a volume of 8,596,000 cards per year.

8.1.2. Existing Program Costs

The costs in this category are comprised of salaries and benefits for 1.3 program staff previously described in Table 4-1.

8.2. Proposed Alternative Cost Worksheet

The total cost (one-time and ongoing) of this solution is estimated at $11,418,004 based on the assumptions outlined in the following subsections.

8.2.1. One-Time IT Project Costs

DMV estimated the level of staff effort from project initiation through implementation at 6.5 PYs in 2006-07 and 9.2 PYs in 2007-08. These project staff will be involved within the project structure outlined in Figure 6-1. The dollars were estimated based on hourly costs associated with a given classification (including benefits). Due to the short duration for the project, DMV will not request backfill of these resources. Any additional one-time DMV costs attributable to the document image capture required under REAL ID will be determined and included in the REAL ID FSR/SPR.

8.2.1.1 Contract Services

This category includes $147,054 for IPOC services, $73,971 for IV&V services and $74,705 for training in Fiscal Year 2007-08. The amount allocated for IV&V/IPOC services is estimated to be five percent of one-time staff resources and the total estimated cost for of the imaging solution over the five year term of the contract. The training allocation is meant to cover overtime for four hours of training for 29 Motor

Vehicle Technicians and 755 Motor Vehicle Field Representatives on a Saturday. In Fiscal Year 2006-07, $80,000 has been budgeted for DGS procurement support services.

8.2.1.2 One-Time Facilities

This category includes costs attributable to spaces for five vendor staff to be on-site at DMV HQ. The costs include $5,000 for modular systems furniture and $1,500 for electrical and cabling per workstation for a total cost of $32,500 for five workstations.

8.2.1.3 One-Time Telecommunications

This category includes costs for the installation of two T-1 lines and one DS3 circuit for a new vendor totaling approximately $15,000

8.2.2. Continuing IT Project Costs

Total ongoing IT project costs for the solution are estimated at approximately $8,467,324 following the assumptions outlined below. Any additional ongoing DMV IT costs attributable to the document image capture required under REAL ID will be determined and included in the REAL ID FSR/SPR.

8.2.2.1 Staff

The same resources currently supporting the DL/ID/SP card production will continue to support the proposed solution.

8.2.2.2 Telecommunications

It is expected that these costs will not change from the current rate of $75,720.

8.2.2.3 Contract Services

One-time contractor costs will be paid through a per card rate. This cost is projected to be $0.90 plus 7.75 percent sales tax per card. The total is based on the volume outlined in Section 8.1.1. The assumptions made to estimate the cost include:

- DMV determined that the solution it was seeking, including automated biometric comparisons, exists in Colorado. A weighted average method was used to compare California's costs to other states the size of Colorado. Since California's costs seemed to be 58 percent lower due to volume, the Colorado cost was adjusted to reflect this and yielded an $0.84 per card cost.

- Although DMV will look to the vendor to propose the best technical solution, some assumptions were made to estimate a per card cost for the document image capture solution. These assumptions include:
  - That 965 relatively small scanners will service the 2,490 workstations and VCS stations Statewide.
  - The average cost for a scanner including refresh will be approximately $1,600. This average is based on six models.
  - The average cost for support will be approximately $988 per scanner. This average is based on published rates from three companies.
  - Thin client software costs will be less than $100 per client (2,490 clients) for a total cost of $207,500.

8.2.2.4 Data Center Services

It is expected that these costs will not change from the current rate of $5,327.

8.2.3. Continuing Existing Costs

These costs are not expected to change except that IT support of the solution has been shifted from the "existing" category to the "continuing" category.

8.3. Alternative 1: Contractor Over-The-Counter Issuance

This alternative assumes average costs of $1.50 per card plus sales tax, based on costs for other states with over-the-counter issuance. The total cost of this solution is $17,663,267 for one-time and one year of ongoing costs.

8.4. Alternative 2: DMV-Owned Over-The-Counter-Issuance

This alternative assumes average costs of $1.78 per card based on costs for the only state available as an example: Arizona. The total cost of this solution is estimated at $28,037,550 for one-time and one year of ongoing costs.

8.5. Economic Analysis Summary

This worksheet summarizes existing system/baseline, proposed solution, and alternative costs.

8.6. Project Funding Plan Worksheet

This worksheet summarizes the costs and redirections previously discussed, and summarizes the funding plan for the project.

Table 8-2. Existing Baseline Costs

EXISTING SYSTEM/BASELINE COST WORKSHEET

Department: Motor Vehicles — All costs to be shown in whole (unrounded) dollars. — Date Prepared: May 31, 2006

Project: Driver License / Identification / Salesperson License Contract

	FY 2005/06		FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		SUBTOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
Continuing Information Technology Costs												
Staff (salaries & benefits)	0.7	50,306	0.7	50,306	0.7	50,306	0.7	50,306	0.0	0	**2.8**	**201,224**
Hardware Lease/Maintenance		0		0		0		0		0		**0**
Software Maintenance/Licenses		0		0		0		0		0		**0**
Contract Services		6,020,424		6,020,424		6,020,424		6,020,424		0		**24,081,696**
Data Center Services		5,327		5,327		5,327		5,327		0		**21,308**
Agency Facilities		0		0		0		0		0		**0**
Other (Telecommunications)		75,720		75,720		75,720		75,720		0		**302,880**
Total IT Costs	**0.7**	**6,151,777**	**0.7**	**6,151,777**	**0.7**	**6,151,777**	**0.7**	**6,151,777**	**0.0**	**0**	**2.8**	**24,607,108**
Continuing Program Costs:												
Staff	1.3	$115,397	1.3	115,397	1.3	115,397	1.3	115,397	0.0	0	**5.2**	**461,588**
Other		0		0		0		0		0		**0**
Total Program Costs	**1.3**	**115,397**	**1.3**	**115,397**	**1.3**	**115,397**	**1.3**	**115,397**	**0.0**	**0**	**5.2**	**461,588**
TOTAL EXISTING SYSTEM COSTS	**2.0**	**6,267,174**	**2.0**	**6,267,174**	**2.0**	**6,267,174**	**2.0**	**6,267,174**	**0.0**	**0**	**8.0**	**25,068,696**

Table 8-3. Proposed Solution Economic Analysis Worksheet

PROPOSED ALTERNATIVE: **Procure New Contract**

Date Prepared: June 14, 2006

Department: Motor Vehicles

All Costs Should be shown in whole (unrounded) dollars.

Project: Driver License / Identification / Salesperson License Contract

	FY 2005/06		FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		SUBTOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs												
Staff (Salaries & Benefits)*	0.0	0	6.5	611,655	9.2	854,202	0.0	0	0.0	0	15.7	1,465,857
Hardware Purchase		0		0		0		0		0		0
Software Purchase/License		0		0		0		0		0		0
Telecommunications		0		0		15,000		0		0		15,000
Contract Services												
Software Customization		0		0		0		0		0		0
Project Management Support		0		0		0		0		0		0
Project Oversight		0		0		147,054		0		0		147,054
IV&V Services		0		0		73,971		0		0		73,971
Other Contract Services (DGS)		0		80,000		0		0		0		80,000
TOTAL Contract Services		0		80,000		221,025		0		0		301,025
Data Center Services		0		0		0		0		0		0
Agency Facilities		0		0		32,500		0		0		32,500
Training		0		0		74,705		0		0		74,705
Total One-time IT Costs	**0.0**	**0**	**6.5**	**691,655**	**9.2**	**1,197,432**	**0.0**	**0**	**0.0**	**0**	**15.7**	**1,889,087**
Continuing IT Project Costs												
Staff (Salaries & Benefits)	0.0	0	0.0	0	0.0	0	0.7	50,306	0.0	0	0.7	50,306
Hardware Lease/Maintenance (Storage)		0		0		0		0		0		0
Software Maintenance/Licenses		0		0		0		0		0		0
Telecommunications		0		0		18,930		75,720		0		94,650
Contract Services		0		0		1,041,997		8,335,971		0		9,377,968
Data Center Services		0		0		666		5,327		0		5,993
Agency Facilities		0		0		0		0		0		0
Other		0		0		0		0		0		0
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**1,061,593**	**0.7**	**8,467,324**	**0.0**	**0**	**0.7**	**9,528,917**
Total Project Costs	**0.0**	**0**	**6.5**	**691,655**	**9.2**	**2,259,025**	**0.7**	**8,467,324**	**0.0**	**0**	**16.4**	**11,418,004**
Continuing Existing Costs												
Information Technology Staff	0.7	50,306	0.7	50,306	0.7	50,306	0.0	0	0.0	0	2.1	150,918
Other IT Costs		6,101,471		6,101,471		5,329,322		0		0		17,532,264
Total Continuing Existing IT Costs	**0.7**	**6,151,777**	**0.7**	**6,151,777**	**0.7**	**5,379,628**	**0.0**	**0**	**0.0**	**0**	**2.1**	**17,683,182**
Program Staff	1.3	115,397	1.3	115,397	1.3	115,397	1.3	115,397	0.0	0	5.2	461,588
Other Program Costs		0		0		0		0		0		0
Total Continuing Existing Program Costs	**1.3**	**115,397**	**1.3**	**115,397**	**1.3**	**115,397**	**1.3**	**115,397**	**0.0**	**0**	**5.2**	**461,588**
Total Continuing Existing Costs	**2.0**	**6,267,174**	**2.0**	**6,267,174**	**2.0**	**5,495,025**	**1.3**	**115,397**	**0.0**	**0**	**7.3**	**18,144,770**
TOTAL ALTERNATIVE COSTS	**2.0**	**6,267,174**	**8.5**	**6,958,829**	**11.2**	**7,754,050**	**2.0**	**8,582,721**	**0.0**	**0**	**23.7**	**29,562,774**
INCREASED REVENUES		0		0		0		0		0		**0**

Table 8-4. Alternative 1 Economic Analysis Worksheet

ALTERNATIVE #1: Contractor Over-the-Counter Issuance

Date Prepared: June 14, 2006

Department: Motor Vehicles

All Costs Should be shown in whole (unrounded) dollars.

Project: Driver License / Identification / Salesperson License Contract

	FY 2005/06		FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		SUBTOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs												
Staff (Salaries & Benefits)	0.0	0	6.5	611,655	9.2	854,202	0.0	0	0.0	0	15.7	1,465,857
Hardware Purchase		0		0		0		0		0		0
Software Purchase/License		0		0		0		0		0		0
Telecommunications		0		0		15,000		0		0		15,000
Contract Services												
Software Customization		0		0		0		0		0		0
Project Management		0		0		0		0		0		0
Project Oversight		0		0		147,054		0		0		147,054
IV&V Services		0		0		73,971		0		0		73,971
Other Contract Services (DGS)		0		80,000		0		0		0		80,000
TOTAL Contract Services		0		80,000		221,025		0		0		301,025
Data Center Services		0		0		0		0		0		0
Agency Facilities		0		0		32,500		0		0		32,500
Training		0		0		74,705		0		0		74,705
Total One-time IT Costs	**0.0**	**0**	**6.5**	**691,655**	**9.2**	**1,197,432**	**0.0**	**0**	**0.0**	**0**	**15.7**	**1,889,087**
Continuing IT Project Costs										0		
Staff (Salaries & Benefits)	0.0	0	0.0	0	0.0	0	0.7	50,306		0	0.7	50,306
Hardware Lease/Maintenance		0		0		0		0		0		0
Software Maintenance/Licenses		0		0		0		0		0		0
Telecommunications		0		0		18,930		75,720		0		94,650
Contract Services		0		0		1,787,603		13,837,712		0		15,625,315
Data Center Services		0		0		666		5,327		0		5,993
Agency Facilities		0		0		0		0		0		0
Other		0		0		0		0		0		0
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**1,807,199**	**0.7**	**13,969,065**	**0.0**	**0**	**0.7**	**15,776,264**
Total Project Costs	**0.0**	**0**	**6.5**	**691,655**	**9.2**	**3,004,631**	**0.7**	**13,969,065**	**0.0**	**0**	**16.4**	**17,665,351**
Continuing Existing Costs												
Information Technology Staff	0.7	50,306	0.7	50,306	0.7	50,306	0.0	0	0.0	0	2.1	150,918
Other IT Costs		6,101,471		6,101,471		5,329,322		0		0		17,532,264
Total Continuing Existing IT Costs	**0.7**	**6,151,777**	**0.7**	**6,151,777**	**0.7**	**5,379,628**	**0.0**	**0**	**0.0**	**0**	**2.1**	**17,683,182**
Program Staff	1.3	115,397	1.3	115,397	1.3	115,397	1.3	115,397	0.0	0	5.2	461,588
Other Program Costs		0		0		0		0		0		0
Total Continuing Existing Program Costs	**1.3**	**115,397**	**1.3**	**115,397**	**1.3**	**115,397**	**1.3**	**115,397**	**0.0**	**0**	**5.2**	**461,588**
Total Continuing Existing Costs	**2.0**	**6,267,174**	**2.0**	**6,267,174**	**2.0**	**5,495,025**	**1.3**	**115,397**	**0.0**	**0**	**7.3**	**18,144,770**
TOTAL ALTERNATIVE COSTS	**2.0**	**6,267,174**	**8.5**	**6,958,829**	**11.2**	**8,499,656**	**2.0**	**14,084,462**	**0.0**	**0**	**23.7**	**35,810,121**
INCREASED REVENUES		0		0		0		0		0		**0**

Table 8-5. Alternative 2 Economic Analysis Worksheet

ALTERNATIVE #2: DMV Owned System & Instant Over-the-Counter Issuance

Date Prepared: June 14, 2006

Department: Motor Vehicles

All Costs Should be shown in whole (unrounded) dollars.

Project: Driver License / Identification / Salesperson License Contract

	FY 2005/06		FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		SUBTOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs												
Staff (Salaries & Benefits)	0.0	0	6.5	611,655	64.6	5,930,621	0.0	0	0.0	0	71.1	6,542,276
Hardware Purchase		0		0		3,670,541		0		0		3,670,541
Software Purchase/License		0		0		0		0		0		0
Telecommunications		0		0		15,000		0		0		15,000
Contract Services												
Software Customization		0		0		0		0		0		0
Project Management		0		0		0		0		0		0
Project Oversight		0		0		147,054		0		0		147,054
IV&V Services		0		0		73,971		0		0		73,971
Other Contract Services (DGS)		0		80,000		0		0		0		80,000
TOTAL Contract Services		0		80,000		221,025		0		0		301,025
Data Center Services		0		0		0		0		0		0
Agency Facilities		0		0		32,500		0		0		32,500
Training		0		0		74,705		0		0		74,705
Total One-time IT Costs	**0.0**	**0**	**6.5**	**691,655**	**64.6**	**9,896,893**	**0.0**	**0**	**0.0**	**0**	**71.1**	**10,588,548**
Continuing IT Project Costs										0		
Staff (Salaries & Benefits)	0.0	0	0.0	0	0.0	0	0.7	50,306		0	0.7	50,306
Hardware Lease/Maintenance		0		0		0		0		0		0
Software Maintenance/Licenses		0		0		0		0		0		0
Telecommunications		0		0		18,930		75,720		0		94,650
Contract Services		0		0		1,922,238		15,377,900		0		17,300,138
Data Center Services		0		0		666		5,327		0		5,993
Agency Facilities		0		0		0		0		0		0
Other		0		0		0		0		0		0
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**1,941,834**	**0.7**	**15,509,253**	**0.0**	**0**	**0.7**	**17,451,087**
Total Project Costs	**0.0**	**0**	**6.5**	**691,655**	**64.6**	**11,838,726**	**0.7**	**15,509,253**	**0.0**	**0**	**71.8**	**28,039,634**
Continuing Existing Costs												
Information Technology Staff	0.7	50,306	0.7	50,306	0.7	50,306	0.0	0	0.0	0	2.1	150,918
Other IT Costs		6,101,471		6,101,471		5,329,322		0		0		17,532,264
Total Continuing Existing IT Costs	**0.7**	**6,151,777**	**0.7**	**6,151,777**	**0.7**	**5,379,628**	**0.0**	**0**	**0.0**	**0**	**2.1**	**17,683,182**
Program Staff	1.3	115,397	1.3	115,397	1.3	115,397	1.3	115,397	0.0	0	5.2	461,588
Other Program Costs		0		0		0		0		0		0
Total Continuing Existing Program Costs	**1.3**	**115,397**	**1.3**	**115,397**	**1.3**	**115,397**	**1.3**	**115,397**	**0.0**	**0**	**5.2**	**461,588**
Total Continuing Existing Costs	**2.0**	**6,267,174**	**2.0**	**6,267,174**	**2.0**	**5,495,025**	**1.3**	**115,397**	**0.0**	**0**	**7.3**	**18,144,770**
TOTAL ALTERNATIVE COSTS	**2.0**	**6,267,174**	**8.5**	**6,958,829**	**66.6**	**17,333,751**	**2.0**	**15,624,650**	**0.0**	**0**	**79.1**	**46,184,404**
INCREASED REVENUES		0		0		0		0		0		0

Table 8-6. Economic Analysis Summary

ECONOMIC ANALYSIS SUMMARY

Date Prepared: June 14, 2006

Department: Motor Vehicles
Project: Driver License / Identification / Salesperson License Contract

All costs to be shown in whole (unrounded) dollars.

	FY 2005/06		FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		SUBTOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
EXISTING SYSTEM												
Total IT Costs	0.7	6,151,777	0.7	6,151,777	0.7	6,151,777	0.7	6,151,777	0.0	0	2.8	24,607,108
Total Program Costs	1.3	115,397	1.3	115,397	1.3	115,397	1.3	115,397	0.0	0	5.2	461,588
Total Existing System Costs	2.0	6,267,174	2.0	6,267,174	2.0	6,267,174	2.0	6,267,174	0.0	0	8.0	25,068,696
PROPOSED ALTERNATIVE	**Procure New Contract**											
Total Project Costs	0.0	0	6.5	691,655	9.2	2,259,025	0.7	8,467,324	0.0	0	16.4	11,418,004
Total Cont. Exist. Costs	2.0	6,267,174	2.0	6,267,174	2.0	5,495,025	1.3	115,397	0.0	0	7.3	18,144,770
Total Alternative Costs	2.0	6,267,174	8.5	6,958,829	11.2	7,754,050	2.0	8,582,721	0.0	0	23.7	29,562,774
COST SAVINGS/AVOIDANCES	0.0	0	(6.5)	(691,655)	(9.2)	(1,486,876)	0.0	(2,315,547)	0.0	0	(15.7)	(4,494,078)
Increased Revenues		0		0		0		0		0		0
Net (Cost) or Benefit	0.0	0	(6.5)	(691,655)	(9.2)	(1,486,876)	0.0	(2,315,547)	0.0	0	(15.7)	(4,494,078)
Cum. Net (Cost) or Benefit	0.0	0	(6.5)	(691,655)	(15.7)	(2,178,531)	(15.7)	(4,494,078)	(15.7)	(4,494,078)		
ALTERNATIVE #1	**Contractor Over-the-Counter Issuance**											
Total Project Costs	0.0	0	6.5	691,655	9.2	3,004,631	0.7	13,969,065	0.0	0	16.4	17,665,351
Total Cont. Exist. Costs	2.0	6,267,174	2.0	6,267,174	2.0	5,495,025	1.3	115,397	0.0	0	7.3	18,144,770
Total Alternative Costs	2.0	6,267,174	8.5	6,958,829	11.2	8,499,656	2.0	14,084,462	0.0	0	23.7	35,810,121
COST SAVINGS/AVOIDANCES	0.0	0	(6.5)	(691,655)	(9.2)	(2,232,482)	0.0	(7,817,288)	0.0	0	(15.7)	(10,741,425)
Increased Revenues		0		0		0		0		0		0
Net (Cost) or Benefit	0.0	0	(6.5)	(691,655)	(9.2)	(2,232,482)	0.0	(7,817,288)	0.0	0	(15.7)	(10,741,425)
Cum. Net (Cost) or Benefit	0.0	0	(6.5)	(691,655)	(15.7)	(2,924,137)	(15.7)	(10,741,425)	(15.7)	(10,741,425)		
ALTERNATIVE #2	**DMV Owned System & Instant Over-the-Counter Issuance**											
Total Project Costs	0.0	0	6.5	691,655	64.6	11,838,726	0.7	15,509,253	0.0	0	71.8	28,039,634
Total Cont. Exist. Costs	2.0	6,267,174	2.0	6,267,174	2.0	5,495,025	1.3	115,397	0.0	0	7.3	18,144,770
Total Alternative Costs	2.0	6,267,174	8.5	6,958,829	66.6	17,333,751	2.0	15,624,650	0.0	0	79.1	46,184,404
COST SAVINGS/AVOIDANCES	0.0	0	(6.5)	(691,655)	(64.6)	(11,066,577)	0.0	(9,357,476)	0.0	0	(71.1)	(21,115,708)
Increased Revenues		0		0		0		0		0		0
Net (Cost) or Benefit	0.0	0	(6.5)	(691,655)	(64.6)	(11,066,577)	0.0	(9,357,476)	0.0	0	(71.1)	(21,115,708)
Cum. Net (Cost) or Benefit	0.0	0	(6.5)	(691,655)	(71.1)	(11,758,232)	(71.1)	(21,115,708)	(71.1)	(21,115,708)		

Table 8-7. Project Funding Plan

PROJECT FUNDING PLAN

Department: Motor Vehicles

All Costs to be in whole (unrounded) dollars

Date Prepared: June 14, 2006

Project: Driver License / Identification / Salesperson License Contract

	FY 2005/06		FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		SUBTOTALS	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
TOTAL PROJECT COSTS	**0.0**	**0**	**6.5**	**691,655**	**9.2**	**2,259,025**	**0.7**	**8,467,324**	**0.0**	**0**	**16.4**	**11,418,004**
RESOURCES TO BE REDIRECTED												
Staff	0.0	0	6.5	611,655	9.2	854,202	0.7	50,306	0.0	0	**16.4**	**1,516,163**
Funds:												
Existing System		0		0		772,149		6,101,471		0		**6,873,620**
Other Fund Sources		0		80,000		0		0		0		**80,000**
TOTAL REDIRECTED RESOURCES	**0.0**	**0**	**6.5**	**691,655**	**9.2**	**1,626,351**	**0.7**	**6,151,777**	**0.0**	**0**	**16.4**	**8,469,783**
ADDITIONAL PROJECT FUNDING NEEDED												
One-Time Project Costs	0.0	0	0.0	0	0.0	343,230	0.0	0	0.0	0	**0.0**	**343,230**
Continuing Project Costs	0.0	0	0.0	0	0.0	289,444	0.0	2,315,547	0.0	0	**0.0**	**2,604,991**
TOTAL ADDITIONAL PROJECT FUNDS NEEDED BY FISCAL YEAR	**0.0**	**0**	**0.0**	**0**	**0.0**	**632,674**	**0.0**	**2,315,547**	**0.0**	**0**	**0.0**	**2,948,221**
TOTAL PROJECT FUNDING	**0.0**	**0**	**6.5**	**691,655**	**9.2**	**2,259,025**	**0.7**	**8,467,324**	**0.0**	**0**	**16.4**	**11,418,004**
Difference: Funding - Costs	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	**0.0**	**0**

Total Estimated Cost Savings	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	**0.0**	**0**

Department: Motor Vehicles

Date Prepared: June 14, 2006

Project: Driver License / Identification / Salesperson License Contract

Annual Project Adjustments	FY 2005/06 PYs	FY 2005/06 Amts	FY 2006/07 PYs	FY 2006/07 Amts	FY 2007/08 PYs	FY 2007/08 Amts	FY 2008/09 PYs	FY 2008/09 Amts	FY 2009/10 PYs	FY 2009/10 Amts
One-time Costs										
Previous Year's Baseline	0.0	0	0.0	0	0.0	0	0.0	343,230	0.0	0
(A) Annual Augmentation /(Reduction)	**0.0**	**0**	**0.0**	**0**	**0.0**	**343,230**	**0.0**	**(343,230)**	**0.0**	**0**
(B) Total One-Time Budget Actions	0.0	0	0.0	0	0.0	343,230	0.0	0	0.0	0
Continuing Costs										
Previous Year's Baseline	0.0	0	0.0	0	0.0	0	0.0	289,444	0.0	2,315,547
(C) Annual Augmentation /(Reduction)	**0.0**	**0**	**0.0**	**0**	**0.0**	**289,444**	**0.0**	**2,026,103**	**0.0**	**(2,315,547)**
(D) Total Continuing Budget Actions	0.0	0	0.0	0	0.0	289,444	0.0	2,315,547	0.0	0
Total Annual Project Budget Augmentation /(Reduction) [A + C]	**0.0**	**0**	**0.0**	**0**	**0.0**	**632,674**	**0.0**	**1,682,873**	**0.0**	**(2,315,547)**

[A, C] Excludes Redirected Resources

Annual Savings/Revenue Adjustments

Cost Savings	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0
Increased Program Revenues		0		0		0		0		0

Appendix A. Acronyms

Term	Definition
AAMVA	American Association of Motor Vehicle Administrators
ANSI	American National Standards Institute
BD/LP	Birth Date/Legal Presence
CDLIS	Commercial Drive License Information System
CIDS	Card Image Database System
CMAS	California Multiple Award Schedule
COTS	Commercial Off The Shelf
CVC	California Vehicle Code
DED	Deliverable Expectation Document
DGS	Department of General Services
DL	Driver License
DLC	Driver License Compact
DOS	Disk Operating System
DMV	Department of Motor Vehicles
DMVA	Department of Motor Vehicles Automation
DOF	Department of Finance
DRM	Driver Record Master
DTS	Department of Technology Services
EDL	Event Driven Language
FO	Field Office
FSR	Feasibility Study Report
FTC	Federal Trade Commission
FTP	File Transfer Protocol
FY	Fiscal Year
HQ	Headquarters
ID	Identification Card
IFB	Invitation for Bid
IPOC	Independent Project Oversight Consultant
IPSO	Information Protection Services Office
ISD	Information Systems Division
ISO	International Standards Organization
ITPP	Information Technology Procurement Plan
IV&V	Independent Verification and Validation

Term	Definition
LAN	Local Area Network
M&O	Maintenance and Operations
MSA	Master Service Agreement
NDR	National Driver Register
NIST	National Institute of Standards and Technology
OL	Occupational Licensing
PDPS	Problem Driver Pointer System
PIER	Post Implementation Evaluation Report
PMBOK	Project Management Body of Knowledge
PMO	DMV Project Management Office
PVC	Permanent Virtual Circuit
QA	Quality Assurance
RFP	Request for Proposal
RJ	Registered Jack
SAM	State Administrative Manual
SAVE	Systematic Alien Verification for Entitlements
SIMM	Statewide Information Management Manual
SME	Subject Matter Expert
SP	Salesperson License
SPR	Special Project Report
SSOLV	Social Security On-Line Verification
TIS	Transaction Inventory System
VCS	Video Capture Station
VIS	Verification Information System
WORM	Write-Once-Read-Many
WSQ	Wavelet Scalar Quantization

Appendix B. AAMVA DL/ID Card Design Specifications Annex C: Security Device Index

Printed with permission from Rich Carter, Director, Technology Standards and Programs, AAMVA. Permission granted December 13, 2005.

The attached can also be located on the AAMVA web site at:
http://www.aamva.org/Documents/std2005DL-IDCardSpecV2FINAL.pdf

Appendix B. AAMVA DL/ID Card Design Specifications Annex C: Security Device Index

Printed with permission from Rich Carter, Director, Technology Standards and Programs, AAMVA. Permission granted December 13, 2005.

The attached can also be located on the AAMVA web site at:
http://www.aamva.org/Documents/std2005DL-IDCardSpecV2FINAL.pdf

American Association of Motor Vehicle Administrators (AAMVA)

Date: 2005-March

AAMVA Uniform ID Subcommittee - UID7 Task Group

Secretariat: AAMVA

Personal Identification — AAMVA International Specification — DL/ID Card Design

Annex C
(informative)

DL/ID Security Device Index

C.1 Introduction

The security device index was developed by AAMVA as a tool to aid in the security design of DL/ID documents and to insure full coverage of common threats to document integrity in North America. The index is designed to be inclusive of security devices available for DL/ID documents. The terms used in the index are written to the extent possible in generic terms rather than using trademarked names. Suggestions for updates should be sent to AAMVA's Standards Program for inclusion in subsequent iterations of this specification.

C.2 Threat Levels

Level 1 - A Level 1 security device supports first line inspection.

Level 2 – A Level 2 security device supports second line inspection.

C.3 Threat Types

Type 1 – Counterfeit/Simulation

Type 2 – Alteration

Type 3 – Photo Substitution

Type 4 – Cannibalization

(Refer to Annex B, section 7.1 for definitions of these terms.)

C.4 Printing

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a. Deliberate Errors/known flaws A feature is purposely made with an intentional mistake known only to the manufacturer or inspection officials.					X			
b. Duplex Patterns A design made up of an interlocking pattern of small irregular shapes, printed in two colors and requiring very close register printing in order to preserve the integrity of the image.	X	X		X	X	X		
c. Fine line background (Guilloche pattern)	X	X	X	X	X	X	X	X

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
A pattern of continuously fine lines constructed by using two or more lines in overlapping bands that repeat a lacy, web-like curve.								
d. Fine line foreground A pattern of continuously fine lines constructed by using two or more lines overlapping bands that repeat a lacy, web-like curve.	X	X	X	X	X	X	X	X
e. Front to back (see through) register A design printed on both sides of a card that forms an interlocking image when held to a light source.	X							
f. Ghost Image Half tone reproduction of the original image that is typically printed in the same area as, and behind, personal data.		X	X	X	X			X
g. Layered printing (on lamination) Printing separate elements of the secure design on different layers of the laminated card body materials so that no single layer contains all of the security features and the entire products is only apparent after lamination.	X	X		X				
h. Micro optical imaging Text, line art, gray scale images and multi—reflectivity images are engineered into optical WORM media at high resolution (over 12,000 dpi). Difficult to simulate the printing resolution.	X	X			X	X	X	
i. Microprinting / nanoprinting 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. Difficult to duplicate.					X			X
j. Moiré pattern (anti-scan/VOID pattern) A new pattern formed by the super positioning of two patterns whose periodicities are not identical. Security designs can be developed so that a scanner or copier will only display part of the pattern and/or word VOID or COPY appears instead of the pattern.					X	X	X	X

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
k. Non standard type fonts Special type that is not available on the commercial market and is reserved for security card use only.	X	X			X	X		
l. Rainbow printing Must demonstrate a controlled exacting color shift subtly in a linear continuous fashion. Accurately designed patterns cannot be easily copied or duplicated via scanning. It is applied using non-commercial method of printing. It is often used with a fine line or medallion pattern in the background of a card.	X							
m. Security code High-resolution color printing systems print a security code within the body of the color printed photo image. The code can be printed in a non-proportional font that can imbed characters on the edge or bottom of the printed picture.					X		X	

C.5 Inks

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a. Chemically Reactive Contains a security agent that is sensitive to chemicals, i.e., polar and non-polar solvents and bleach, commonly used to alter documents. The chemical reaction is for the ink to run, stain, and bleed to show evidence of document tampering.		X				X		
b. Infrared fluorescent Forms a visible image when illuminated with light in the infrared / red visible part of the spectrum.					X	X		
c. Infrared drop-out Forms a visible image when illuminated with light in the visible part of the spectrum, but cannot be detected in the infrared region.					X	X		

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
d. Metallic, pearlescent, and iridescent Inks that fluctuate in brilliance depending on the angle of illumination of the viewing. Difficult to mimic the luster and hard to copy or scan.	X	X	X					
e. Metameric The use of a pair of ink colors that differ in spectral composition but match one another under certain lighting conditions. Under incandescent light that may appear the same, but under colored light they appear as different colors.					X			
f. Phosphorescent Contains a pigment that glows when exposed to a light source of appropriate wavelength. The reactive glow decays after the light source is removed.					X	X		
g. Tagged Contains taggants or compounds that are not naturally occurring and that can be detected using special equipment that reacts to electromagnetic energy identifying the grouping or type.					X			
h. Thermochromatic Ink that exhibits a sharp, reversible color change when exposed to heat, i.e., finger rubbing or hot air.	X				X	X		
i. Ultraviolet fluorescence Invisible inks that emit visible color under exposure to ultraviolet light. Colors can be formulated that are not commercially available, making resistance to counterfeiting higher.					X	X	X	X

C.6 Substrate Inclusion

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a. Core inclusion The manufacture of card stock with different layers. A colored core material may be placed inside to create a colored edge along the card.	X							
b. Embedded thread, fiber or planchette Small, often fluorescent particles or platelets incorporated into a card material at the time of manufacture that can be seen later under certain lighting conditions. The embedded elements may have magnetic or other machine-readable properties that may be used to enhance the levels of security provided.					X	X		
c. Opacity mark Similar to a watermark, it is a plastic that contains a unique translucent mark.	X							
d. Security bonding The card periphery incorporates a security bonding material that bonds all of the layers together. Tamper evidence is seen if access is attempted to obtain the internal structures of the card.					X	X		X
e. Ultraviolet features Card bodies are made UV dull or possess a controlled response to UV light so they exhibit fluorescence that can be distinguished in color from the "blue" used in commonly available fluorescent materials.					X	X		

C.7 Optically Variable Devices (OVD)

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a.1 Metalized DOVID (Diffractive Image) Opaque metalized DOVID (diffractive optically variable image device). OVD authentication effects cannot be photo copied or digitally recreated. OVDs are holographically mastered or digitally mastered using computer-guided lasers or electron beams.	X	X	X					

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a.1.1 De-Metalized OVD (Diffractive Image) A combination of metal and transparency on the same foil or laminate. Hi resolution OVD has selective de-metallization, either transparent or opaque, as defined above.	X	X	X					
a.2. Transparent DOVID Transparent DOVID (diffractive optically variable image device). When incorporated into a driver license design, feature will not interfere with photo or data information. Transparent OVD authentication effects cannot be photo copied or digitally recreated. OVDs are holographically mastered or digitally mastered using computer-guided lasers or electron beams.	X	X	X					
b. Film - Color Shifting OVD Semi-transparent, multilayer light interference film creates noticeable, reflecting color shifts, i.e., clear to blue, magenta to blue, yellow to orange, etc. When incorporated into a driver license design, feature will minimally interfere with photo or data information. OVD color shifting effect cannot be photo copied or digitally recreated.	X	X	X					
c. Ink - Color Shifting OVD Printed opaque, multilayer light interference ink pigment creates noticeable, reflecting color shifts, i.e., gold to green, green to blue, etc. similar to what is seen on many global identification documents including driver licenses, banknotes, passports, and visas. The color shifting and authentication effect cannot be replicated or digitally recreated. Tightly controlled and only available for the most secure document applications.	X	X						
d. Liquid Crystal - Color Shifting OVD Semi-transparent, liquid crystal light interference layers create noticeable, reflecting color shifts, i.e., orange to green. When incorporated into a driver license design, feature will minimally interfere with photo or data information. OVD color shifting effect cannot be photo copied or digitally recreated.	X	X	X					

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
e. Personalized OVD OVD that is personalized for each card based upon biographical data, portrait, or signature of the cardholder.	X	X	X	X	X	X	X	X
f. Virtual Image OVD Transparent or semi-transparent virtual image appears to float above or sink below the surface of the document, as the viewing angle changes. When incorporated into a driver license design, feature will not interfere with photo or data information. OVD virtual image effect cannot be photo copied or digitally recreated.	X	X	X					

C.8 Additional Features

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a. Biometric feature (template) A biometric template of the customer's physical characteristics.					X	X	X	X
b. Covert Device – Readable and Storage Technology Unique individual Near IR or IR invisible data mark, 2-dimenional encrypted bar code, capable of storing independent information or details					X	X	X	X
c. Covert variable pixel manipulation Covert dot matrix images that are converted to visible text with a special reader or lens.					X	X	X	X
d. Digital Seal A method of securing and validating data by electronic means using digital signature technology. The issuing authority "signs" the information contained in the MRT .					X	X		X
e. Embedded Image					X	X	X	X

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
An image or information that is embedded or encoded within a primary visual image.								
f. Laminates (security) Transparent layers or films with an integrated security feature(s) are applied to the card with an adhesive or fused by heat. Available in a number of forms, security laminates are designed to be tamper evident and carry other security features to the card.	X	X	X	X				
g. Laser encoded optical image Image and text files are placed to an optical WORM media as a visible diffraction pattern image that is eye-readable under a variety of lighting conditions.	X	X	X					
h. Laser engraving The information cannot be mechanically or chemically removed without surface damage to the card. Can be used for photos, characters, bar codes, OCR, etc.	X	X	X			X		
i. Laser perforation Holes are made with the laser beam of images or objects. The image is visible when held up to a light source. It has a tactile feel with conical holes that are larger at the entrance than exit.	X	X	X	X				
j. Machine readable technology (MRT) Magnetic stripe, smart card, bar codes, OCR, optical WORM media, etc. Verifies the authenticity of the document, the data or the person presenting the card by the use of a reader and comparison of the stored data to other information.					X	X	X	X
k. Magnetic media fingerprinting Tracks unique, random patterns of magnetic media formed as a by-product manufacture of card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.					X	X		X
l. Optical media fingerprinting					X	X	X	X

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
Tracks unique, random patterns of optic media (e.g., fibers) on card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.								
m. Optical watermark Fine line images that are engineered into optical WORM medial with a very high resolution (12,000 dpi). The watermark is overwritten with a laser-encoded optical image, locking together a preformatted document security feature with a laser encoded personalization security feature.	X	X			X	X		X
n. Overlay An ultra-thin film or protective coating that may be applied to the surfaced of a card in place of a security laminate and which may contain optically variable features.	X	X	X	X				
o. Overlapping data Variable data, such as digitized signature, seals or text can be placed over another field such as a photo image. Both fields must be altered if a substitution is to take place making it more difficult.		X	X	X	X	X	X	X
p. Redundant data Display of data in more than one location on the card. A visual inspection may determine if all of the fields match. Usually, the data is displayed in a variety of colors and fonts to further deter alteration.		X						
q. Retroreflective device Optical constructions that reflect light such that covert logos become visible over the entire document when viewed using a focused light source or retroreflective viewer. Level 1 capability is based on a distinctive tactile quality.	X	X	X	X	X	X	X	X

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
r. Security threads Metal or plastic, these threads are seen on currency. With special metallized film, demetallized text is invisible in reflected light and therefore is difficult to copy. When viewed in transmitted light, the opaque aluminum letters are clearly visible.	X	X	X		X	X	X	X
s. Thin film interference filters Multiple layer structures that produced color effects by interference.					X			
t. Tactile feature A feature which is apparent to touch or feel without requiring a special instrument. This could include texture, flexibility, or weight of the document and/or a feature incorporated in the card structure or card components.	X	X						