Audit Report

Department of Transportation
Office of Transportation Technology Services

March 2014

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

March 24, 2014

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Delegate Guy J. Guzzone, 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 transportation business units (TBU) 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 TBUs.

Our audit disclosed that logging and monitoring of security-related events for critical databases were not sufficient and that monitoring and access controls over critical firewalls (including Internet facing firewalls) also were not sufficient to ensure OTTS' network was properly secured. We also noted that the intrusion detection and prevention system was not properly used or protected.

Systems that operate on 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,

Thomas J Barnickel III

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

Information Systems Security and Control

Background Information

Agency Responsibilities

The Maryland Department of Transportation - Office of Transportation Technology Services (OTTS) provides computing and network resources to the transportation business units (TBU) 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 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 TBUs and headquarters, as well as providing connections to a few State networks and to multiple external vendor networks associated with the TBUs' 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 a virtual private network and web-based connections. We were advised by agency personnel that approximately 13,000 individuals use the MDOT network. According to OTTS records, the WAN connects to more than 200 remote locations.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the five findings contained in our preceding audit report dated April 24, 2009. We have determined that OTTS had satisfactorily addressed all five of these findings.

Findings and Recommendations

Information Systems Security and Control

Finding 1
Logging and monitoring of security-related events for critical databases were not sufficient.

Analysis
Logging and monitoring of security-related events were not sufficient to readily identify potential unauthorized database modifications. Specifically, we noted the following conditions:

- For an important database, the use of numerous critical privileges (for example, grant any privilege and update any table) was not logged. In addition, the Maryland Department of Transportation (MDOT) - Office of Transportation Technology Services (OTTS) did not investigate insert, update, and delete activity for nine tables used by this database. Finally, even when security logs were reviewed for this database, documentation supporting the events identified on these logs was not obtained or reviewed.

- Changes made by five accounts that were authorized to directly modify critical production tables for numerous transportation business units' (TBU) databases were not reviewed.

The Maryland Department of Information Technology's (DoIT) *Information Security Policy,* requires that information systems must generate audit records for all security-relevant events and that procedures must be developed to routinely (for example daily or weekly) review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials for prompt resolution.

Recommendation 1
We recommend that OTTS

a. log the use of all critical system privileges and investigate the use of insert, update, and delete activity for the aforementioned database;
b. properly investigate any unusual security events associated with this database, document these investigations, and retain the resultant documentation for future reference; and
c. review all direct modifications to the aforementioned TBU critical production database tables.

Finding 2
Monitoring and access controls over critical firewalls were not sufficient to ensure OTTS' network was properly secured.

Analysis
Monitoring and access controls over critical firewalls were not sufficient to ensure OTTS' network was properly secured. Specifically, we noted the following conditions:

- Our review of 12 firewalls with Internet interfaces disclosed that firewall configuration changes were not monitored for 4 of these 12 firewalls and that changes to existing firewall rules were not monitored for 5 additional firewalls. We also noted that failed firewall login attempts were not monitored for 9 of these 12 firewalls. As a result of these conditions, OTTS lacked assurance that all firewalls were properly configured to protect the MDOT network.

- Remote administrative access to the OTTS data center's two redundant firewalls was not adequately restricted to network administrators and network management servers. Firewall rules improperly allowed the entire MDOT internal network to establish remote connections to these two firewalls.

DoIT's *Information Security Policy* requires that only authorized individuals have access to confidential information and that such access is strictly controlled, audited and that it supports the concepts of "least possible privilege" and "need to know."

Recommendation 2
We recommend that OTTS

a. review all configuration changes (including changes to firewall rules) for its critical firewalls,
b. monitor failed firewall login attempts for its critical firewalls, and
c. limit remote administrative connections to the data center's redundant firewalls to network administrators and network management servers.

Finding 3
The intrusion detection and prevention system was not properly used or protected.

Analysis

OTTS operated a network-based intrusion detection and prevention system (IDPS) to help secure the MDOT network. However, the IDPS was not properly used or protected. Specifically, we noted the following conditions:

- IDPS coverage did not exist for numerous untrusted third-party network connections into the MDOT wide area network. Although IDPS protection existed for many untrusted third-party connections, we identified numerous untrusted third-party connections (for example Internet and vendor connections) that were not subject to IDPS coverage.

- Remote administrative access to the network-based IDPS module was not adequately restricted to only those users who required such access. Any address on the MDOT wide area network could make a connection to the IDPS module and attempt a login.

- Password controls over access to the network-based IDPS module were not in accordance with DoIT *Information Security Policy* requirements. Specifically, password aging, complexity and history requirements were not adequately enforced.

DoIT's *Information Security Policy* requires that agency systems be configured to monitor and control communications at external boundaries. Strong network security uses a layered approach, relying on various resources, and is structured according to assessed network security risk. Properly configured IDPS protection can aid significantly in the detection/prevention of and response to potential network security breaches and attacks. Furthermore, without proper monitoring, critical network security breaches may occur that could otherwise possibly be detected and prevented.

Recommendation 3

We recommend that OTTS

a. **perform a documented review and assessment of its network security risks, identify how IDPS coverage should be best applied to the MDOT network, and implement such coverage for all critical portions of the MDOT network;**

b. **restrict remote access to the network-based IDPS module to only those users requiring such access; and**

c. implement password controls over the IDPS module that comply with the aforementioned DoIT's *Information Security Policy* requirements.

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 June 2012 to June 2013. Additionally, fieldwork associated with our audit of the network was conducted during the period from March 2013 to August 2013. 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's internal control over its data center and network and to evaluate its compliance with applicable State laws, rules, and regulations for computer systems that support MDOT and the transportation business units (TBU). 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. 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 November 2, 2012. We also determined the status of the findings included in our preceding audit report.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of materiality and risk. The areas addressed by the audit included procedures and controls over the mainframe operating system, security software, and critical databases. 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 over internal MDOT network traffic between TBUs. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of OTTS's operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. The reliability of data used in this report for background or informational purposes was not assessed.

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 that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect OTTS' ability to 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

James T. Smith, Jr.
Secretary

March 14, 2014

Thomas J. Barnickel III, CPA
Acting Legislative Auditor
Office of Legislative Audits
Department of Legislative Services
Room 1202
301 West Preston Street
Baltimore MD 21201

Dear Mr. Barnickel:

Enclosed please find the Department's responses to the draft Legislative Auditor's Report for the Maryland Department of Transportation (MDOT) – Office of Transportation Technology Services (OTTS). Additionally, an electronic version of this document has been sent to your office via email at response@ola.state.md.us.

If you have any questions or need additional information, please do not hesitate to contact me or Mr. David L. Fleming, Chief Financial Officer. Mr. Fleming can be reached at 410-865-1035.

Sincerely,

James T. Smith, Jr.
Secretary

Enclosure

cc: Ms. Brenda Cachuela, Director, Office of Audits, Maryland Department of Transportation
Mr. Leif A. Dormsjo, Deputy Secretary, Maryland Department of Transportation
Mr. David L. Fleming, Chief Financial Officer, Maryland Department of Transportation
Mr. Wilson H. Parran, Deputy Secretary, Maryland Department of Transportation
Mr. B. Guy Reihl, Acting Director, Office of Transportation Technology Services, Maryland Department of Transportation

Maryland Department of Transportation
Office of Transportation Technology Services
Draft Audit Report Responses

Information Systems Security and Control

Finding 1
Logging and monitoring of security-related events for critical databases were not sufficient.

Recommendation 1
We recommend that OTTS

a. log the use of all critical system privileges and investigate the use of insert, update, and delete activity for the aforementioned database;
b. properly investigate any unusual security events associated with this database, document these investigations, and retain the resultant documentation for future reference; and
c. review all direct modifications to the aforementioned TBU critical production database tables.

Response 1:

MDOT concurs with the findings and will implement the recommendations. Recommendations a and c have already been implemented. Work is in progress on recommendation b and will be implemented by June 30, 2014.

Finding 2
Monitoring and access controls over critical firewalls were not sufficient to ensure OTTS' network was properly secured.

Recommendation 2
We recommend that OTTS

a. review all configuration changes (including changes to firewall rules) for its critical firewalls,
b. monitor failed firewall login attempts for its critical firewalls, and
c. limit remote administrative connections to the data center's redundant firewalls to network administrators and network management servers.

Maryland Department of Transportation
Office of Transportation Technology Services
Draft Audit Report Responses

Response 2:
MDOT concurs with the findings. All of the recommendations have been implemented.

Finding 3
The intrusion detection and prevention system was not properly used or protected.

Recommendation 3
We recommend that OTTS

a. **perform a documented review and assessment of its network security risks, identify how IDPS coverage should be best applied to the MDOT network, and implement such coverage for all critical portions of the MDOT network;**

b. **restrict remote access to the network-based IDPS module to only those users requiring such access; and**

c. **implement password controls over the IDPS module that comply with the aforementioned DoIT's *Information Security Policy* requirements.**

Response 3:
MDOT concurs with the findings and recommendations. Recommendations b and c have been implemented. Concerning recommendation a, the documented review will be initiated by June 30, 2014 and implemented thereafter, the time line will be subject to the outcome of the analysis.

Audit Team

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

R. Brendan Coffey, CPA, CISA
Omar A. Gonzalez, CPA
Information Systems Senior Auditors

J. Gregory Busch
Matthew D. Walbert
Information Systems Staff Auditors