OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Department of Public Safety

Web-based Motor Vehicle Registration Renewal System

As of April 2001

AUGUST 17, 2001 01-43

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota State government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately fifty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year and one best practices review.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of Representatives and Senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1727 (voice), or the Minnesota Relay Service at 651-297-5353 or 1-800-627-3529.

All OLA reports are available at our Web Site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, evaluation, or best practices review, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

OLA
OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Charlie Weaver, Commissioner
Department of Public Safety

We have conducted an information technology audit of the Web-based Motor Vehicle Registration Renewal System. Our audit assessed the adequacy of controls that protect the integrity and confidentiality of data and ensure the continued availability of the system. The individual chapters of this report discuss our specific objectives and the conclusions that we reached.

We conducted our audit in accordance with *Government Auditing Stan*dards, as issued by the Comptroller General of the United States. These standards require us to obtain an understanding of management controls relevant to the audit. They also require that we design the audit to provide reasonable assurance that the Department of Public Safety complied with the provisions of laws, regulations, contracts, and grants significant to the audit. Management of the department is responsible for establishing and maintaining the internal control structure and complying with applicable laws, regulations, contracts, and grants.

This report is intended for the information of the Legislative Audit Commission and the management of the Department of Public Safety. This restriction is not intended to limit the distribution of this report, which we released as a public document on August 17, 2001.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen
Deputy Legislative Auditor

End of Fieldwork: May 4, 2001

Report Signed On: August 14, 2001

Room 140, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Department of Public Safety
Web-based Motor Vehicle Registration Renewal System

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Christopher Buse, CPA, CISA, CISSP	Information Technology Audit Manager
Mark Mathison, CPA, CISA	Auditor-In-Charge
Eric Wion, CPA, CISA	Auditor
Neal Dawson	Auditor
Steve Johnson, CPA, CISA	Auditor

The following member of the Department of Administration's Electronic Government Services Support Group also provided us with assistance during this audit:

David Gillespie, CISSP	Information Technology Specialist

Exit Conference

The following staff from the Department of Public Safety participated in the exit conference held on August 2, 2001:

Janet Cain	Chief Information Officer
Sara Schlauderaff	Assistant Commissioner
Brian Lamb	Director, Driver and Vehicle Services
Bob Cheney	Support Services Director, Driver and Vehicle Services
Judith Franklin	Enterprise Technology Manager, Driver and Vehicle Services

Department of Public Safety
Web-based Motor Vehicle Registration Renewal System

Report Summary

Security weaknesses exposed sensitive data to a high risk of fraud, misuse, or inappropriate disclosure.

Conclusions:

The Department of Public Safety did not develop or implement an effective security infrastructure for the Web-based Motor Vehicle Registration Renewal System. The department did not formally identify and assess risks or document specific policies, procedures, and standards to appropriately secure the system. The security infrastructure that resulted was a collection of automated tools that lacked a cohesive policy foundation.

The 10 findings and 17 recommendations in this report address a broad array of security weaknesses. These findings highlight deficiencies in the department's:

- organization and planning of the system;
- system development methodology;
- day to day security and support activities; and
- monitoring.

Collectively, these security weaknesses leave the system and its data vulnerable to tampering, disruption, and misuse from both internal and external sources.

Background:

On October 18, 2000, the Department of Public Safety unveiled a new system that gave citizens the ability to renew their motor vehicle license tabs over the Internet. Using a standard web browser, such as Netscape's Navigator or Microsoft's Internet Explorer, citizens now can pay their registration renewal fees from the convenience of their home.

Financial-Related Audit Reports address internal control weaknesses and noncompliance issues found during our audits of state departments and agencies. The scope of our work at the Department of Public Safety was limited to a review of controls that protect the integrity and confidentiality of data on the Web-based Motor Vehicle Registration Renewal System.

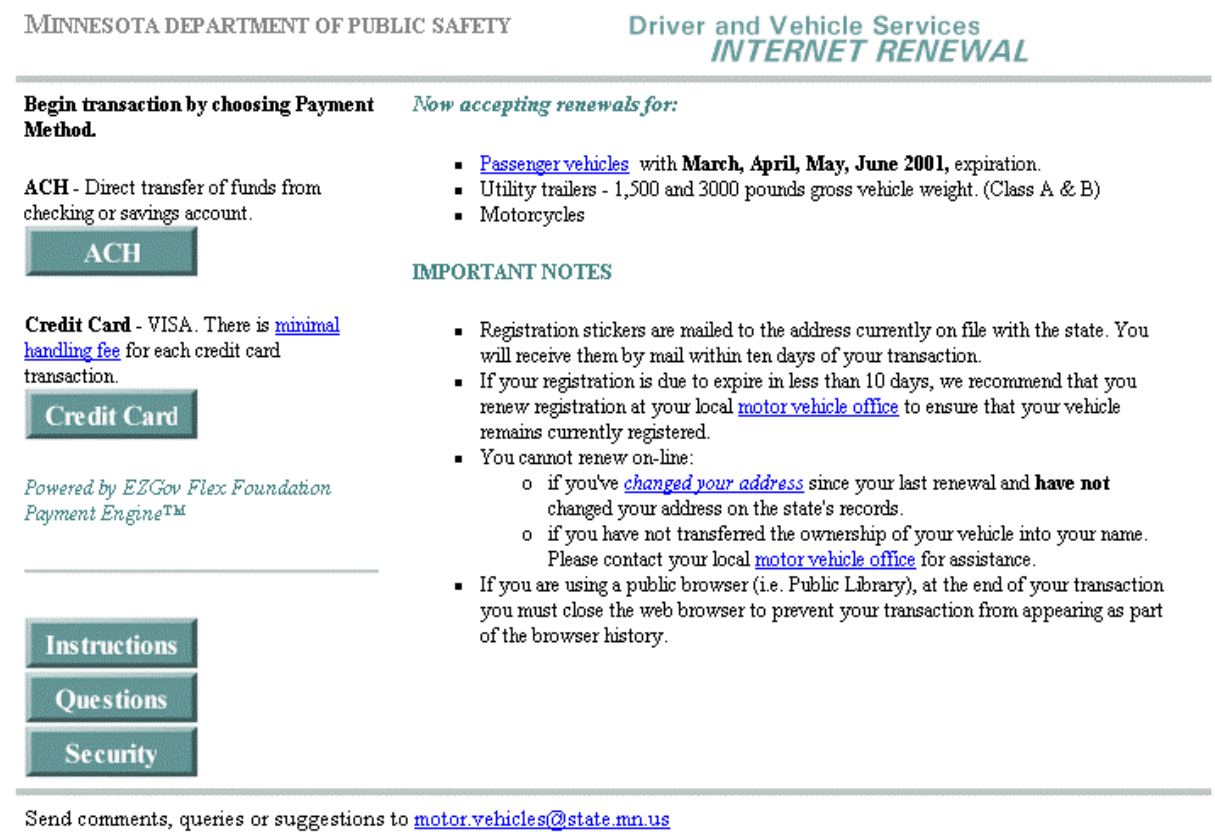
This page intentionally left blank.

Chapter 1. Introduction

This information technology audit assessed the adequacy of controls in the Web-based Motor Vehicle Registration Renewal System as of April 2001. On October 18, 2000, the Department of Public Safety unveiled a new system that gave citizens the ability to renew their motor vehicle license tabs over the Internet. Using a standard web browser, such as Netscape's Navigator or Microsoft's Internet Explorer, citizens now can pay their registration renewal fees from the convenience of their home.

Citizens can access this new system from the State of Minnesota's home page, commonly referred to as "North Star." The North Star portal brings citizens to the Department of Public Safety's web site, which houses the new Web-based Motor Vehicle Registration Renewal System. Figure 1-1 depicts the first screen that citizens encounter. This screen contains detailed instructions to help citizens who are unfamiliar with the new system. It also provides citizens with options to either pay by credit card or by have money directly withdrawn from their checking or savings account.

Figure 1-1
Web-based Motor Vehicle Registration Renewal System Home Page



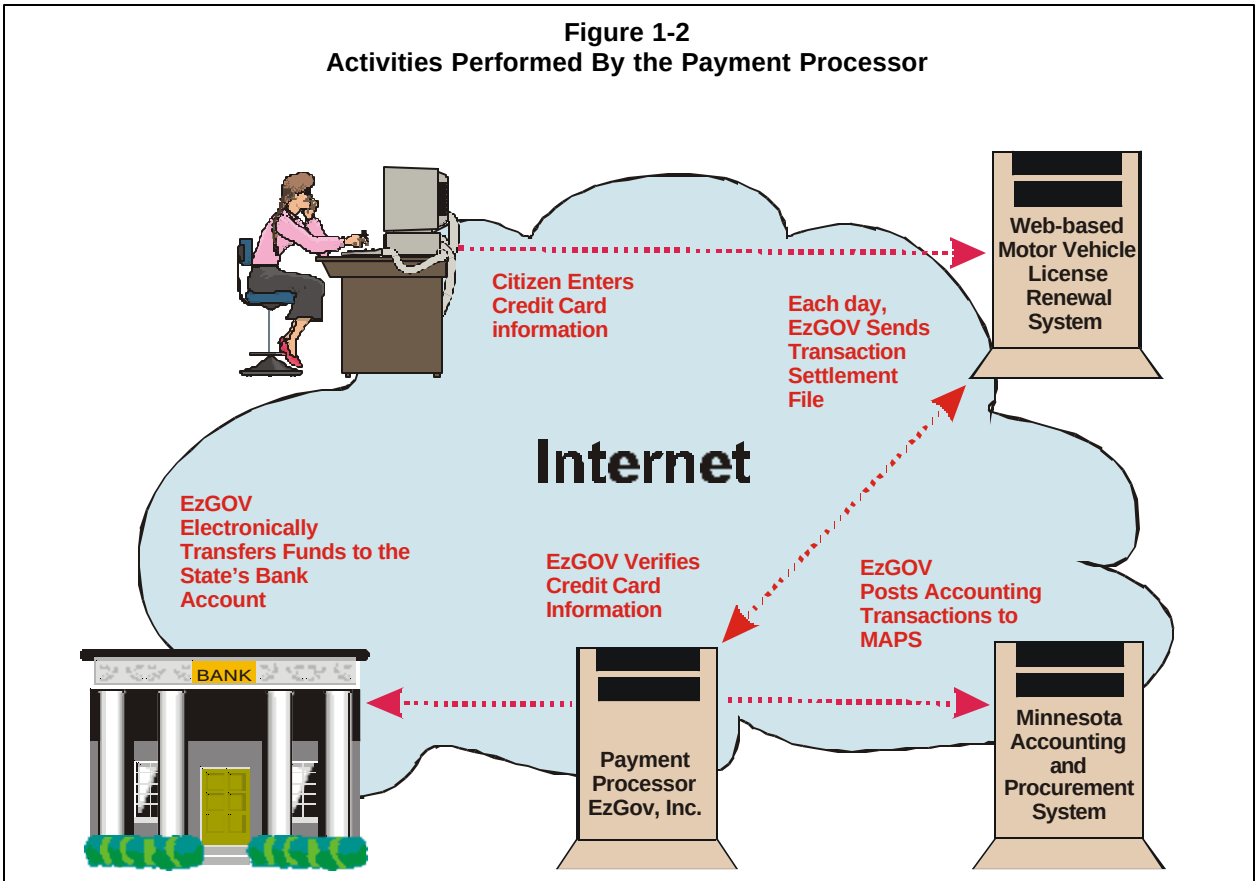
Source: Department of Public Safety's Web Site (May 2001).

Department of Public Safety
Web-based Motor Vehicle Registration Renewal System

Underneath the graphical interface seen by citizens is an extremely complex computerized business system. The Department of Public Safety used several different computers, commonly referred to as file servers, to deploy the Web-based Motor Vehicle Registration Renewal System. These file servers contain several databases with vehicle registration information and various computer programs that perform all of the system's functions. The department used state of the art web-based programming languages to design the computer programs.

The Web-based Motor Vehicle Registration Renewal System interacts with a payment processor, EzGov Incorporated, of Atlanta, Georgia. The payment processor confirms the validity of credit cards and interacts with the banking community on behalf of the department. Each day, EzGov transfers funds to the state's bank account and sends a transaction settlement file back to the department. EzGov also posts license renewal revenue transactions to the Minnesota Accounting and Procurement System. All of these payment processor activities take place over the Internet. Figure 1-2 illustrates the primary functions performed by EzGOV, Inc.

Figure 1-2
Activities Performed By the Payment Processor



Source: Auditor prepared.

The Department of Public Safety and other state agencies now place extensive reliance on computerized business systems to deliver services to citizens. These systems capture, process, and store information that is arguably the lifeblood of government. It is growing increasingly clear that this trend will not change. In fact, technological advances continue to provide state agencies with unprecedented opportunities to reduce costs and become more responsive. The

Department of Public Safety
Web-based Motor Vehicle Registration Renewal System

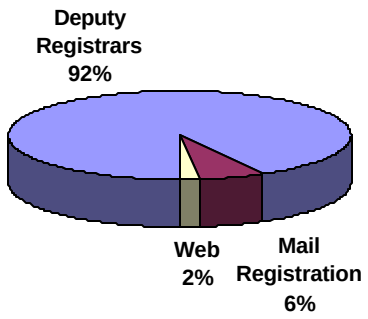
Web-based Motor Vehicle Registration Renewal System is an example of one such system, giving citizens an opportunity to order new license tabs from the convenience of their home.

Unfortunately, these same technological advances are spawning a new spectrum of vulnerabilities that state agencies must understand and manage. Agencies that fail to do so face potentially disastrous consequences, including:

- disruptions to mission-critical computer systems;
- unauthorized disclosures of confidential information; and
- unauthorized modifications to or the deletion of critical government data.

The threats to state agency computer systems and data are real, and they come from both internal and external sources. The fact that many systems like the Web-based Motor Vehicle Registration Renewal System communicate over the Internet compounds these threats. Once connected to the Internet, the constraints of time, distance, and speed are virtually nonexistent.

Figure 1-3
Registration Renewal Fees by Collection Method
October 2000 Through April 2001



Source: Minnesota Accounting and Procurement System Data.

The Department of Public Safety collected approximately $229 million in motor vehicle registration renewal fees between October 2000 and April 2001. However, as illustrated in Figure 1-3, only two percent of these fees were collected through the Web-based Motor Vehicle Registration Renewal System. The vast majority of citizens still renewed their motor vehicle registrations in person at Deputy Registrars, who maintain an inventory of vehicle tabs. Citizens who use the Web-based Motor Vehicle Registration Renewal System must wait for their tabs to arrive by mail. They also must pay an additional processing fee if they use a credit card to renew their license tabs. This processing fee is not assessed to citizens who elect to have money directly withdrawn from their checking or savings accounts.

Although the Web-based Motor Vehicle Registration Renewal System accounted for a low percentage of the total registration renewal revenue, it is significant because it is the first of many web-based computer systems that will most likely be deployed by state agencies in the upcoming years. As such, the findings and recommendations in this report can have an educational value that extends beyond the management of the Department of Public Safety. Chapter 2 discusses the specific scope and objectives of our work and the conclusions that we reached.

This page intentionally left blank.

Chapter 2. Data Integrity, Data Confidentiality, and System Availability Controls

Chapter Conclusions

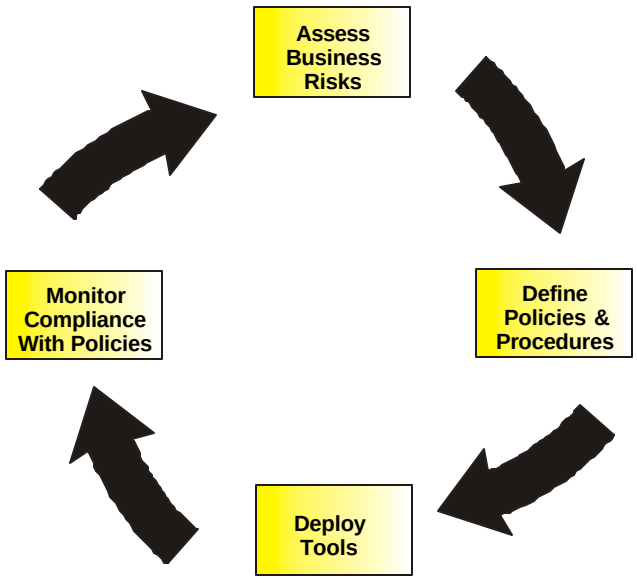
Security weaknesses expose the Web-based Motor Vehicle Registration Renewal System data to unnecessarily high risks and jeopardize the continued availability of the system. The department did not adequately plan or document the security infrastructure. Of greatest significance, the department did not prepare a formal risk assessment to identify potential security vulnerabilities, nor did it document appropriate policies, procedures, and standards to mitigate its risks.

Inadequate planning has resulted in a security infrastructure with many weaknesses. Many employees had complete access to sensitive computer programs and data, though they did not need such clearance. We also identified some sensitive system functions and data that could be accessed by unauthorized people from the Internet. Should inappropriate activities occur, the department may not detect them in a timely manner because it did not actively monitor the system or deploy intrusion detection software.

Following industry-standard system development principles could have averted many of these security weaknesses. The department adopted an extremely rapid development timeframe, even though its employees had little experience building web-based computer systems. The department then bypassed important system development activities to meet its self-imposed deadline. Little documentation now exists to support the system's computer programs, data structures, or security infrastructure. The department also allowed one employee to oversee most aspects of the system's development with little oversight or backup. After this employee resigned, the department struggled to understand and manage its new computer system.

Organizations conducting business over the Internet need robust security controls to ensure data integrity, data confidentiality, and system availability. Data integrity controls help protect the accuracy and completeness of data, both in storage and while in transit. Confidentiality controls help ensure that sensitive data, such as credit card numbers, cannot be seen by unauthorized individuals. Finally, system availability controls help minimize the amount of time when citizens cannot use the system to conduct business.

Figure 2-1
The Ongoing Security Management Lifecycle



Source: Auditor Prepared

Even with strong controls it is impossible to be completely secure, particularly when conducting business over the Internet. This fact makes designing and implementing a security infrastructure an ongoing exercise in risk management, much like buying insurance. As illustrated in Figure 2-1, organizations typically begin this process by performing a detailed risk analysis to identify potential vulnerabilities. The results of this analysis help organizations design policies and procedures to reduce their exposures to a level that executive management is willing to accept. Security professionals then deploy tools, such as access control software, to enforce the policies and procedures that were sanctioned by management. Information provided by these tools helps organizations monitor compliance with their policies and procedures and fine tune subsequent risk assessments in the ongoing security management lifecycle.

Audit Scope, Objectives, and Methodology

This information technology audit assessed the adequacy of controls in the Web-based Motor Vehicle Registration Renewal System. Specifically, we designed our work to answer the following questions:

- Did the department design and implement controls to protect the integrity and confidentiality of data?

- Did the department design and implement controls to ensure the continued availability of the system?

To answer these questions, we interviewed and obtained documentation from information technology professionals at the Department of Public Safety and the Minnesota Office of Technology. The Minnesota Office of Technology negotiated the contract with the payment processor, EzGOV Incorporated. We also used a variety of different computer-assisted auditing tools to analyze critical aspects of the security infrastructure. This analysis included a review of selected file servers, personal computers, database management systems, and the department's firewall. Finally, the Department of Administration's Electronic Government Services Support

Group provided us with assistance during this audit. The Electronic Government Services Support Group used a special software program to search for known security weaknesses in the Web-based Motor Vehicle Registration Renewal System's hardware and software.

Evaluation Criteria

We obtained our evaluation criteria from the Control Objectives for Information and Related Technology (COBIT), published by the Information Systems Audit and Control Foundation. The mission of COBIT is:

> *To research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.*

The COBIT Framework includes 34 high-level control objectives and 318 detailed control objectives, grouped in the following four domains:

Planning and Organization	This domain covers strategic planning and concerns the way that information technology can best contribute to the achievement of business objectives. It addresses the need to plan, communicate, and manage a strategic vision.
Acquisition and Implementation	This domain includes control objectives that pertain to acquiring, developing, and implementing information technology solutions. It also covers control objectives that pertain to changing existing systems.
Delivery and Support	This domain includes the process that must be in place to deliver information technology services on a daily basis. Some of these processes include ensuring systems security and managing data.
Monitoring	This domain addresses the need to regularly assess the quality of information technology processes. It addresses management's oversight of the control processes and independent assurance provided by internal and external audit.

We organized the findings and recommendations in this chapter by these four COBIT domains.

Planning and Organization

The department's technical and human resource planning activities were incomplete in several respects. As discussed in Finding 1, the department built and implemented the Web-based Motor Vehicle Registration Renewal System without performing a formal risk assessment. As discussed in Finding 2, the department also did not clearly define employees' roles and

responsibilities or allocate sufficient staff to perform critical system management functions. Finally, as discussed in Finding 3, the department did not define an acceptable level of downtime for the new system or plan for potential service disruptions.

1. The department did not plan an appropriate security infrastructure for the Web-based Motor Vehicle Registration Renewal System.

The security infrastructure for the new registration renewal system was a patchwork of automated tools that lacked a policy foundation. Although the department completed a high-level risk assessment for the entire agency, it did not prepare a detailed risk assessment for the new system or develop written security policies, procedures, and standards. Creating a written policy foundation is important because it provides security professionals with criteria to program access control tools. Written documentation also helps security professionals make consistent access control decisions that comply with the directives of management. Finally, it helps ensure the continued understanding and operation of critical security controls after key employees leave the organization.

As evidenced by Findings 5 through 10, the security infrastructure underlying the Web-based Motor Vehicle Registration Renewal System had weaknesses. The primary factors that led to these weaknesses were a deficient system development methodology and inadequate staffing. Findings 2 and 4 discuss these issues in more detail. Serious documentation shortcomings and the resignation of the employee who designed the system compounded these security weaknesses. It was evident that the remaining information technology professionals who managed the system did not understand many of its security controls or why they were originally created. These employees also did not know who had oversight responsibility for certain security controls. Written security policies, procedures, and standards could have alleviated these problems.

Recommendations

- *The department should adopt a formal process to identify and assess information technology risks.*

- *The department should use this risk assessment process as a foundation to develop appropriate security policies, procedures, and standards for its new system.*

2. The department did not allocate sufficient staff to the new system or clearly define their roles and responsibilities.

One employee oversaw most aspects of the system's development with little oversight or backup. This employee designed the system, wrote and quality tested the computer programs, performed database administration functions, and implemented most security features. Giving an individual

employee this level of authority was problematic because it created an environment where errors or irregularities could occur and go undetected. It also caused the department to become overly reliant on one information technology professional. Consequently, when the employee who oversaw most development functions resigned, the remaining employees struggled to understand and manage the new computer system.

The department also did not clearly define the day to day management responsibilities before implementing the new system. Two divisions jointly managed the new system: Driver and Vehicle Services and the Office of Technology Support Services. Employees in these divisions were unclear who was responsible for performing important system management functions. Of greatest significance, there was confusion about who was responsible for making security decisions and programming the tools that controlled access to the system's file servers and database management systems. They also were unsure who was responsible for installing the software patches that are provided by vendors to fix exploitable security weaknesses. The former employee who designed the system initially performed many of these duties.

Finally, as discussed in more detail in Finding 9, the department did not allocate staff to actively monitor security events. Management of the department told us that they did not have sufficient staff to perform these security duties each day.

Recommendations

- *The department should clearly define the job duties of all employees responsible for managing the new system and ensure that incompatible duties are properly separated.*

- *The department should allocate sufficient staff to monitor security events each day.*

3. The department did not define an acceptable level of downtime for the new system or plan for potential service disruptions.

The department did not perform fault tolerance planning when designing the Web-based Motor Vehicle Registration Renewal System. The first step in fault tolerance planning is to define how long a system can be unavailable without adversely impacting the organization or its customers. This management decision helps guide the selection of controls to avoid service disruptions that could exceed this limit. Extensive controls are necessary if management determines that a system cannot be down for more than one hour. However, if it is acceptable for a system to be unavailable for several weeks, fewer fault tolerance controls will be necessary. We found no evidence that the Department of Public Safety defined an acceptable period of downtime when designing its new system.

The new system had many potential single points of failure that could lead to extended service disruptions. For example, the department did not implement redundant computers to keep the

system running if one machine fails. Coping with these and other disruptions may prove challenging because the department did not develop written contingency plans for the system. The documentation and staffing deficiencies, discussed in Findings 1, 2, and 4, could further magnify the time it takes to recover from a disruption.

Recommendations

- *The department should define an acceptable downtime for its new system.*
- *The department should ensure that it has appropriate controls to avoid service disruptions that exceed its acceptable downtime.*

Acquisition and Implementation

The department adopted an overly aggressive development deadline for its new licensing system. To meet this self-imposed deadline, the department bypassed important system development activities. Finding 4 discusses our concerns in more detail.

4. The department did not follow industry-standard development principles when building the Web-based Motor Vehicle Registration Renewal System.

The department did not follow a comprehensive and repeatable methodology to design and implement the Web-based Motor Vehicle Registration Renewal System. Instead, the department followed an unstructured development path to implement the system as quickly as possible. Though the system became operational on October 18, 2000, many important system development activities still have not been finished. For example, the department did not develop comprehensive design specifications for the new system or adequately document its computer programs or data structures. The department also did not develop procedure manuals for the employees who must use the system to register vehicles. Finally, as discussed in Finding 1, the department did not plan and document an appropriate security infrastructure. Unless resolved, these shortcomings will increase future maintenance costs and could ultimately lead to security breaches.

The department has policies and procedures to control new system development and changes to existing systems. However, it did not follow these policies and procedures during the design and implementation of the Web-based Motor Vehicle Registration Renewal System. As discussed in Finding 2, a former employee designed, programmed, and quality tested most of the computer programs underlying the system. We found no evidence that these computer programs were subjected to independent quality testing. We also found no evidence that subsequent modifications to these programs followed the department's normal change management procedures. These independent quality assurance processes may have been bypassed because other information technology professionals did not understand the web-based programming languages that were used to develop the system. At the inception of every project, most system development methodologies require organizations to conduct a technical feasibility study. One

purpose of this study is to assess whether the staff possesses the appropriate technical skills to design, implement, and manage the system long-term. A technical feasibility study may have alerted the department early on that collectively its staff needed additional web-based programming skills.

Formal system development methodologies help organizations control complex computer projects by dividing them into manageable phases and defining deliverables for each phase. Management of the project team must approve the deliverables of each phase before work on a new phase can commence. This process helps ensure that all development efforts are properly documented, important activities are not overlooked, and that the project stays on schedule.

Recommendation

- *The department should follow a structured system development methodology for all significant computer projects.*

Delivery and Support

The department implemented various automated tools to limit access to the system and its data. For example, the department encrypts data before transferring it over the Internet to protect it from eavesdropping. The department also designed and implemented a firewall to protect the system from unscrupulous individuals on the Internet. However, weaknesses in other aspects of the security infrastructure exposed critical business data to unnecessary and unacceptable risks. As discussed in Findings 5 and 6, critical data and system resources were not properly secured. In Finding 7, we discuss security exposures that resulted from untimely and inconsistent system maintenance. Finally, Finding 8 discusses physical security weaknesses that came to our attention.

5. Critical business data and system components were not properly protected from unauthorized access.

As discussed in Finding 1, the department did not plan a comprehensive security infrastructure with policies, procedures, and standards. Without this criteria, it was difficult to determine who management intended to have access to sensitive business data and for what purpose. As discussed in Finding 2, it was also unclear who was responsible for programming the access control tools. Though the department implemented a series of tools to limit access to its system and data, the security infrastructure contained many weaknesses:

- An excessive number of people had extremely powerful security clearances. The department deployed the new registration system on computers that were already used for other purposes. Many employees who had existing clearances to these computers obtained inappropriate access to the registration system and its data by default.
- The former employee who developed the system still had active accounts that gave him complete and unfettered access.

- The department could not identify the owner or purpose of some accounts with extremely powerful security clearances.
- Password management controls were weak. Many people with powerful security clearances were not required to change their passwords and some had not for several years. Furthermore, the department did not limit the number of unsuccessful login attempts, leaving critical computers vulnerable to automated hacker exploits.
- Many powerful accounts that had been inactive for extended periods were not suspended or removed.
- Test versions of computer programs that were stored on some of the system's computers provided an unauthorized access point to anyone on the Internet.

The Department of Public Safety must eliminate these security weaknesses immediately to prevent unauthorized changes to or the disclosure of sensitive data.

Recommendations

- *The department should establish formal processes to grant, revoke, and periodically recertify security clearances.*

- *The department should remedy existing security weaknesses by:*
  -- *enforcing strong password controls;*
  -- *removing accounts that are no longer needed; and*
  -- *restricting peoples' access to only the data and computer resources that they need to fulfill their job duties.*

6. Transaction reports and credit card refunds were not properly secured.

Due to a security oversight, some transaction reports obtained from the payment processor could be accessed by anyone on the Internet. Although the reports did not contain credit card numbers, they disclosed citizens' names, addresses, and the amount that they paid to renew their license tabs. In some cases, Minnesota statutes prohibit the disclosure of this information without citizens' consent.

A second security oversight permitted anyone on the Internet to process credit card refund transactions. This security weakness increased the chance that citizens could obtain vehicle license tabs without paying the proper fees. It also could lead to inaccuracies in the department's motor vehicle records.

Recommendation

- *The department should fix the security weaknesses that permit unauthorized access to transaction reports and refund transactions.*

7. The department did not timely or consistently perform important system maintenance procedures.

We identified some software patches that were not installed on the computers underlying the new registration system. We also found patches that were installed on some computers, but not others. Confusion about job responsibilities, as discussed in Finding 2, may have led to these maintenance inconsistencies.

The Web-based Motor Vehicle Registration Renewal System uses many commercially available software packages. Unfortunately, computer hackers routinely discover and exploit flaws in commercial software to gain unauthorized access to organizations' computer systems. When these exploits occur, reputable vendors immediately develop and publish software patches to correct the deficiencies in their products. Organizations that do not promptly install these software patches make their systems easy targets for computer hackers.

Recommendation

- *The department should promptly install software security patches.*

8. Access to the data center housing the licensing system was not properly controlled.

The department did not have effective policies and procedures to restrict physical access to its data center. The department did not define who was responsible for authorizing data center access requests. Though the department has a security officer, this employee was not always involved in data center access decisions. The department also did not specify who was responsible for monitoring physical security clearances or how and when the monitoring should be done. It is important to restrict data center access to minimize the risk of damage or theft to critical computer equipment. Restricting data center access also helps protect confidential data from unauthorized disclosure.

The department did not detect several physical security weaknesses. The department was not aware that many cards with data center clearances were in the custody of a private company. This private company controlled the software that lets employees access the building and certain sensitive areas inside, such as the data center. The department also did not realize that an employee was granted data center access in error, and that a former employee and a former consultant's clearances were not revoked. The department could have detected these security weaknesses had it requested reports from the company that manages physical access to its facilities.

Recommendations

- *The department should define who is responsible for making physical access decisions and monitoring clearances.*
- *The department should periodically recertify physical security clearances and promptly change clearances as employees' job duties change.*

Monitoring

Monitoring of the Web-based Motor Vehicle Registration Renewal System is deficient in several respects. As discussed in Finding 9, the department does not actively monitor the system to identify security breaches. Finding 10 discusses financial activity reconciliation weaknesses that came to our attention.

9. The department did not have effective procedures or tools to detect and respond to potential security breaches.

The security infrastructure of the new licensing system lacked important controls to detect inappropriate activities, such as attacks by computer hackers. The best security controls are those that prevent inappropriate events from happening. Unfortunately, though, history has shown that it is virtually impossible to design flawless preventive defenses. It is a sad reality that unscrupulous individuals discover new security exploits daily and use that knowledge to penetrate organizations with many layers of preventive defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack. Since time is of the essence when under attack, every organization also must have decisive incident response procedures. Those that do not may fail to discover that they are completely unsecured until extensive damage has been done.

A minor security breach occurred during the course of our audit that provided a citizen with inappropriate access to a computer that is part of the new registration system. The citizen communicated the security weakness to both the department and a local television news station. Unfortunately, the employee who learned about this weakness did not promptly notify the security officer. As a result, the security officer was unable to begin his investigation until he learned about the security incident from a television reporter. Had this been a more serious breach, the department's untimely response could have been disastrous.

The department did not actively monitor security-related events for the Web-based Motor Vehicle Registration Renewal System. Some of the commercial software products underlying the system log activities to help organizations identify and respond to unusual events. Typically, organizations can customize these logs to meet their specific security needs. When questioned, the department told us that it did not have sufficient staff to monitor logs on a regular basis. The department also did not deploy any commercially available intrusion detection software packages. Intrusion detection software actively monitors logs and other system components. When unusual events occur, these software packages can immediately contact the appropriate individual to begin an investigation.

Finally, we had the Department of Administration's Electronic Government Services Support Group probe the registration system with a vulnerability scanner and found many exploitable security weaknesses. Vulnerability scanners are special software packages that probe systems to find exploitable security weaknesses. An example of one such weakness is a bug in a commercial software product that could force a computer program to perform an unauthorized

operation. Vendors that sell vulnerability scanners update their products frequently to include the most recent security exploits. Since hackers often take advantage of these exploits, it is important to find and correct them as quickly as possible. Had the department performed periodic vulnerability scans, it could have identified and corrected the security weaknesses that we found during our audit.

Recommendations

- *The department should develop and communicate security monitoring and incident response procedures to all employees.*
- *The department should obtain the staff and tools necessary to actively monitor the system for potential security breaches.*
- *The department should periodically scan its system to identify exploitable security weaknesses.*

10. The department did not verify the accuracy of all registration fee deposits.

The department did not develop procedures to ensure that all credit card registration fees were accurately deposited in the state treasury. The payment processor deposits registration fees in the state treasury and posts those deposits to the Minnesota Accounting and Procurement System. Controls over this process are weak because the department does not reconcile these deposits to the registration renewal transactions recorded in the Web-based Motor Vehicle Registration Renewal System. Without this reconciliation, deposit shortages could occur and go undetected.

Recommendation

- *The department should reconcile credit card deposits to the transactions recorded in the new system.*

This page intentionally left blank.

MINNESOTA DEPARTMENT OF PUBLIC SAFETY

Office of the Commissioner

445 Minnesota St., Suite 1000, North Central Life Tower, St. Paul, Minnesota 55101-5000
Phone: 612/296-6642 FAX: 612.297-5728 TTY: 612/282-6555
Internet: http://www.dps.state.mn.us

Alcohol & Gambling Enforcement

Bureau of Criminal Apprehension

Capitol Security

Driver & Vehicle Services

Emergency management / Emergency Response Commission

State Fire Marshal / Pipeline Safety

State Patrol

Traffic Safety

August 13, 2001

James R. Nobles
Legislative Auditor
1st Floor South
Centennial Building
St. Paul, MN 55155

Dear Mr. Nobles:

At the audit exit conference on August 2, 2001, we were provided a copy of the draft audit report of the Web-based Motor Vehicle License Renewal System. Our written response to the findings and recommendations are in the order presented in the draft report.

Brian Lamb, Director of Driver & Vehicle Services is responsible for the findings.

1. The department did not plan an appropriate security infrastructure for the Web-based Motor Vehicle License Renewal System.

Recommendations:

- *The department should adopt a formal process to identify and assess information technology risks.*
- *The department should use this risk assessment process as a foundation to develop appropriate security policies, procedures, and standards for its new system.*

Response:

DPS/DVS is working on putting a formal process in place to assure a secure environment for department applications. DPS participated, with the Office of Technology and a third party vendor, in the analysis of security risks for the implementation of several state initiatives involving financial transactions. The analysis did not point to any deterrents in proceeding with this application. In addition, the Legislature did set financial benchmarks (16E.04sub3) for determining when an in-depth risk analysis was needed for a project. This Internet registration renewal application did not meet the financial investment to require an in-depth risk analysis.

During the development and before implementation, there was planning for the physical/network security infrastructure for the application.

- The application was installed within the physical and network security infrastructure maintained both by Intertech and the department for the Town Square location.
- The database and application servers were placed behind a firewall.

- The communications between the web server and the application and database servers was on a randomly selected port, other than the one set by default.
- The application used secure socket layer encryption (SSL) for transactions across network wires.

During the vulnerability study by Intertech, referenced in the audit report and responded to in #9 below, there were no significant concerns reported for intrusion outside the firewall. However, DPS/DVS technology staff, new after the project was live, has identified (along with the audit team) concerns about system security and have taken appropriate actions to correct. In addition, the department is identifying training opportunities for staff on security best practices.

2. The department did not allocate sufficient staff to the new system or clearly define their roles and responsibilities.

Recommendations:

- *The department should clearly define the job duties of all employees responsible for managing the new system and ensure that incompatible duties are properly separated.*
- *The department should allocate sufficient staff to monitor security events each day.*

Response:

Since the audit DPS has hired programmers with web development skills, defined the roles of system and applications management, and increased cross training so that backups are available for all critical roles.

3. The department did not define an acceptable level of downtime for the new system or plan for potential service disruptions.

Recommendations:

- *The department should define an acceptable downtime for its new system.*
- *The department should ensure that it has appropriate controls to avoid service disruptions that exceed its acceptable downtime.*

Response:

Since the implementation of the system ten months ago, the system has been operational for over 99.9% of that time. Scheduled and multiple backups enable DPS/DVS to respond in a timely manner to any corruption of hardware, software, or data and to recover the system in less than 4 hours.

In addition, when the service has not been available, we have communicated this on the website so those citizens were aware of the downtime. In the event of the electronic system not being available, citizens can renew via mail or at the Central Office in St Paul or at any of 172 deputy registrar offices.

During the timeframe of the audit, DPS/DVS has increased physical and personnel resources to maintain this Internet renewal application as a production system, within the parameters over which the department has control.

4. The department did not follow industry-standard development principles when building the Web-based Motor Vehicle License Renewal System.

Recommendations:

· *The department should follow a structured system development methodology for all significant computer projects.*

Response:

DPS/DVS agrees that the development of this software did not follow a structured methodology. The department has brought in staff with technical skills and they were able to take over the management and continued development of the system; however their work was made more difficult because the system lacked any documentation for design, business logic, procedures, source code, and hardware.

DPS/DVS staff has implemented methodologies in new developments for change control management of servers, systems, databases, data, and procedures for documentation and storage of software source. In addition the department's staff will use appropriate parts of the department's system methodology tool in developing future web applications.

5. Critical business data and system components were not properly protected from unauthorized access.

Recommendations:

· *The department should establish formal processes to grant, revoke and periodically recertify security clearances.*
· *The department should remedy existing security weaknesses by:*
  - *enforcing strong password controls;*
  - *removing accounts that are no longer needed; and*
  - *restricting peoples' access to only the data and computer resources that they need to fulfill their job duties.*

Response:

DPS/DVS has corrected all the recommended system security accesses identified above by the audit team and others that new management has identified in the application. With new methodologies in place, we can continue the security process that enables access correlated with functional responsibilities.

6. Transaction reports and credit card refunds were not properly secured.

Recommendations:

• *The department should fix the security weaknesses that permit unauthorized access to transaction reports and refund transactions.*

Response:

The web page that permitted access to transaction reports required an individual to guess a valid 16-digit confirmation number. Even though this presents a minimal security risk, the department has secured the web page and it is available only for the cashier staff.

The web pages that permitted access to refund transactions were also secured. During the ten months of operation, there have been no unauthorized refunds except during the testing period.

7. The department did not timely or consistently perform important system maintenance procedures.

Recommendations:

• *The department should promptly install software security patches.*

Response:

DPS/DVS agrees on the importance of timely security patches and has applied to all of their web and application/database servers. DPS is a member of MNCert as its primary source of security vulnerability and patch information. In addition, staff have now been identified and tasked with belonging to security list servers in order to proactively obtain timely information on security risks, preventive measures, and patch availability.

8. Access to the data center housing the licensing system was not properly controlled.

Recommendations:

• *The department should define who is responsible for making physical access decisions and monitoring clearances.*
· *The department should periodically recertify physical security clearances and promptly change clearances as employees' job duties change.*

Response:

The department has defined and implemented staff responsibilities for physical security. DPS/DVS has started the process of defining administrative controls for a variety of security activities, including clearances for new, changing, and departing employees.

9. The department did not have effective procedures or tools to detect and respond to potential security breaches.

Recommendations:

• *The department should develop and communicate security monitoring and incident response procedures to all employees.*
· *The department should obtain the staff and tools necessary to actively monitor the system for potential security breaches.*
· *The department should periodically scan its system to identify exploitable security weaknesses.*

Response:

The results of the audit, combined with the vulnerability report by Intertech, support the statement in security journals that the greatest security risks are internal, rather than external.

The department also agrees with this concept and therefore realizes that user awareness must be a critical part of our security plan. We will start the process of defining and implementing an appropriate and workable procedure to increase the involvement of all employees in security monitoring. DPS is in the process of creating a CERT Team for security incident planning and response.

The department has now purchased hardware and software tools for security monitoring and, in addition, has increased the number of staff responsible for security. Ongoing training for staff is a commitment of the department.

We have already begun the discussion and planning for periodic reviews of security. The department will partner with both third party vendors and Intertech, to utilize the expertise of security analysts for periodic review.

10. The department did not verify the accuracy of all license fee deposits.

Recommendations:

• *The department should reconcile credit card license fee deposits to the transactions recorded in the licensing system.*

Response:

DVS started the design of the reconciliation program during the audit and the application has been installed and is operational.

If you have any questions or concerns, feel free to contact me.

Sincerely,

/s/ Charles R. Weaver

Charles R. Weaver, Jr.
Commissioner, Department of Public Safety

Cc: Sara Schlauderaff
Frank Ahrens
Brian Lamb