Audit Report

Maryland Department of Transportation
Office of Transportation Technology Services

April 2019

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900
Toll Free in Maryland: 1-877-486-9964
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

April 1, 2019

Senator Craig J. Zucker, Co-Chair, Joint Audit Committee
Delegate Shelly L. Hettleman, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Maryland Department of Transportation (MDOT) – Office of Transportation Technology Services (OTTS). OTTS provides computing and network resources to the transportation business units (TBUs) of 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 intrusion detection and prevention system (IDPS) coverage did not exist for encrypted traffic flowing into OTTS data center servers. The absence of this IDPS coverage creates a network security risk, as such traffic could contain undetected malicious data. We also noted that certain OTTS servers and a management server used for administering network routers and switches on the MDOT wide area network were running outdated software, making them vulnerable to malicious software.

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.

Our audit also included a review to determine the status of the three findings contained in our preceding audit report. We determined that OTTS satisfactorily addressed these findings.

MDOT's response to this audit, on behalf of OTTS, is included as an appendix to

this report. We reviewed the response to our findings and related recommendations, and have concluded that the corrective actions identified are sufficient to address all audit issues.

We wish to acknowledge the cooperation extended to us during the audit by OTTS. We also wish to acknowledge MDOT's and OTTS' willingness to address the audit issues and implement appropriate corrective actions.

Respectfully submitted,

Gregory A. Hook

Gregory A. Hook, CPA
Legislative Auditor

Background Information

Agency Responsibilities

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

OTTS operates a data center with 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 registrations 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 certain 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 22,000 user accounts were defined for use on 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 three findings contained in our preceding audit report dated March 24, 2014. We determined that OTTS satisfactorily addressed these findings.

Findings and Recommendations

Information Systems Security and Control

Finding 1
Intrusion detection and prevention system (IDPS) coverage did not exist for encrypted traffic flowing into the Office of Transportation Technology Services (OTTS) data center.

Analysis
IDPS coverage did not exist for untrusted encrypted traffic flowing into the OTTS data center. Specifically, neither server host-based intrusion prevention system coverage nor network device decryption and inspection coverage occurred for such encrypted traffic. We identified 17 firewall rules that allowed traffic from any source to 42 unique server destinations inside the data center, via encrypted methods without IDPS coverage. The absence of IDPS coverage for untrusted encrypted traffic entering the data center creates a network security risk, as such traffic could contain undetected malicious data.

The State of Maryland *Information Security Policy* requires protection against malicious code and attacks by using IDPS coverage to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information. 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.

Recommendation 1
We recommend that OTTS ensure that IDPS protection exists for all critical portions of the MDOT network including encrypted traffic flowing to critical servers within the OTTS data center.

Finding 2
Certain OTTS servers were running outdated device management or operating system software, which made them vulnerable to malicious software.

Analysis
Certain OTTS servers were running outdated device management or operating system software. Consequently, assurance was lacking that the related servers and network devices were properly protected against malicious software.

- An OTTS server, used to control administrative access to over 1,200 devices on MDOT's wide area network, was running outdated network device management software that was no longer supported by the related developer. As a result, no security updates had been provided for this software since July 31, 2017. At the time of our review, this software was subject to three known, high-risk software vulnerabilities.

- Twenty-four other OTTS servers were running outdated operating system software, which was no longer supported by the operating system developer. Developer support for this software ended July 14, 2015, and since then updates for this software to address newly discovered vulnerabilities have not been provided.

The above conditions create potential system security vulnerabilities from malicious software. The State of Maryland *Information Security Policy* states that system hardening procedures shall be created and maintained to ensure up-to-date security best practices are deployed at all levels of IT systems (operating systems, applications, databases, and network devices).

Recommendation 2
We recommend that OTTS ensure all servers operate with current and vendor supported versions of administration software and operating system software.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of 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 2017 to September 2017. Additionally, fieldwork associated with our audit of the network was conducted during the period from December

2017 to April 2018. 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 computer systems that support MDOT and the transportation business units (TBUs). Specifically, given OTTS' 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.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of significance 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. We also determined the status of the findings included in our preceding audit report.

Our audit did not include OTTS' fiscal operations which are audited separately as part of our audit of the MDOT – Secretary's Office. At this report's publication, the latest report that covered OTTS' fiscal operations was issued on February 1, 2016.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of OTTS' operations. We also performed other auditing procedures that we considered necessary to achieve our audit 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 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 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

Larry Hogan
Governor

Boyd K. Rutherford
Lt. Governor

Pete K. Rahn
Secretary

Office of the Secretary

March 25, 2019

Gregory A. Hook, CPA
Office of Legislative Audits
Department of Legislative Services
301 West Preston Street, Room 1202
Baltimore MD 21201

Dear Mr. Hook:

Enclosed please find the Maryland Department of Transportation Office of Transportation Technology Services (MDOT OTTS) responses to the Office of Legislative Audit's audit report dated March 2019. Additionally, an electronic version of this document has been sent to your office via email.

If you have any additional questions or concerns, please contact Ms. Jaclyn D. Hartman, MDOT Chief Financial Officer at 410-865-1035 or jhartman1@mdot.maryland.gov. Of course, you may always contact me directly.

Sincerely,

Pete K. Rahn
Secretary

Confidential Enclosures

cc: Ms. Jaclyn D. Hartman, Chief Financial Officer, MDOT

Maryland Department of Transportation
Office of Transportation Technology Services
Audit Responses
March 2019

Information Systems Security and Control

Finding 1
Intrusion detection and prevention system (IDPS) coverage did not exist for encrypted traffic flowing into the Office of Transportation Technology Services (OTTS) data center.

Recommendation 1
We recommend that OTTS ensure that IDPS protection exists for all critical portions of the MDOT network including encrypted traffic flowing to critical servers within the OTTS data center.

Response:

MDOT concurs with the recommendation and have been actively remediating since before the audit began. Remediation is expected to be complete in June 2019.

Finding 2
Certain OTTS servers were running outdated device management or operating system software, which made them vulnerable to malicious software.

Recommendation 2
We recommend that OTTS ensure all servers operate with current and vendor supported versions of administration software and operating system software.

Response:

MDOT concurs with the recommendation. Remediation of these systems is in progress, with an expected completion date of August 2019.

AUDIT TEAM

Richard L. Carter, CISA
R. Brendan Coffey, CPA, CISA
Information Systems Audit Managers

J. Gregory Busch, CISA
Edwin L. Paul, CPA, CISA
Information Systems Senior Auditors

Joseph R. Clayton
Robert H. Dean
Roman J. Gouin
Information Systems Staff Auditors