OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Department of Public Safety

Security Audit: Web-based Motor Vehicle Registration Renewal System

APRIL 19, 2005 **05-23**

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 forty 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.

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 651-296-1235 (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, or evaluation, 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. Michael Campion, Commissioner
Department of Public Safety

We have conducted an information technology audit of the Web-based Motor Vehicle Registration Renewal System. The scope of our audit focused on security controls used to protect the integrity and confidentiality of data collected, processed, or stored by the system. The Report Summary highlights our overall conclusion. Our specific audit objective and conclusions are contained in Chapter 2 of this report.

This is our second audit of the Web-based Motor Vehicle Registration Renewal System. Our first audit, released in August 2001, contained 10 findings and 17 recommendations that addressed a broad array of security weaknesses. Unfortunately, many findings in our last report were not addressed. We also found additional serious security weaknesses during this audit. Collectively, these weaknesses exposed the system and citizens' private data to an unacceptable risk of tampering, disruption, and misuse. As such, we are recommending that the department shut down the Web-based Motor Vehicle Registration Renewal System until an appropriate security infrastructure has been defined, tested, and installed.

We would like to thank staff from the Department of Public Safety for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: March 10, 2005

Report Signed On: April 15, 2005

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
Security Audit

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Chris Buse, CPA, CISA, CISSP	Information Technology Audit Manager
Eric Wion, CPA, CISA	Auditor-in-Charge
Mark Mathison, CPA, CISA	Auditor
Neal Dawson, CPA, CISA	Auditor
John Kelcher	Auditor

Exit Conference

We discussed the findings and recommendations in this report with the following staff of the Department of Public Safety on April 6, 2005:

Michael Campion	Commissioner
Mary Ellison	Deputy Commissioner
Janet Cain	Chief Information Officer
Patricia McCormack	Director of Driver and Vehicle Services

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

Report Summary

Key Conclusion:

Serious security weaknesses have exposed the Web-based Motor Vehicle Registration Renewal System and citizens' private data to an unacceptable risk of tampering, disruption, and misuse. Until significant security enhancements are made, the system should not be used to conduct business.

Findings:

- The department did not implement an effective security program. (Finding 1, page 8)
- Computer programs developed by the Driver and Vehicle Services Division contained security flaws. (Finding 2, page 10)
- Poorly configured wireless access devices provided a way to bypass the department's firewall. (Finding 3, page 11)
- Sensitive customer data and critical system components were not properly protected. (Finding 4, page 12)
- The department did not promptly perform important system maintenance procedures. (Finding 5, page 13)
- The department did not adequately monitor its systems. (Finding 6, page 14)

Audit Scope:

Audit Period:
We assessed security controls as of March 2005

Selected Audit Areas:
The Web-based Motor Vehicle Registration Renewal System

Background:

The Department of Public Safety developed and implemented the Web-based Motor Vehicle Registration Renewal System in 2000. The system gives citizens the ability to renew their motor vehicle license tabs and plates over the Internet. Using a standard web browser, such as Microsoft's Internet Explorer, citizens can pay their registration renewal taxes from the convenience of their home. Revenue from the web-based system increased from $6.6 million in fiscal year 2001 to $30.5 million in fiscal year 2004.

This page intentionally left blank.

Chapter 1. Introduction

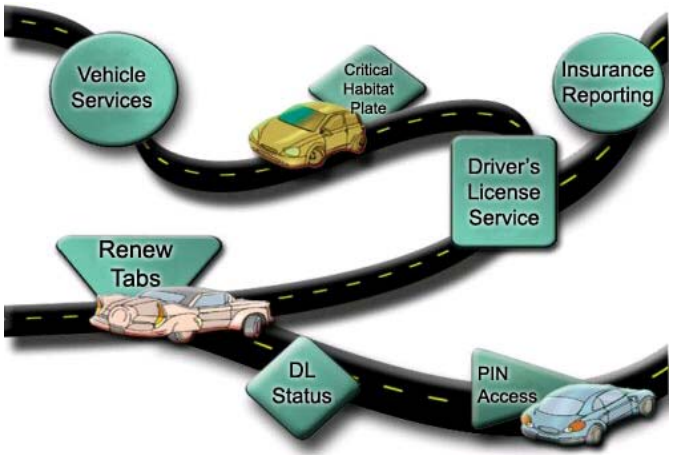
This information technology audit assessed the adequacy of security controls in the Web-based Motor Vehicle Registration Renewal System. The system gives citizens the ability to renew their motor vehicle license tabs and order plates over the Internet. Using a standard web browser, such as Microsoft's Internet Explorer, citizens can pay their registration renewal taxes and fees from the convenience of their home.

This is our second audit of the Web-based Motor Vehicle Registration Renewal System. Our first audit, released in August 2001, contained 10 findings and 17 recommendations that addressed a broad array of security weaknesses. These findings highlighted deficiencies in the:

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

Our prior audit concluded that security weaknesses left the system and its data vulnerable to tampering, disruption, and misuse from both internal and external sources. We structured this audit to follow-up on some of the most significant findings in our last report.

Figure 1-1
Driver and Vehicle Services Home Page



Source: Department of Public Safety Web Site.

Citizens access the Web-based Motor Vehicle Registration Renewal 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 system. Figure 1-1 depicts the Driver and Vehicle Services Home Page. From this page, citizens can renew vehicle tabs, order plates, and update driver's license and vehicle insurance information.

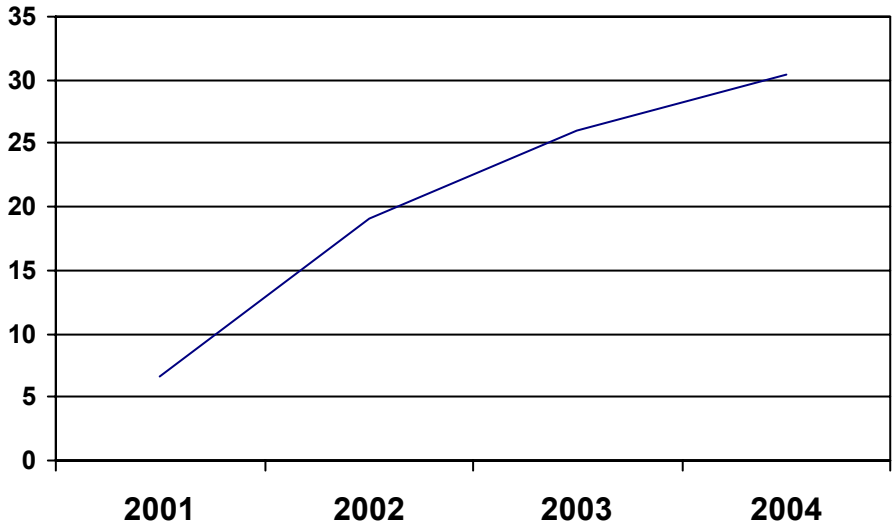
Underneath the screens seen by citizens are extremely complex computerized business systems. The Department of Public Safety uses several different computers to deploy the Web-based

Motor Vehicle Registration Renewal System. These computers house the programs that perform all of the system's functions and several large databases containing vehicle registration data.

Citizens can pay registration renewal fees with a credit card or have funds directly withdrawn from their bank account. With assistance from a financial institution, the department processes transactions that withdraw funds from citizens' bank accounts. For credit card transactions, 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 tax revenue transactions to the State of Minnesota's accounting system.

As illustrated in Figure 1-2, Web-based Motor Vehicle Registration Renewal System revenue increased from $6.6 million in fiscal year 2001 to $30.5 million in fiscal year 2004. However, most citizens still renew their motor vehicle registrations by mail or in person at Deputy Registrar offices. 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.

Figure 1-2
Web-based Motor Vehicle Registration Renewal System Revenue
Fiscal Years 2001 through 2004
(In Millions)



Source: Minnesota Accounting and Procurement System.

Audit Approach

We conducted this audit in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. These standards require that we obtain an understanding of internal controls relevant to the audit objectives.

For information technology audits, we obtain evaluation criteria from the Control Objectives for Information and Related Technology (COBIT). Published by the IT Governance Institute, COBIT includes 34 high-level control objectives and 318 detailed control objectives, grouped in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. We also obtain technology-specific evaluation criteria from other sources. On this audit, we used the Ten Most Critical Web Application Security Vulnerabilities Report, distributed by the Open Web Application Security Project. Web application vulnerabilities on this list require immediate remediation because they are actively targeted by attackers. To evaluate controls over specific computer operating and database management systems, we relied on information published by the developers of those products. Finally, we used publications distributed by recognized security experts, such as the National Institute of Standards and Technology.

Information technology audits frequently include the review of sensitive security data that is legally classified as nonpublic under the Minnesota Data Practices Act. In some cases, to protect state resources and comply with the Minnesota Data Practices Act, we must withhold security-related details from our publicly released reports. When these situations occur, we communicate all pertinent details to agency leaders in a separate, confidential document. For this audit, we issued a separate, confidential document to the management of the department.

This page intentionally left blank.

Chapter 2. Security Controls

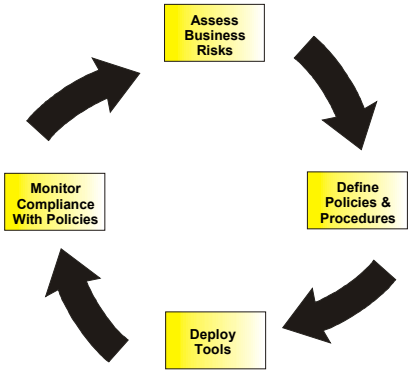
Chapter Conclusions

Without significant security enhancements, the Web-based Motor Vehicle Registration Renewal System should not be used to conduct business. Serious security weaknesses identified in our August 2001 audit of the system have not been properly addressed. We also found additional serious weaknesses during this audit. Collectively, these weaknesses exposed the system and citizens' private data to an unacceptable risk of tampering, disruption, and misuse.

Conducting business over the Internet with web-based systems poses unique risks. Most organizations have firewalls to protect sensitive internal computer networks and data from unscrupulous people on the Internet. However, by design, traffic going to web-based systems often flows freely through firewalls. Recognizing this inherent architecture weakness, hackers have developed many ways to exploit design flaws in web-based systems to gain unauthorized access to internal computer networks and data.

Organizations with web-based systems must deploy robust security controls to ensure data integrity, 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
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 Objective

We designed our audit work to answer the following question:

- Did the department design and implement controls to protect the integrity and confidentiality of data collected, processed, and stored by the Web-based Motor Vehicle Registration Renewal System?

To address this objective, we interviewed information technology and business professionals who oversee the system and its controls and used computer-assisted audit tools to test selected controls.

Current Findings and Recommendations

1. PRIOR FINDING NOT RESOLVED. The department did not implement an effective security program.

The findings in this report are the byproducts of an ineffective security program. They identify serious weaknesses in the Web-based Motor Vehicle Registration Renewal System, managed by the Driver and Vehicle Services Division (DVS). However, the findings have implications that go beyond just one system or even one division in the Department of Public Safety. Specifically, we found that

- Appropriate security controls have not been installed to mitigate risks found in today's web-based computing environments;
- Security controls that were deployed were often ad hoc and undocumented; and
- The effectiveness of security controls was rarely monitored.

The department has a security policy that defines the broad expectations of management. However, management did not devote enough resources to carry out the detailed provisions in this policy. Though the department delegates critical security duties to each division, the chief information officer (CIO) and an information security unit retain the overall responsibility and authority for the protection of information assets. As outlined in Table 2-1, this responsibility includes setting standards for divisions to follow and monitoring compliance with those standards. Resource restrictions prevented the CIO and information security unit from performing these and other critical security duties. The CIO has many duties besides security. After budget cuts, the information security unit was left with only one employee, who quit in August 2004 and was not replaced. The department assigned some duties to a supervisor, who provided only minimal support due to his other workload constraints. The resulting culture is one that allows divisions to operate autonomously, without department-wide standards or appropriate internal controls.

Table 2-1
Significant Security Responsibilities Outlined in Policy

Chief Information Officer	Information Security Unit
• Overall responsibility and authority for the protection of information assets. • Review and approve division policies to ensure consistency with department policy. • Approve exceptions to the security policy.	• Serve as internal and external point of contact on all security matters. • Set and manage department wide security strategies. • Monitor compliance with security policies, conduct annual information security audits, and oversee external audits. • Develop and coordinate security awareness training and incident handling and change control process. • Maintain all security documentation in a secure location. • Approve wireless network connections and contractor access requests.

Source: Department of Public Safety's Information Resources Security and Acceptable Use Policy.

Security practices in DVS were extremely lax. The division did not take appropriate action to remedy significant security issues cited in our August 2001 report. The division also failed to comply with and ensure that employees understood important provisions in the department's security policy. Several times during our audit, we were able to exploit security weaknesses that could have allowed us to take control of the system, had we chosen to do so. If allowed to continue, poor security practices in DVS could lead to the inappropriate disclosure of citizens' private data and undermine public confidence in the department.

The Web-based Motor Vehicle Registration Renewal System's computer programs and security infrastructure are poorly documented. Because a strong security program is essential, organizations should carefully plan and document all security decisions before deploying a computer system. This painstakingly detailed effort provides information technology professionals with the data needed to properly configure access control software and other security tools. It also provides them with a documented basis to either allow or disallow future access requests made by employees. Though recommended in our last audit, DVS still has not defined the security architecture for the Web-based Motor Vehicle Registration Renewal System. We examined the security tools that control access to the system and found people and software products that had more clearance than necessary. Without documentation, DVS had difficulty and often could not explain why many of these security clearances were needed. This difficulty was compounded by the fact that several of the clearances appeared to have been created by employees who no longer worked for the division.

DVS did very little monitoring of the hardware and software that it controls. As a result, intrusion attempts by hackers or unauthorized system use by employees could occur and go undetected. The division has not defined what it considers to be significant security-related events or configured its security tools to log those events. By default, most security tools log

certain events, such as failed access attempts. However, employees in DVS did not regularly review those logs. The division has not deployed any commercial intrusion detection software and does not periodically scan its computers with software that is used by most organizations to identify commonly exploited security vulnerabilities. Had it done so, DVS would have found many of the serious security weaknesses identified by our audit.

Findings 2 through 6 contain additional details about the security concerns identified by our audit. After considering all of the findings in this report, we conclude that the Web-based Motor Vehicle Registration Renewal System should not be used to conduct business. To improve controls, Department of Public Safety management needs to begin by making a long-term commitment to information security. This commitment must be communicated to all divisions through a comprehensive security program that includes policies, procedures, standards, security awareness training, and forms of oversight to validate the ongoing effectiveness of controls.

Recommendations

- *The department should develop a comprehensive security program to effectively manage security risks throughout the organization.*

- *The department should shut down the Web-based Motor Vehicle Registration Renewal System until an appropriate security infrastructure has been defined, tested, and installed.*

2. PRIOR FINDING NOT RESOLVED. Computer programs developed by DVS contained security flaws.

The computer programs used by citizens to interact with the Web-based Motor Vehicle Registration Renewal System contained significant security weaknesses. Our audit team was able to exploit these weaknesses using popular hacker techniques. Had we chosen to do so, we could have taken control of the Web-based Motor Vehicle Registration Renewal System and other systems in the department. Hackers could have exploited these same weaknesses to steal private data, install their own malicious programs on DVS computers, or perform other destructive acts. After being alerted to these weaknesses, the division shut down the Web-based Motor Vehicle Registration Renewal System for a weekend to make emergency security fixes.

In our last audit, we reported that the department lacked a comprehensive and repeatable system development methodology for its web-based computer systems. That is still the case today. The system development standards followed by DVS are not documented. Therefore, we found it difficult to determine precisely what the standards were and if people actually followed them. We also could not tell if DVS subjected its computer programs to rigorous testing. We found examples of computer programs with unnecessary security clearances. We also found programs that were vulnerable to common hacker exploits or had poorly designed security features, such as edits, that could be circumvented. These examples lead us to conclude that the informal testing methodology was either inadequate or not followed.

We found an overall lack of documentation for computer programs written by DVS, which could increase future maintenance costs. At the conclusion of our audit, DVS told us that it is in the process of hiring a consultant to rewrite the Web-based Motor Vehicle Registration Renewal System. Sparse documentation for the existing system is a key reason why such a costly solution may be necessary.

To improve controls, the department needs to adopt and follow formal system development standards for its web-based computer systems. These standards should address security throughout the development process and provide for independent testing. The department also should thoroughly test its other web-based computer systems to determine if they are susceptible to the same security weaknesses that we found in the Web-based Motor Vehicle Registration Renewal System. We performed a cursory review of several other systems and found evidence that they also may be vulnerable.

Recommendation

- *The department should adopt formal system development standards and thoroughly test all of its web-based computer systems to ensure that they are secured.*

3. Poorly configured wireless access devices provided a way to bypass the department's firewall.

The department connected two unsecured wireless access points to its internal network. Our audit team used these improperly configured devices to circumvent the department's firewall and gain access to its private internal network. The department disconnected the two devices after we told employees about the security risks.

Organizations deploying wireless technologies must adopt very stringent security standards. Hackers routinely target wireless devices because they are often the least secure point of entry into an organization's private network. Wireless technologies are also attractive targets because they can be exploited without physical access to a building. In its security policy, the department states that the information security unit must approve all wireless security devices. However, the department did not develop or publish any configuration standards. The two devices that we compromised had no security in place and could be accessed by anyone in or outside the building with a laptop computer.

To prevent future security breaches, the department should develop detailed standards for configuring wireless devices. These standards should ensure that wireless connections can only be made by specific people who have been properly authenticated. They also should ensure that wireless communications are encrypted with a robust algorithm that cannot be deciphered by hackers. And finally, the standards should require periodic scans of the building to detect unauthorized wireless access points.

Recommendations

- *The department should develop security standards for wireless technologies.*

- *The department should periodically scan its environment to search for unauthorized wireless access points.*

4. PRIOR FINDING NOT RESOLVED. Sensitive customer data and critical system components were not properly protected.

During our audit, we identified people with security clearances that exceeded what was necessary to fulfill their job duties. We also found some accounts used by software products that had been assigned unnecessary clearances. The department's security policy requires each division to develop access control standards for its systems. Since DVS did not comply with this directive for the Web-based Motor Vehicle Registration Renewal System, we could not determine if management had sanctioned these or other powerful security clearances.

Controls over accounts with access to sensitive databases were particularly weak and rarely complied with the department's security policy. For example, all accounts with access to the database could run sensitive computer programs, even though few needed such access. We also found that information technology professionals with powerful security clearances often shared accounts and passwords. This practice, forbidden by the department's security policy, makes it extremely difficult to trace actions back to individuals. And finally, we found many powerful database accounts with either blank passwords or simple passwords that were easy to guess. We communicated these and many other access control deficiencies to the department in a separate, confidential document.

The department did not adequately secure transaction reports and credit card refunds. Though only needed by employees, the web pages used to initiate transaction reports and credit card refunds were accessible to anyone on the Internet. Furthermore, the account and password used to secure these web pages were not protected from unauthorized disclosure. From the Internet, we were able to obtain the account and password with minimal effort.

Information security relies on certain principles including: 1) positively confirming the identity of system users, 2) always having a mechanism to trace critical events back to specific individuals, and 3) limiting system access to the minimum necessary for employees to fulfill their job duties. By not choosing to vigorously enforce these principles, DVS exposed the Web-based Motor Vehicle Registration Renewal System and its data to unnecessary risks.

Recommendations

- *The department should document access control standards for the Web-based Motor Vehicle Registration Renewal System.*

- *The department should limit accounts assigned to people and software products to the minimum security clearance that is necessary.*

- *The department should enforce its policy that forbids employees from sharing accounts and passwords.*

- *The department should enforce its policy that requires employees to select complex passwords that are difficult to guess.*

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

5. PRIOR FINDING NOT RESOLVED. The department did not promptly perform important system maintenance procedures.

Some security-related software patches were not installed promptly on Web-based Motor Vehicle Registration Renewal System computers. The department uses many commercial software packages, including computer operating and database management systems. Unfortunately, computer hackers routinely discover and exploit flaws in commercial software to gain unauthorized computer system access. When these exploits occur, reputable vendors immediately develop and publish software patches to correct the product deficiencies. Organizations that do not promptly install these software patches make their systems easy targets for computer hackers.

Identifying and patching computers can be an extremely daunting task, particularly in environments with many computers, like the Department of Public Safety. To improve controls, the department needs to better define, document, and enforce patch management standards and procedures. The department should also consider automated solutions to streamline patch management tasks. Currently, information technology professionals install software patches manually on each computer.

Recommendation

- *The department should implement procedures to promptly install security-related patches.*

6. PRIOR FINDING NOT RESOLVED: The department did not adequately monitor its systems.

The department did not have controls to detect and promptly respond to security-related events, such as unauthorized access attempts made by hackers. The best security controls are those that prevent inappropriate events from happening. Unfortunately, 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 defined incident response procedures. Organizations that do not have effective procedures may fail to discover that they are completely unsecured until extensive damage has been done.

Many commercial software products used by the department can be customized to log various types of security events. Many can even send alerts to specific individuals when events occur. In most cases, the department did not define specific events to log. Furthermore, the logs that were generated by some products were of little value because they were rarely reviewed. Though time consuming, the department must now go back and define specific security-related events to log for the Web-based Motor Vehicle Registration Renewal System. An excellent time to do this will be when the department develops access control standards, as discussed in Finding 4. For example, management may decide that no employee is allowed to view bank routing numbers supplied by citizens. By logging and investigating all instances when bank routing numbers are viewed, management could help ensure compliance with its standard.

Finally, the department did not run vulnerability assessment software to search for commonly known 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 several of the security weaknesses that we found during our audit.

Recommendations

- *The department should define specific security events to log and regularly review those logs to identify potential security breaches or system misuse by employees.*
- *The department should periodically scan its computers to search for security weaknesses that are commonly exploited by hackers.*

Status of Prior Audit Issues
As of March 4, 2005

Most Recent Audit

Legislative Audit Report 01-43 assessed the adequacy of controls that protect the integrity and confidentiality of data and ensure the continued availability of the system. The 10 findings and 17 recommendations in the report addressed a broad array of security weaknesses. The findings highlighted deficiencies in the organization and planning of the system, system development methodology, day to day security and support activities, and monitoring.

We designed our current approach to follow-up on seven of the ten findings in our last report. None of these seven prior audit findings had been adequately resolved. During this audit, we did not perform procedures to follow-up on Findings 3, 8, and 10 that appeared in our prior report.

State of Minnesota Audit Follow-Up Process

The Department of Finance, on behalf of the Governor, maintains a quarterly process for following up on issues cited in financial audit reports issued by the Legislative Auditor. The process consists of an exchange of written correspondence that documents the status of audit findings. The follow-up process continues until Finance is satisfied that the issues have been resolved. It covers entities headed by gubernatorial appointees, including most state agencies, boards, commissions, and Minnesota state colleges and universities. It is not applied to audits of the University of Minnesota, any quasi-state organizations, such as metropolitan agencies or the State Agricultural Society, the state constitutional officers, or the judicial branch.

This page intentionally left blank.

MINNESOTA DEPARTMENT OF PUBLIC SAFETY

Office of the Commissioner

445 Minnesota Street • Suite 1000 • Saint Paul, Minnesota 55101-5100
Phone: 651.296.6642 • Fax: 651.297.5728 • TTY: 651.282.6555
www.dps.state.mn.us

Alcohol and Gambling Enforcement

ARMER/911 Program

Bureau of Criminal Apprehension

Driver and Vehicle Services

Homeland Security and Emergency Management

Minnesota State Patrol

Office of Communications

Office of Justice Programs

Office of Traffic Safety

State Fire Marshal and Pipeline Safety

Mr. James R. Nobles
Legislative Auditor
1st Floor South
Centennial Building
St. Paul, MN 55115

April 14, 2005

Dear Mr. Nobles,

While the Department of Public Safety is committed to addressing the security issues that have been raised in the Web-based Vehicle Registration Renewal audit and intends to act on all the recommendations included in the report, it is important to note that, within the scope of this audit, no evidence was found to indicate that any of the systems that were examined had been compromised. This does not mean that the Department has not acted quickly in response to the issues raised in the audit. The Department has already taken many steps toward correcting identified security problems. The Department is also working closely with the Department of Administration's InterTechnologies Group to provide and obtain services to address immediate needs raised in this audit. However, as you know, the recommendations to strengthen security programs, create, implement, monitor and enforce detailed security standards are a long term and continuous endeavor. At this time, the Department cannot provide specific dates for completing those recommendations because of outstanding questions related to the time required to bring on the highly skilled and specialized staff that is essential to adequately implement the majority of the recommendations in the audit report. The Department will provide the Auditor with a progress report on July 1, 2005 including the assignment of responsibilities and projected completion dates that are known at that time.

It is our intent to continue to work with the Office of the Legislative Auditor over the long term to improve and strengthen security services at the Department of Public Safety. Please contact me if you have any questions regarding our response to the Web-based Vehicle Registration Renewal Audit.

Sincerely,

/s/ Michael Campion

Michael Campion
Commissioner, Department of Public Safety

General Response:
Within the scope of this audit, no evidence was found to indicate that any of the systems that were examined had been compromised.

Finding Number 1:Prior Finding not Resolved: The Department did not implement an effective security program

Recommendation 1: The department should develop a comprehensive security program to effectively manage security risks throughout the organization
The Department will strengthen its department-wide information systems security program.

The Department of Public Safety took steps to implement an effective security program within the constraints of the resources available to implement the department-wide program. Finding people with the skills to do the necessary work was difficult since people with this skill set are very much in demand in all public and private sector organizations but the Department did establish a two person department-wide security unit with an Information Security Officer and a Security Technical Specialist. The Department also has some staff in divisions that perform security functions at the division level.

A strong security policy was developed and user security awareness training was initiated. Both security staff left the unit for jobs with higher compensation. To conserve funds for other priorities, some of the information Security Officer's basic responsibilities were assigned to a supervisor with security certification to take on as additional duties. This put many of the policy implementation, standards development and user awareness functions on hold. Consequently, what started as a lean but serious security effort was reduced. The proactive aspect of the security program was severely curtailed while maintenance of the fundamental security technology such as firewalls and virtual private networks was retained.

Security for information systems is a continuous process. It is often a "painstakingly detailed effort" as noted by the Legislative Auditor. Designing, developing and implementing an information systems security program is an extremely labor intensive process that requires a high level of planning, analytical, technical, and coordination skills and activities. The Department of Public Safety has a federated information systems environment to meet the delivery needs of its diverse programs. This computing environment must rely heavily on the involvement of many individuals and levels of staff to communicate and collaborate to reach a uniform approach to information systems planning and operations at the Department of Public Safety. This takes a significant amount of time and has not always been effective. To address this problem, in 2004, the Commissioner convened a department-wide Information Resource Management Workgroup to recommend an approach to managing information systems within the DPS organization. The Workgroup examined the governance structures of several state departments and, in December, made its recommendation to the Commissioner. The Commissioner approved the recommendations and a new Information Technology Governance Group and information systems management process was created. The new Governance Group began its work in January 2005. This group is composed of the DPS Deputy Commissioner, the DPS CIO and all DPS Division Directors. A committee of technical staff and selected business staff has been created to advise the DPS Governance Group on all aspects of information systems planning and operations so that the Governance Group can make sound, department–wide decisions related to information systems including security policies, standards and procedures. Instituting and maintaining a new, more structured approach to planning, implementing and sustaining DPS information systems is a long term effort.

The findings of the Legislative Auditor have moved systems security to the top of the agenda for the DPS IT Governance Group to address. They have already met to take action on short term requirements for resolving security deficiencies and will have a large role in setting a unified and strengthened direction for the information systems security program at DPS.

The DPS IT Governance Group has already approved a staffing level to include;

- Allocating funding to restore the Information Security Officer position
- Redirecting funding to restore the Security Technical Specialist position
- Redirecting funding to create and fill two new Information Systems Security Auditing positions

Through the DPS IT Governance Group, the Department will also

- Examine all security assets in the department including personnel and tools and determine whether they can be leveraged to better advantage to address department-wide security needs.
- After further evaluation, if needed, the department will examine other options to expand the breadth and depth of the department-wide security effort.

Recommendation 2: The department should shut down the Web based Motor Vehicle Registration Renewal System until an appropriate security infrastructure has been defined tested and installed.
No evidence was found during the audit to indicate that DPS information Systems had been compromised. However to address the security issues that were raised, the Department has taken the application off-line as recommended by the Legislative Auditor. The system is currently being assessed to determine the best approach to bringing this application back on-line.

2. Prior Finding Not Resolved: Computer programs developed by DVS contained Security flaws

Recommendation 1: The department should develop formal standards for its web-based computer systems.
The Department will ensure that formal standards will be followed in the development of DVS web-based systems.

Recommendation 2: The Department should thoroughly test all web-based computer systems to determine if they are susceptible to the same weaknesses found in the web-based Motor vehicle Registration Renewal System.
The Department is working with the Department of Administration's InterTechnologies Group to examine other DVS web-based systems for security weaknesses.

3. Poorly configured wireless devices provided a way to bypass the department's firewall.

Recommendation 1: The department should develop standards for wireless technologies.
The department will adopt a department-wide standard for wireless technologies prior to implementing wireless services. The two wireless phones were immediately removed from service when they were reported to DPS staff.

Recommendation 2: The department should periodically scan its environment to search for unauthorized wireless access points.
The department will conduct periodic scans to search for unauthorized wireless access points.

4. Prior Finding not Resolved; Sensitive customer data and critical system components were not properly protected.

Recommendation 1: The department should document standards for the Web-based Motor Vehicle Registration Renewal System.

The Department is conducting a complete review and upgrade of the Vehicle Registration Renewal System including security measures. As a part of that upgrade, applicable standards will be documented.

Recommendation 2: The department should limit accounts assigned to people and software products to the minimum security clearance that is necessary.
As a part of the complete review for the Vehicle Registration and Renewal System, account security and management will be implemented in a way that allows minimum security clearance that is necessary for staff that work with the system.

Recommendation 3: The department should enforce its policy that forbids employees from sharing accounts and passwords.
The department will establish an internal IT audit function. When instances are uncovered that are in conflict with Department policies, they will be investigated and appropriate action will be taken to ensure compliance.

Recommendation 4: The department should enforce its policy that requires employees to select complex passwords that are hard to guess
The department will explore implementing automated complex password enforcement where it is available and will, through selected IT audits, verify the use of complex passwords. When instances are found that that are in conflict with Department policies, they will be investigated and appropriate action will be taken to ensure compliance.

Recommendation 5: The department should fix its security weaknesses that permit access to transactions reports and refund transactions
The upgrade of the Vehicle Registration Renewal system will correct these weaknesses.

5. Prior Finding Not Resolved: The department did not promptly perform important system maintenance procedures.

Recommendation 1: The department should implement procedures to promptly install security-related patches
The Department will enforce the patching procedures identified in the Department's IT security policy.

6. Prior Finding Not Resolved: The department did not adequately monitor its systems

Recommendation 1: The department should define specific security events to log and regularly review those logs to identify potential security breaches or systems misuse by employees
This recommendation will be addressed as a part of the overall strengthening of the department-wide systems security program.

Recommendation 2: The department should periodically scan its computers to search for security weaknesses that are commonly exploited by hackers.
The Department will conduct periodic scans of its computers.