Audit Report

Comptroller of Maryland
Information Technology Division
Annapolis Data Center Operations

March 2015

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 through the Office's website, by a toll-free call to 1-877-FRAUD-11, or by mail to the Fraud Hotline, c/o Office of Legislative Audits.

The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

March 31, 2015

Senator Guy J. Guzzone, Co-Chair, Joint Audit Committee
Delegate Craig J. Zucker, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Comptroller of Maryland – Information Technology Division (ITD). ITD operates the Annapolis Data Center which provides computing and network resources and operates as a computer services bureau for the Comptroller of Maryland and other customer agencies. Our audit included an internal control review of the data center and network administered by ITD.

Our audit disclosed that mainframe security software access controls were not adequate, and ITD did not properly monitor mainframe security software reports and changes to critical production procedure programs. In addition, on-site contractors had unnecessary access to critical ITD systems, and sensitive information maintained on the mainframe was not protected from inappropriate disclosure.

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

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

Table of Contents

Background Information 4

Agency Responsibilities 4
Status of Findings From Preceding Audit Report 4

Findings and Recommendations 5

Mainframe Software
* Finding 1 – Mainframe Security Software Access and Monitoring Controls Were Not Sufficient 5

Network Security
* Finding 2 – Contractors Had Unnecessary Network-Level Access to the Comptroller's Network 6
Finding 3 – Controls Over the Comptroller's Data Loss Prevention System Need Improvement 6

Audit Scope, Objectives, and Methodology 8

Agency Response Appendix

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

Background Information

Agency Responsibilities

The Information Technology Division (ITD) operates the Annapolis Data Center as a computer service bureau, and all operating costs are reimbursed by user agencies that are charged for services performed. In addition, ITD develops and maintains application systems for agencies under the Comptroller of Maryland and provides data center disaster recovery capabilities. Additionally, ITD maintains the operating system and security software environment in which agency applications are executed. Some of the applications supported by ITD include the Maryland State Integrated Tax System, the State Payroll System, the Maryland State Financial Management and Information System, and the State's Medical Care Programs Administration (Medicaid) System.

ITD operates an internal network that provides services, including Internet and Statewide Intranet access, email, and file sharing, to all the divisions of the Comptroller of Maryland. According to the State's records, ITD fiscal year 2014 expenditures totaled approximately $27 million.

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 December 21, 2010. We determined that these findings were not satisfactorily addressed and are repeated as two findings in this report.

Findings and Recommendations

Mainframe Software

Finding 1
Mainframe security software access and monitoring controls were not sufficient.

Analysis
Mainframe security software access and monitoring controls were not adequate.

- Fifteen accounts had unnecessary direct unlogged or logged access to many critical production programs and 18 accounts had necessary but unlogged access to many critical production programs. Accordingly, unauthorized changes to these production programs could occur, that could result in inappropriate changes to production data and, for unlogged items, these changes could go undetected.

- Security software violation logs for certain critical ITD data files only included violations by ITD employees, rather than all violations, which would include other agency users. In addition, although the violation logs for all other critical ITD data files included violations from all employees, ITD's review of these logs only included activity by ITD personnel. Accordingly, there was a lack of assurance as to the propriety of the changes made to critical data files.

- Changes to critical production procedure programs, which initiate and control the processing of agency production programs and data files, were not adequately monitored. Specifically, for 8 of 14 of these changes tested, there was no documentation evidencing that these program changes were independently reviewed by management. As a result, there was a lack of assurance that production data and programs were processed in a manner approved by management.

Similar conditions were commented upon in our preceding audit report.

Recommendation 1
We recommend that ITD
a. restrict access to critical production programs to only those individuals requiring such access and log all such accesses (repeat),
b. ensure that violation logs include all violations and that the review of these logs includes activity for all users (repeat), and

c. ensure that all changes made to production procedure programs are independently reviewed and approved by appropriate supervisory personnel and retain evidence of these reviews and approvals (repeat).

Network Security

Finding 2
Contractors had unnecessary network-level access to the Comptroller's network.

Analysis
Contractors had unnecessary network-level access to the Comptroller's network. The Comptroller was developing several new systems with extensive use of untrusted contractors. These contractors worked both on-site at Comptroller locations and remotely with assigned virtual computers on the Comptroller's network. We were advised that these contractors only required access to the specific development servers involved with their projects and certain support servers, such as email servers. Although, ITD had implemented various controls to help secure its network from these contractors, these contractors had unnecessary network-level access to numerous Comptroller workstations and critical servers other than the aforementioned development servers. A similar condition was commented upon in our preceding audit report.

Recommendation 2
We recommend that ITD restrict each contractor's network-level access to only those servers and workstations that each contractor needs to access (repeat).

Finding 3
Controls over the Comptroller's Data Loss Prevention system need improvement.

Analysis
Controls over the Comptroller's Data Loss Prevention (DLP) system need improvement. Specifically, ITD implemented a DLP system to scan outbound network traffic for exfiltration of sensitive personally identifiable information (PII) which is stored on the Comptroller's network. Our review of this DLP system disclosed the following conditions:

- The devices used to scan this outbound traffic were configured to only monitor traffic and not block traffic that contains sensitive PII.

- Formal reviews of the DLP system logs were not performed. In addition, documentation of any informal reviews that were performed did not exist. As such, there was a lack of assurance that these reviews were performed.

- We were advised that encrypted outbound traffic for an estimated 90 percent of the users was not scanned by the DLP scanning devices. For the DLP devices to monitor encrypted traffic the traffic must first be decrypted and then scanned. However, the encrypted outbound traffic was not decrypted before it was sent to the DLP scanning devices.

As a result of these conditions, there was a lack of assurance that unauthorized transmissions of PII did not occur.

Guidance from the Department of Information Technology's *Information Security Policy* states that agencies must protect confidential data using encryption technologies and/or other substantial mitigating controls (such as Data Loss Prevention, Network Security Event Monitoring and strict database change monitoring). The policy also states that a comprehensive DLP solution includes use of an automated tool on network perimeters that blocks sensitive information transfers while alerting information security personnel.

Recommendation 3
We recommend that ITD

a. configure the DLP devices to block unauthorized transmissions that contain sensitive PII,
b. document all reviews of DLP system logs of outbound traffic scanned by the DLP devices and retain this documentation for future reference, and
c. decrypt all outbound encrypted traffic sent to the DLP scanning devices.

Audit Scope, Objectives, and Methodology

We have audited the Comptroller of Maryland – Information Technology Division (ITD). Fieldwork associated with our audit of ITD was conducted during the period from June 2014 to January 2015. 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 State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine ITD's internal control over the Comptroller's data center and network and to evaluate its compliance with applicable State laws, rules, and regulations for the computer systems that support the Comptroller and user agencies. ITD's fiscal operations are audited separately as part of our audit of ITD. The latest report that covered ITD's fiscal operations was issued on June 16, 2014.

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 the security controls related to ITD's wireless connectivity and the use of anti-malware software to protect the Comptroller's computers. We also determined the state of the findings included in our preceding audit report on ITD.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of ITD'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.

ITD's 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 ITD's ability to operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes a finding regarding a significant instance of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to ITD that did not warrant inclusion in this report.

The response from the Comptroller, on behalf of ITD, 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 the Comptroller regarding the results of our review of its response.

APPENDIX

COMPTROLLER of MARYLAND
Serving the People

Peter Franchot
Comptroller

David F. Roose
Deputy Comptroller

March 26, 2015

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

Dear Mr. Barnickel:

Thank you for the opportunity to respond to your audit report on the Comptroller of the Treasury - Information Technology Division (ITD) for the period beginning December 31, 2009 and ending June 2, 2014.

Enclosed is our response to the recommendations contained in the audit report. We thank you and your staff for providing suggestions and recommendations, most of which have already been implemented, that will enable the Division to improve fiscal operations and strengthen internal controls.

If you desire any additional information, we will be happy to respond to your request.

Sincerely,

David F. Roose
Deputy Comptroller

Stan Kizior, Director
Information Technology Division

Enclosure
cc. The Honorable Peter Franchot

Finding #1—Mainframe security software access and monitoring controls were not sufficient

The Information Technology Division (ITD) agrees with the principle of "least possible privileges" and that this type of access should be logged. ITD has reviewed the access, removed the unnecessary accounts, and enabled logging for accounts with direct modification access.

ITD agrees the review of violation logs for critical ITD datasets should include activity of non-ITD personnel. ITD will develop consolidated reports to make the review process efficient and effective.

ITD agrees that changes made to production procedure programs should be independently reviewed and approved by appropriate supervisory personnel and will maintain records of reviews and approvals.

Finding #2—Contractors had unnecessary network-level access to the Comptroller's network

ITD agrees that contractors' network-level access should be restricted to only those servers and workstations to which each contractor requires access. We have initiated a project to reengineer our existing network, segmenting it with additional VLANs, and we will begin development of high-level access control lists. Given the current staffing and budgetary realities, however, we cannot commit to a specific target date at this time.

While we understand that the Office of Legislative Audits uses "untrusted contractors" as a term of art meaning that the contractors are not directly employed or controlled by the Comptroller's Office, we note that our contractors are subject to the same scrutiny and requirements as employees of the Comptroller's Office.

Finding #3—Controls over the Comptroller's Data Loss Prevention system need improvement

ITD agrees that data loss prevention (DLP) is an important part of our security program and will continue to mature its capabilities over time.

As of February 24, 2015, DLP rules were implemented to block suspected unauthorized outbound e-mails containing sensitive personally identifiable information. These rules and policies will be subject to continual analysis and incremental improvements.

As of February 24, 2015, DLP training for reviewers was completed and investigation protocols went into effect. Automated reporting has been configured, review procedures are in place, and documentation of the reviews will be maintained.

ITD is in the process of enabling the decryption of all outbound encrypted traffic sent to the DLP scanning devices, however they must be implemented in a very deliberate, controlled manner to mitigate risks to existing critical business processes, particularly during the income tax filing season. This implementation should be completed by the end of calendar year 2015.

AUDIT TEAM

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

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

Edward O. Kendall
Matthew D. Walbert
Information Systems Staff Auditors