Audit Report

Department of Transportation
Office of Transportation Technology Services

April 2009

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.

- Electronic copies of our audit reports can be viewed or downloaded from our website at http://www.ola.state.md.us.

- Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.

- The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Bruce A. Myers, CPA
Legislative Auditor

April 24, 2009

Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Senator Verna L. Jones, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Maryland Department of Transportation – Office of Transportation Technology Services (OTTS). OTTS provides computing and network resources to the modal units of the Maryland Department of Transportation (MDOT), and operates as a computer service bureau for these units. Our audit included an internal control review of the OTTS data center and the network administered by OTTS that supports MDOT and its modal units.

Our audit disclosed that proper internal control had not been established over several significant areas. Specifically, the MDOT internal network was not adequately protected from external exposures. Furthermore, OTTS lacked assurance that a certain critical system was adequately protected.

Systems that operate on the OTTS' computing platforms include the Motor Vehicle Administration's (MVA) Titling and Registration Information System, the MVA Driver's Licensing Processing System, the MVA Maryland International Registration Plan, the Maryland Port Administration's marine terminal system, MDOT's Financial Management Information System, and MDOT's payroll system.

MDOT's response, on behalf of OTTS, to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by OTTS.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

* **Denotes item repeated in full or part from preceding audit report**

Background Information

Agency Responsibilities and Description

The Maryland Department of Transportation - Office of Transportation Technology Services (OTTS) provides computing and network resources to the modal units of the Maryland Department of Transportation (MDOT) and operates as a computer service bureau for these units.

OTTS operates a mainframe computer for applications, which include the Motor Vehicle Administration's (MVA) Titling and Registration Information System, the MVA Driver's Licensing Processing System, the Maryland Port Administration's marine terminal system, MDOT's Financial Management Information System, and MDOT's payroll system. In addition, OTTS also operates certain server-based applications, such as the Maryland International Registration Plan, which processes the registration of interstate commercial vehicles and associated fees. OTTS, in conjunction with an MDOT contractor, operates a wide area network (WAN) connecting computer users from the modal units and headquarters, as well as providing connections to a few State networks and to multiple external vendor networks associated with the modal units' activities. The WAN performs data transmission using a large number of routers.

OTTS provides numerous network services to the above-described parties including Internet access, email service, and remote access to various servers within the internal network via Virtual Private Network (VPN) and web-based connections. We were advised by agency personnel that approximately 9,000 individuals use the MDOT network. According to OTTS records, the WAN connects to more than 200 remote locations. For fiscal year 2008, OTTS had 114.5 authorized positions and expenditures totaled approximately $34.5 million.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the four findings contained in our preceding audit report dated October 17, 2005. We determined that OTTS satisfactorily addressed three of these four findings. The remaining finding is repeated in this report.

We also determined the status of one finding included in our preceding audit report, dated August 31, 2005, on the Maryland Port Administration that was applicable to a function performed by OTTS. Because OTTS did not satisfactorily address this prior audit recommendation, it is repeated in this report.

Findings and Recommendations

Network Security and Control

Background

The Maryland Department of Transportation's (MDOT) wide area network includes numerous backbone routers, core routers within the MDOT modal administrations, and distribution routers, which serve as connections for remote locations. In addition, MDOT employs numerous firewalls and virtual private network (VPN) devices to help enforce security on the MDOT wide area network. Furthermore, OTTS uses automated processes and tools to assist in the administration and monitoring of these devices.

The MDOT wide area network also includes the Maryland Port Administration (MPA) network and a connection to the Internet. MPA operates an internal computer network connecting various Port of Baltimore marine terminals and office locations. MPA uses a critical system to support operations at its marine terminals; a key component of this system tracks shipping containers that enter and leave the Port. A dedicated firewall is maintained by OTTS to help protect the servers that host this system.

Finding 1
Critical network devices were not securely configured to protect against attack.

Analysis

Critical network devices were not securely configured to protect against attack. Specifically, we performed a security review of a backbone router, a core router, and a distribution router. For all three routers tested, we found that certain controls over how network traffic was routed could be circumvented because of a configuration command that was enabled, but should have been disabled. Furthermore, we noted that administrative connections to all three routers tested used insecure (not encrypted) protocols, and that connection lines to all three routers were not properly secured.

The Department of Information Technology's (DoIT) *State Network Security Standard* states that all network devices (including routers) shall be hardened against attack.

Recommendation 1
We recommend that adequate controls be established over all backbone, core, and distribution routers to protect the MDOT wide area network from security exposures. We made detailed recommendations to OTTS, which, if implemented, should provide for adequate security over these devices.

Finding 2
Administration and monitoring of critical firewalls and VPN devices were not adequate.

Analysis
Administration and monitoring of critical firewalls and VPN devices on the MDOT wide area network were not adequate. Specifically, we noted the following conditions:

- Password and account controls set on two authentication servers used to authenticate administrators attempting to access numerous firewalls and VPN devices were not in compliance with related DoIT and MDOT standards. For example, password aging and account lockout were not enabled. In this regard, MDOT requires passwords to be changed every 30 days and DoIT requires that accounts be disabled after not more than four consecutive failed logon attempts.

- Passwords on a critical firewall (which did not use the aforementioned authentication servers) were not changed in a timely manner. We noted that, as of July 10, 2008, passwords for the six administrator accounts on this firewall had not been changed for periods ranging from 65 to 294 days.

- OTTS consolidated all firewall and VPN device activity onto a central logging server and used an automated script to identify significant security events. However, this script was out of date and did not identify several critical security events for newer devices placed into production. As a result, certain critical security-related events were not identified for review and follow up. DoIT's *State Network Security Standard* requires that agencies maintain comprehensive audit trails that allow for monitoring of all critical security events.

Recommendation 2
We recommend that OTTS

a. ensure that password and account controls are in compliance with both MDOT and DoIT standards; and

b. update, on a continuing basis, its firewall and VPN logging script to identify all critical security events for these devices.

Finding 3
The MDOT internal computer network was not adequately secured from external exposures.

Analysis
The MDOT internal network was not adequately secured from external exposures from untrusted third parties. Specifically, certain traffic from numerous untrusted third parties, including certain contractors and federal agencies, was not adequately filtered. Therefore, such traffic could unnecessarily access, at the network level, MDOT internal network devices.

Access rules for critical network devices should use a "least privilege" security strategy which gives users only the access needed to perform assigned tasks.

Recommendation 3
We recommend that adequate controls be established to protect the internal network from external exposures. We made detailed recommendations to OTTS, which, if implemented, should provide for adequate security in this area.

Finding 4
MPA's internal network was not adequately secured from external exposures and the firewall protecting this network was not properly secured.

Analysis
MPA's internal network was not adequately secured from external exposures and the firewall protecting this network was not properly secured. Specifically, we noted the following conditions:

- Several untrusted connections (including the Internet and the MDOT wide area network) had unnecessary access, at a network level, to numerous

internal network devices. A similar condition was commented upon in our preceding audit report on the Maryland Port Administration dated August 31, 2005.

- Numerous firewall rules existed which were either no longer necessary or addressed network devices that were no longer in use.

- The password and account controls over the server which hosts the firewall protecting the MPA network were not adequate. Specifically, accounts did not need passwords and, after a designated number of consecutive failed logon attempts, account lock out was not enabled.

Access rules for critical network devices should use a "least privilege" security strategy, which gives users only the access needed to perform assigned tasks. Furthermore, DoIT's *State Security Access Control Standard* requires the use of strong passwords and account lockout.

Recommendation 4
We recommend

a. that OTTS adjust the aforementioned firewall rules to implement a "least privilege" security strategy to properly protect MPA's critical system (repeat), and

b. that password and account controls on the server hosting MPA's firewall comply with the requirements of DoIT's *State Security Access Control Standard*.

Data Center Information System Security and Control

Finding 5
Data security controls pertaining to a critical OTTS database application were not adequate.

Analysis
Data security controls pertaining to the Maryland International Registration Plan (MIRP) system were not adequate. Specifically, we noted the following conditions:

- Password complexity, expiration, history, and account lockout for six user accounts did not meet the requirements of DoIT's *State Security Access Control Standard.* For example, the database system account lockout was not

utilized for these accounts (that is, these accounts were not disabled after a set number of failed login attempts).

- Thirty-one users had unnecessary, direct modification access, at the operating system level, to critical MIRP database directories and associated database files.

- Database rules unnecessarily granted modification access to 134 database tables to a default group, which gave 28 active database users this access.

- Security monitoring for the MIRP database was inadequate because auditing capabilities (such as for certain critical privileges) for the database system were not enabled.

MIRP is an application used for the registration of interstate commercial vehicles and the collection of associated fees. According to the State's accounting records, such registration fees collected during fiscal year 2008 totaled approximately $50.7 million. As a result of the above conditions, unauthorized or inappropriate changes could be made to the database without detection by management. Similar conditions were commented upon in our preceding audit report.

Recommendation 5

We recommend

a. that MIRP password and user account settings comply with the requirements of the aforementioned DoIT *Standard* (repeat),

b. that access rules permit modification access to only those individuals who require such access for their job responsibilities (repeat),

c. that MIRP database auditing be enabled and the recorded information be reported and reviewed (repeat), and

d. that evidence of the reviews be retained for audit verification (repeat).

Audit Scope, Objectives, and Methodology

We have audited the Maryland Department of Transportation (MDOT) - Office of Transportation Technology Services (OTTS). Fieldwork associated with our audit of the data center was conducted during the period from December 2007 to April 2008. Additionally, fieldwork associated with our audit of the network was conducted during the period from July 2008 to January 2009. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine OTTS' internal control over its data center and network and to evaluate its compliance with applicable State laws, rules, and regulations for the computer systems that support MDOT and modal user agencies. Specifically, given OTTS's widespread responsibility for the MDOT Network, our audit included an evaluation of the security control environment for all portions of the MDOT Network controlled by OTTS. Our audit also included an assessment of the security controls for critical routers, firewalls, switches and virtual private network appliances, as well as an assessment of security controls related to MDOT's wireless connectivity, the use of software vulnerability assessments for critical network servers, and the controls over internal MDOT network traffic between modal administrations. OTTS' fiscal operations are audited separately as part of our audit of the MDOT – Secretary's Office. The latest report that covered OTTS' fiscal operations was issued on July 7, 2006. We also determined the status of the findings included in our preceding audit report on OTTS and the status of one of the seven findings included in our preceding audit report on the Maryland Port Administration that was applicable to a function performed by OTTS.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of materiality and risk. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of OTTS' operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

OTTS' management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect OTTS' ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to OTTS that did not warrant inclusion in this report.

MDOT's response, on behalf of OTTS, to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise MDOT regarding the results of our review of its response.

APPENDIX

Maryland Department of Transportation
The Secretary's Office

Martin O'Malley
Governor

Anthony G. Brown
Lt. Governor

John D. Porcari
Secretary

Beverley K. Swaim-Staley
Deputy Secretary

April 22, 2009

Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
Department of Legislative Services
301 West Preston Street
Baltimore MD 21201

Dear Mr. Myers:

Enclosed please find the Department's responses to the draft Legislative Auditor's Report dated April 7, 2009 pertaining to your audit of the Maryland Department of Transportation – Office of Transportation Technology Services for the period ending November 2008. Additionally, an electronic version of this document has been sent to your office via email (filename: OTTSFinal DraftResponsesApril2009) to response@ola.state.md.us.

If we may be of further assistance, please do not hesitate to contact me or Mr. David L. Fleming, Chief Financial Officer, Maryland Department of Transportation (MDOT) at 410-865-1035, toll-free 888-713-1414 or via email at dfleming@mdot.state.md.us.

Sincerely,

John D. Porcari
Secretary

Enclosure

cc: Mr. Charles Bristow, Chief Information Officer, Maryland Department of Transportation
Mr. David L. Fleming, Chief Financial Officer, Maryland Department of Transportation
Mr. Joseph J. Lambdin, Director, Office of Audits, Maryland Department of Transportation
Mr. Guy Reihl, Director, Office of Transportation Technology Services, Maryland Department of Transportation
Ms. Beverley K. Swaim-Staley, Deputy Secretary, Maryland Department of Transportation

Maryland Department of Transportation
Office of Transportation Technology Services
Draft Legislative Audit Report Responses
For the period ending November 2008

Network Security and Control

Finding #1
Critical network devices were not securely configured to protect against attack.

MDOT RESPONSE:
The Department concurs with the auditor's recommendations and will implement adequate controls over all backbone, core and distribution routers to further harden those devices.

Finding # 2
Administration and monitoring of critical firewalls and VPN devices were not adequate.

MDOT RESPONSE:
a. The Department concurs with the auditor's recommendation and will ensure that all firewalls comply with password and account control standards.

b. The Department concurs with the auditor's recommendation and will update its logging script on a continuing basis.

Finding #3
The MDOT internal computer network was not adequately secured from external exposures.

MDOT RESPONSE:
The Department concurs with the auditor's recommendations and will implement the appropriate controls to protect the MDOT Network from external exposures.

Finding # 4
MPA's internal network was not adequately secured from external exposures and the firewall protecting this network was not properly secured.

MDOT RESPONSE:
a. The Department concurs with the auditor's recommendation and has implemented the recommended controls.

b. The Department concurs with the auditor's recommendation and has implemented the recommended controls.

Maryland Department of Transportation
Office of Transportation Technology Services
Draft Legislative Audit Report Responses
For the period ending November 2008

Data Center Information System Security and Control

Finding #5
Data security controls pertaining to a critical OTTS database application were not adequate.

MDOT RESPONSE:

a. The Department concurs with the auditor's recommendation and will implement the appropriate controls effective July 1, 2009.

b. The Department concurs with the auditor's recommendation and will implement the appropriate controls effective July 1, 2009.

c. The Department concurs with the auditor's recommendation and will implement the appropriate controls effective July 1, 2009.

d. The Department concurs with the auditor's recommendation and will implement the appropriate controls effective July 1, 2009.

AUDIT TEAM

Richard L. Carter, CISA
Steven P. Jersey, CPA, CISA
Information Systems Audit Managers

R. Brendan Coffey, CPA
Edwin L. Paul, CPA
Information Systems Senior Auditors

David J. Burger
Amanda L. Trythall
Information Systems Staff Auditors