DETAILED RISK ASSESSMENT REPORT

Executive Summary

During the period June 1, 2004 to June 16, 2004 a detailed information security risk assessment was performed on the Department of Motor Vehicle's Motor Vehicle Registration Online System ("MVROS").

The MVROS provides the ability for State vehicle owners to renew motor vehicle registrations, pay renewal fees, and enter change of address information.

The assessment identified several medium risk items that should be addressed by management.

DETAILED ASSESSMENT

1. Introduction

1.1 Purpose

The purpose of the risk assessment was to identify threats and vulnerabilities related to the Department of Motor Vehicles – Motor Vehicle Registration Online System ("MVROS"). The risk assessment will be utilized to identify risk mitigation plans related to MVROS. The MVROS was identified as a potential high-risk system in the Department's annual enterprise risk assessment.

1.2. Scope of this risk assessment

The MVROS system comprises several components. The external (customer) interface is a series of web pages that allow the user to input data and receive information from the application. The online application is a web-based application developed and maintained by the DMV. The application is built using Microsoft's Internet Information Server and uses Active Server Pages. The application has an interface with the motor vehicle registration database and with Paylink – an e-commerce payment engine provided by a third party vendor. DMV IT department hosts the application. The application components are physically housed in the DMV's data center in Anytown.

The scope of this assessment includes all the components described above except for Paylink. The Paylink interface – the component managed by DMV IT – is in scope. Also in scope are the supporting systems, which include: DMZ network segment and DMZ firewalls. The web application, DMV database and operating systems supporting these components are all in scope.

2. Risk Assessment Approach

2.1 Participants

Role	Participant
System Owner	John Smith
System Custodian	Mary Blue
Security Administrator	Tom Sample
Database Administrator	Elaine Ronnie
Network Manager	David Slim
Risk Assessment Team	Eric Johns, Susan Evans, Terry Wu

2.2 Techniques Used

Technique	Description
Risk assessment questionnaire	The assessment team used a customized version of the self-assessment questionnaire in NIST SP-26 “Security Self-Assessment Guide for Information Technology Systems”. This questionnaire assisted the team in identifying risks.
Assessment Tools	The assessment team used several security testing tools to review system configurations and identify vulnerabilities in the application. The tools included nmap, nessus, AppScan
Vulnerability sources	The team accessed several vulnerability sources to help identify potential vulnerabilities. The sources consulted included: • SANS Top 20 (www.sans.org/top20/) • OWASP Top 10 (www.owasp.org/documentation/topten.html) • NIST I-CAT vulnerability database (icat.nist.gov) • Microsoft Security Advisories (www.microsoft.com/security) • CA Alert service (www3.ca.com/securityadvisor)

Technique	Description
Transaction walkthrough	The assessment team selected at least one transaction (use case) of each type and walked each transaction through the application process to gain an understanding of the data flow and control points.
Review of documentation	The assessment team reviewed DMV security policies, system documentation, network diagrams and operational manuals related the MVROS.
Interviews	Interviews were conducted to validate information.
Site visit	The team conducted a site visit at the Data Center and reviewed physical access and environmental controls

2.3 Risk Model

In determining risks associated with the MVROS, we utilized the following model for classifying risk:

Risk = Threat Likelihood x Magnitude of Impact

And the following definitions:

Threat Likelihood

Likelihood (Weight Factor)	Definition
High (1.0)	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium (0.5)	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (0.1)	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Magnitude of Impact

Impact (Score)	Definition
High (100)	The loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals. Examples: • A severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions • Major damage to organizational assets • Major financial loss • Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Medium (50)	The loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals. • Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced • Significant damage to organizational assets • Significant financial loss • Significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low (10)	The loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals. Examples: • Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced • Minor damage to organizational assets • Minor financial loss • Minor harm to individuals.

Risk was calculated as follows:

	Impact		
Threat Likelihood	*Low (10)*	*Medium (50)*	*High (100)*
High (1.0)	Low Risk (10 x 1.0 = 10)	Medium Risk (50 x 1.0 = 50)	High Risk (100 x 1.0 = 100)
Medium (0.5)	Low Risk (10 x 0.5 = 5)	Medium Risk (50 x 0.5 = 25)	Medium Risk (100 x 0.5 = 50)
Low (0.1)	Low Risk (10 x 0.1 = 1)	Low Risk (50 x 0.1 = 5)	Low Risk (100 x 0.1 = 10)

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

3. System Characterization

3.1 Technology components

Component	Description
Applications	In-house developed uses Microsoft Active Server Pages running under Microsoft Internet Information Server 4.0
Databases	Microsoft SQL Server 2000
Operating Systems	Microsoft Windows NT version 4.0 SP 2
Networks	Checkpoint Firewall Cisco Routers
Interconnections	Interface to PayLink
Protocols	SSL used for transmission between client web browser and web server

3.2 Physical Location(s)

Location	Description
Data Center	260 Somewhere Street, Anytown
Help Desk	5500 Senate Road, Anytown
NOC	1600 Richmond Avenue, Anytown

3.3 Data Used By System

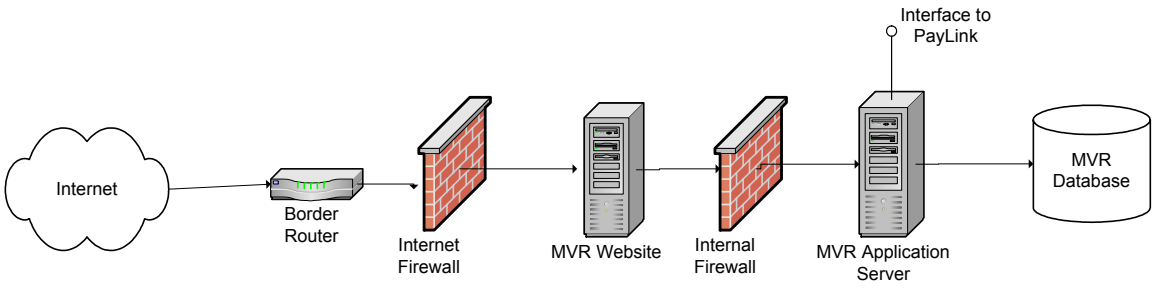
Data	Description
Personally identifiable information	Includes: • Name • Address (current and previous) • Phone Number • SSN # • DOB
Vehicle information	Includes • Vehicle identification number • Tag # • Date of last emissions test
Financial information	• Credit card # • Verification code • Expiry date • Card type • Authorization reference • Transaction reference
Tax	Registration fee

3.4 Users

Users	Description
State Vehicle Owners	Access the system via a web browser. Can renew vehicle registration provided they have a valid credit card. Can also enter change of address information.
DMV IT Personnel	Manage the MVROS system including firewalls and networks. Maintain security configuration of system.
DMV Operations	Utilize information contained in the MVR database for management reporting. Generate reports and database queries.
DMV Offices	Utilize the MVR application for in-person renewals.

3.5 Flow Diagram

The following diagram shows the in-scope technology components reviewed as part of the MVROS.



4. Vulnerability Statement

The following potential vulnerabilities were identified:

Vulnerability	Description
Cross-site scripting	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
SQL injection	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
Password strength	Passwords used by the web application are inappropriately formulated. Attackers could guess the password of a user to gain access to the system.
Unnecessary services	The web server and application server have unnecessary services running such as telnet, snmp and anonymous ftp

Vulnerability	Description
Disaster recovery	There are no procedures to ensure the ongoing operation of the system in event of a significant business interruption or disaster
Lack of documentation	System specifications, design and operating processes are not documented.
Integrity checks	The system does not perform sufficient integrity checks on data input into the system.

5. Threat Statement

The team identified the following potential threat-sources and associated threat actions applicable to the MVROS:

Threat-Source	Threat Actions
Hacker	• Web defacement • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	• Identity theft • Spoofing • System intrusion
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	• Browsing of personally identifiable information • Malicious code (e.g., virus) • System bugs • Unauthorized system access
Environment	• Natural disaster

5. Risk Assessment Results

{Note: Only partial list included in this example}

Item Number	Observation	Threat-Source/ Vulnerability	Existing controls	Likelihood	Impact	Risk Rating	Recommended controls
1	User system passwords can be guessed or cracked	Hackers/ Password effectiveness	Passwords must be alpha-numeric and at least 5 characters	Medium	Medium	Medium	Require use of special characters
2	Cross site scripting	Hackers/ Cross-site scripting	None	Medium	Medium	Medium	Validation of all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification of what should be allowed
3	Data could be inappropriately extracted/modified from DMV database by entering SQL commands into input fields	Hackers + Criminals / SQL Injection	Limited validation checks on inputs	High	Medium	Medium	Ensure that all parameters are validated before they are used. A centralized component or library is likely to be the most effective, as the code performing the checking should all be in one place. Each parameter should be checked against a strict format that specifies exactly what input will be allowed.
4	Web server and application server running unnecessary services	All / Unnecessary Services	None	Medium	Medium	Medium	Reconfigure systems to remove unnecessary services

Item Number	Observation	Threat-Source/ Vulnerability	Existing controls	Likelihood	Impact	Risk Rating	Recommended controls
5	Disaster recovery plan has not been established	Environment / Disaster Recovery	Weekly backup only	Medium	High	Medium	Develop and test a disaster recovery plan