



MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

QUALIFIED VOTER FILE AND
DIGITAL DRIVER'S LICENSE SYSTEMS

DEPARTMENT OF STATE AND
DEPARTMENT OF INFORMATION TECHNOLOGY

March 2005



THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

“...The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.”

– Article IV, Section 53 of the Michigan Constitution

Audit report information may be accessed at:

<http://audgen.michigan.gov>



Michigan
Office of the Auditor General
REPORT SUMMARY

Performance Audit
Qualified Voter File and Digital Driver's
License Systems
Department of State and Department of
Information Technology

Report Number:
23-591-04

Released:
March 2005

The Department of State operates the Qualified Voter File (QVF) System in order to maintain a single Statewide database of registered voters. It also operates the Digital Driver's License (DDL) System to electronically record, store, and query images and signatures of Michigan drivers and personal identification card applicants. The Department of Information Technology provides services to the Department of State. These services include such things as security, server operation and administration, and network communications.

Audit Objective:

To assess the Departments' effectiveness in controlling access to the central QVF database server.

Audit Conclusion:

The Departments were not effective in controlling access to the central QVF database server. Our assessment disclosed one material condition relating to QVF database server security (Finding 1). As a result, there was a significant risk that the Departments' access controls could not prevent or detect unauthorized access to the QVF database server. This could compromise the confidentiality, integrity, and availability of voter registration data.

Material Condition and Agency Response:
QVF Database Server Security

The Departments did not effectively secure the QVF database server (Finding 1).

Agency Response: Both the Department of State and the Department of Information Technology agreed with the finding. The Departments have continued to work together to evaluate and implement reasonable and cost-effective strategies that mitigate the level of risk to the State's QVF database server. The Departments informed us that despite these vulnerabilities, they were not aware of any instances in which the confidentiality, integrity, and availability of QVF information was compromised.

~ ~ ~ ~ ~

Audit Objective:

To assess the Departments' effectiveness in maintaining security over confidential voter registration data during network transmission.

Audit Conclusion:

The Departments were generally effective in maintaining security over confidential voter registration data during network transmission. Our report does not include any reportable conditions related to this audit objective.

~ ~ ~ ~ ~

Audit Objective:

To assess the Departments' effectiveness in monitoring the third-party contractor's efforts to secure the DDL System.

Audit Conclusion:

The Departments were not effective in monitoring the third-party contractor's efforts to secure the DDL System. Our assessment disclosed one material condition related to security concerns with the DDL contract (Finding 2). Consequently, the Departments have assumed an unknown level of risk that the confidentiality, integrity, and availability of driver's license data and images could be compromised, which may lead to identity theft.

Material Condition and Agency Response:
Security Concerns With DDL Contract

The Departments did not ensure that the third-party contractor effectively secured the DDL System (Finding 2).

Agency Response: Both the Department of State and the Department of Information Technology agreed with the finding. The Department of State, in consultation with the Department of Information Technology, has continued to work with the third-party contractor to effectively secure the DDL System. The Departments informed us that despite the noted risks, they were not aware of any instances in which the confidentiality, integrity, and availability of DDL System information was compromised.

~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: <http://audgen.michigan.gov>



Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General



STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

March 18, 2005

The Honorable Terri Lynn Land
Secretary of State
Treasury Building
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
Landmark Building
Lansing, Michigan

Dear Secretary Land and Ms. Takai:

This is our report on the performance audit of the Qualified Voter File and Digital Driver's License Systems, Department of State and Department of Information Technology.

This report contains our report summary; description of systems; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agencies' responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

AUDITOR GENERAL

This page left intentionally blank.

TABLE OF CONTENTS

QUALIFIED VOTER FILE AND DIGITAL DRIVER'S LICENSE SYSTEMS DEPARTMENT OF STATE AND DEPARTMENT OF INFORMATION TECHNOLOGY

| | <u>Page</u> |
|--|-------------|
| INTRODUCTION | |
| Report Summary | 1 |
| Report Letter | 3 |
| Description of Systems | 6 |
| Audit Objectives, Scope, and Methodology and Agency Responses | 8 |
| COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES | |
| Effectiveness in Controlling Access to the Central QVF Database Server | 12 |
| 1. QVF Database Server Security | 12 |
| Effectiveness in Maintaining Security Over Confidential Voter Registration Data | 14 |
| Effectiveness in Monitoring Contractor's Efforts to Secure the DDL System | 14 |
| 2. Security Concerns With DDL Contract | 15 |
| GLOSSARY | |
| Glossary of Acronyms and Terms | 18 |

Description of Systems

The Department of State operates the Qualified Voter File (QVF) System in order to maintain a single Statewide database* of registered voters. It also operates the Digital Driver's License (DDL) System to electronically record, store, and query images and signatures of Michigan drivers and personal identification card applicants.

The Department of Information Technology provides services to the Department of State. These services include such things as security, server operation and administration, and network communications. The Department of Information Technology also acts as a general contractor between the State's information technology users and private sector providers of information technology products and services.

Both Departments share responsibility for the overall security of the QVF and DDL Systems:

a. Qualified Voter File (QVF) System

Mandated under Act 441, P.A. 1994, and placed into operation for the 1998 election cycle, the QVF System links election officials throughout the State to a fully automated, interactive Statewide voter registration database.

The QVF System offers local jurisdictions various election management features, including components created to assist with absent voter ballot processing, petition and candidate tracking, election planning, and election inspector tracking.

The QVF System ties 468 local jurisdictions and 83 counties to a fully automated, interactive Statewide voter registration database that contains the names and addresses of approximately 6.8 million registered voters.

Effective in April 2000, Act 118, P.A. 1999, as amended, requires the Secretary of State to update the QVF System when a driver's license address change occurs.

* See glossary at end of report for definition.

b. Digital Driver's License (DDL) System

Designed to facilitate the production of driver's licenses, the DDL System was first implemented in 1998. DDL processing begins at one of the Department of State's 174 branch offices, where individuals' photographs are taken. Photographs and signatures are digitally captured and, along with demographic data, sent electronically to a third-party contractor.

The Departments contract with a third-party contractor to administer the DDL System. The contractor produces driver's licenses and personal identification cards and administers the DDL System, which stores the digital images after retrieval from the State's network. Our audit coverage included the original DDL System contract, which became effective in 1997, and was later expanded to include a technological upgrade that the Departments will implement in 2004. This upgrade includes replacing image and communication servers as well as image-capturing workstations in the branch offices.

As of January 2004, the Department of State had on file approximately 7.2 million driver's licenses and approximately 1 million personal identification cards.

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of the Qualified Voter File (QVF) and Digital Driver's License (DDL) Systems, Department of State and Department of Information Technology, had the following objectives:

1. To assess the Departments' effectiveness* in controlling access to the central QVF database server.
2. To assess the Departments' effectiveness in maintaining security over confidential voter registration data during network transmission.
3. To assess the Departments' effectiveness in monitoring the third-party contractor's efforts to secure the DDL System.

Audit Scope

Our audit scope was to examine the information processing and other records of the Qualified Voter File System and to review the Departments' monitoring practices and third-party contractual agreements for the Digital Driver's License System. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of the Departments' information processing and other records primarily for the period September 30, 1997 through June 30, 2004. We performed our audit fieldwork from January through June 2004. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

We conducted a preliminary review of the Departments' client/server*, web, and e-commerce* systems. We used this review to determine the extent of our detailed analysis and testing.

* See glossary at end of report for definition.

2. Detailed Analysis and Testing Phase

We performed an assessment of internal control* pertaining to the management and organization of the information technology functions that support the QVF and DDL Systems. Specifically, we assessed:

a. Effectiveness in Controlling Access to the QVF Server and Securing QVF Data:

- (1) We reviewed the systems security policies and procedures.
- (2) We evaluated the security and configuration of the QVF operating system* and database management system using manufacturers' recommendations and best practices.
- (3) We evaluated the controls over the replication process between local jurisdictions and the central QVF database.

b. Effectiveness in Monitoring the Third-Party Contractor's Security Over the DDL System:

- (1) We evaluated the security policies and programs and the monitoring practices in place relating to the third-party contractor.
- (2) We reviewed the audit history of the third-party contractor to determine the completion of independent audits.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase. We provided management with the detailed security weaknesses that support our findings. Many of the security weaknesses are sensitive and could jeopardize the Departments' ability to protect the QVF and DDL Systems if released to the public. This report summarizes the material conditions* we have identified and the recommendations we made.

Agency Responses

Our audit report contains 2 findings and 2 corresponding recommendations. The agency preliminary responses indicated that the Department of State and the

* See glossary at end of report for definition.

Department of Information Technology agreed with the findings and have partially complied or will comply with the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require the Department of State and the Department of Information Technology to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS IN CONTROLLING ACCESS TO THE CENTRAL QVF SYSTEM DATABASE SERVER

COMMENT

Audit Objective: To assess the Department of State's and Department of Information Technology's effectiveness in controlling access to the central Qualified Voter File (QVF) database server.

Conclusion: **The Departments were not effective in controlling access to the central QVF database server.** Our assessment disclosed one material condition relating to QVF database server security (Finding 1). As a result, there was a significant risk that the Departments' access controls could not prevent or detect unauthorized access to the QVF database server. This could compromise the confidentiality, integrity, and availability of voter registration data.

FINDING

1. QVF Database Server Security

The Departments did not effectively secure the QVF database server. As a result, the Departments could not ensure that confidential voter registration data was protected from unauthorized access.

We identified numerous and, in some cases, very significant vulnerabilities in the configuration of the QVF operating system and database that preclude management from preventing or detecting unauthorized access. Several of these vulnerabilities were also identified in an October 2002 vulnerability assessment of the QVF database server performed by a private contractor at the request of the Department of State. These vulnerabilities, if exploited, could result in unauthorized access to voter registration data that may adversely affect the confidentiality, integrity, and availability of the QVF System.

During our review of the QVF database server, we noted the following circumstances that contributed to security vulnerabilities:

- a. The Departments did not prepare and maintain a configuration and security plan for the QVF database server as required by the State's security guidelines.

- b. The Departments indicated that the QVF System, as originally designed by the Department of State in 1997, could not easily be modified to meet the State's current security guidelines. We were informed that the original design strategies were necessary in order to persuade local jurisdictions to accept a single Statewide qualified voter file.

State security strategies and recent federal legislation call for the security of confidential voter information. In October 2001, the Department of Information Technology established security guidelines for server-based information systems. The purpose of these guidelines was to maintain the highest possible security level and system reliability to support the State of Michigan's computing environment. The federal Help America Vote Act of 2002 requires that the appropriate state and/or local officials provide "adequate security"* measures to prevent unauthorized access to computerized voter registration lists, such as Michigan's QVF.

The Departments have expressed concerns that additional system security measures may negatively impact system performance and functionality. However, the Department of State should work with the Department of Information Technology's Office of Enterprise Security to evaluate and implement reasonable and cost-effective strategies that mitigate the level of risk to the State's QVF.

RECOMMENDATION

We recommend that the Departments effectively secure the QVF database server.

AGENCY PRELIMINARY RESPONSE

Both the Department of State and the Department of Information Technology agreed with the finding.

The Departments have continued to work together to evaluate and implement reasonable and cost-effective strategies that mitigate the level of risk to the State's QVF database server. The Departments informed us that they have developed a security plan consistent with the State's security guidelines and have already corrected significant vulnerabilities identified with the existing configuration.

* See glossary at end of report for definition.

Additional security measures are also being reviewed. The Departments also informed us that despite these vulnerabilities, they were not aware of any instances in which the confidentiality, integrity, and availability of QVF information was compromised.

EFFECTIVENESS IN MAINTAINING SECURITY OVER CONFIDENTIAL VOTER REGISTRATION DATA

Audit Objective: To assess the Departments' effectiveness in maintaining security over confidential voter registration data during network transmission.

Conclusion: The Departments were generally effective in maintaining security over confidential voter registration data during network transmission. Our report does not include any reportable conditions* related to this audit objective.

EFFECTIVENESS IN MONITORING CONTRACTOR'S EFFORTS TO SECURE THE DDL SYSTEM

COMMENT

Audit Objective: To assess the Departments' effectiveness in monitoring the third-party contractor's efforts to secure the Digital Driver's License (DDL) System.

Conclusion: The Departments were not effective in monitoring the third-party contractor's efforts to secure the DDL System. Our assessment disclosed one material condition related to security concerns with the DDL contract (Finding 2). Consequently, the Departments have assumed an unknown level of risk that the confidentiality, integrity, and availability of driver's license data and images could be compromised, which may lead to identity theft.

* See glossary at end of report for definition.

FINDING

2. Security Concerns With DDL Contract

The Departments did not ensure that the third-party contractor effectively secured the DDL System. Consequently, the Departments have assumed an unknown level of risk that the confidentiality, integrity, and availability of driver's license data and images could be compromised, which may lead to identity theft.

In reference to managing the services of a third-party contractor, the Control Objectives for Information and Related Technology (COBIT) Framework* highlights the importance of security relationships and monitoring activities. A security plan should be detailed, implemented, and monitored.

Our review of the Departments' efforts to monitor the third-party contractor's security over the DDL System disclosed:

- a. The Departments did not monitor the third-party contractor's security of the DDL System.

COBIT provides management with the framework to effectively monitor information technology resources and services that are contracted to third parties. To increase the confidence and trust among the departments and the third-party contractor, management should obtain independent certification and accreditation of security and internal controls, evaluate the effectiveness of security and internal controls on a routine cycle, and obtain assurance of the third-party contractor's compliance with legal and regulatory requirements.

- b. The Departments' efforts to establish an information security plan for the DDL System fell short of meeting State standards.

The functional design specifications prepared in October 2003 for the extension of the DDL service contract indicate that the Departments began to address the security needs of the DDL System. However, the Departments did not ensure that these needs fully addressed the State's information security standards.

* See glossary at end of report for definition.

A security plan communicates a coherent standard to management and technical staff and defines the procedures to configure, document, and operate resources in order to minimize security risks and formalize ongoing risk-reducing processes.

- c. The Departments did not ensure that the language of the third-party DDL System contract included a detailed security plan and monitoring practices.

The Department of Information Technology's security procedures outline the security expectations for the State's resources. These expectations need to be clearly defined within the language of all information technology contracts to ensure that the Department of Information Technology's security standard is upheld with contractual agreements.

RECOMMENDATION

We recommend that the Departments ensure that the third-party contractor effectively secures the DDL System.

AGENCY PRELIMINARY RESPONSE

Both the Department of State and the Department of Information Technology agreed with the finding.

The Department of State, in consultation with the Department of Information Technology, has continued to work with the third-party contractor to effectively secure the DDL System. The Departments informed us that as part of this effort, a special physical security review was conducted late in 2004 and discussions are continuing on additional monitoring requirements. In addition, the Departments will compare the existing security arrangements with the State's information security standards and will continue to work with the Department of Management and Budget to ensure future contracts routinely provide language which ensures that the security standard is upheld. The Departments also informed us that despite the noted risks, they were not aware of any instances in which the confidentiality, integrity, and availability of DDL System information was compromised.

GLOSSARY

Glossary of Acronyms and Terms

| | |
|---|---|
| adequate security | Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes ensuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls. (Definition taken from Appendix III, "Security of Federal Automated Information Resources," to U.S. Office of Management and Budget Circular A-130, revised.) |
| client/server | A design model used on a network in which individual workstations (clients) and shared servers work together to process applications. In this model, certain functions are allocated to the client workstations and the server. Typically, the server provides centralized, multiuser services, whereas the client workstations support user interaction. |
| Control Objectives for Information and Related Technology (COBIT) Framework | <p>In April 1996, the Information Systems Audit and Control Foundation (ISACF) developed an internal control framework to manage, use, and audit information technology. The framework (referred to as COBIT) consists of 34 high-level control objectives associated with primary information technology processes, grouped into four domains. The four domains are planning and organization, acquisition and implementation, delivery and support, and monitoring.</p> <p>The basic philosophy of the COBIT framework is to center the need for internal controls over information technology processes according to a natural grouping of common information technology processes. The framework is based on the concept that management must first achieve a complete understanding of the department's business processes before it can effectively develop, manage, and audit the processes for implementing information and related</p> |

technology solutions. The framework is based on the underlying assumption that a department's core business processes drive the need for implementing information and related technology. Control objectives define the criteria that must be met to ensure delivery of technology solutions that meet the department's business requirements.

| | |
|--------------------|---|
| database | A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer. |
| DDL | Digital Driver's License. |
| effectiveness | Program success in achieving mission and goals. |
| e-commerce | The process by which organizations conduct business electronically with their customers, suppliers, and other external business partners, using the Internet as an enabling technology. |
| internal control | The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition. |
| material condition | A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program. |

| | |
|----------------------|--|
| operating system | The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running. |
| performance audit | An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action. |
| QVF | Qualified Voter File. |
| reportable condition | A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner. |

This page left intentionally blank.

