Audit Report

Comptroller of Maryland
Information Technology Division

December 2010

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 W. 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

December 21, 2010

Senator Verna L. Jones, Co-Chair, Joint Audit Committee
Delegate Steven J. DeBoy, Sr., 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 provides computing and network resources and operates as a computer services bureau for the Comptroller of Maryland and other customer agencies.

Our audit disclosed that mainframe security software access and password 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 intrusion detection and prevention systems were not used to monitor traffic on a data line used by certain data center partners, such as financial institutions, to access the mainframe computer.

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 our audit by ITD.

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

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, the ITD develops and maintains application systems for the Comptroller of Maryland, and provides data center disaster recovery capabilities. Additionally, the ITD maintains the operating system and security software environment in which agency applications are executed.

The 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 (approximately 1,200 employees). According to the State's records, the ITD fiscal year 2010 operating budget totaled $29.4 million.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the two findings contained in our preceding audit report dated September 13, 2006. We determined that ITD satisfactorily addressed one of these findings. The remaining finding is repeated in this report.

Findings and Recommendations

Mainframe Software

Finding 1
Mainframe security software access and password controls were not adequate.

Analysis
Mainframe security software access and password controls were not adequate. Specifically, we noted the following conditions:

- Eighty-four users had unnecessary direct unlogged or logged access to many critical production programs. Accordingly, unauthorized changes to these production programs could occur, resulting in unauthorized changes to production data and, for unlogged items, these changes could go undetected.

- Fifty-two active accounts, with access to critical files, had passwords set to never expire. Of these 52 accounts, 3 were user accounts and 49 were system/application accounts, which could be used by individuals to directly log on to the system. Accordingly, if the passwords for these accounts were compromised, they could be used as long as the accounts are active. For the aforementioned 49 accounts, we noted that ITD could enable parameters to prevent such access by individual users.

- The Information Technology Division (ITD) Help Desk, which can perform password resets for users who forget their passwords, did not request sufficient information to adequately verify the legitimacy of an individual requesting a password reset. Specifically, the Help Desk only requested the name of the individual requesting the reset. As a result, individuals could fraudulently gain access to a legitimate user's account and improperly use the privileges associated with that account.

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,
b. enforce appropriate password lifetimes and restrict direct user logon with system/application accounts, and
c. request sufficient information to adequately verify the legitimacy of individuals requesting password resets.

Finding 2
Monitoring of security software reports and controls over changes to critical production procedure programs were not adequate.

Analysis
Monitoring of security software reports and controls over changes to critical production procedure programs were not adequate. Specifically, we noted the following conditions:

- Security software violation logs for critical ITD data files were reviewed only for violations by ITD employees, rather than for all violations, which would include other agency users. Additionally, security software reports of changes to userids and failed logon attempts were not reviewed. Furthermore, entries on the log of changes to security rules were not verified to ensure the propriety of the changes made, and the person who reviewed this log could change the security rules. 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 controlled. Specifically, for four of five of these changes tested, a change request form did not exist, and there was no documentation that these changes were 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. A similar condition was commented upon in our preceding audit report.

Recommendation 2
We recommend that ITD
a. review the aforementioned security software logs and reports for all users,
b. perform an independent verification of the propriety of changes to security rules, and
c. generate and retain a change request form for all changes to critical production procedure programs and retain evidence of the review and approval of these forms (repeat).

Network Security

Finding 3
The ITD internal network was not properly secured.

Analysis
The ITD internal network was not properly secured from third parties. Specifically, we noted the following conditions:

- The Comptroller of Maryland is developing a new tax system with extensive use of on-site contractors. We were advised that these contractors only required access to the new tax system's servers and to a few support systems, such as email. However, these on-site contractors had unnecessary network level access to numerous critical ITD systems.

- The ITD computer network was not effectively protected by intrusion detection and prevention system (IDPS) devices, which are used to monitor network traffic. Specifically, IDPS protection was not applied to traffic on ITD's data line used by certain data center partners, such as financial institutions, to access the mainframe computer. Although the ITD had previously purchased an IDPS device for this line, it was not installed at the time of our audit.

Recommendation 3
We recommend that ITD

a. restrict contractors' network level access to only those systems to which they require access,

b. perform a documented review and assessment to identify how IDPS coverage should be applied to its network and implement such coverage (including installing the previously-purchased IDPS device on the aforementioned data line) for all critical segments of its network.

Audit Scope, Objectives, and Methodology

We have audited the Comptroller of Maryland – Information Technology Division (ITD). Fieldwork associated with our review of the data center was conducted during the period from January 2010 to June 2010. Additionally, fieldwork associated with our audit of the network was conducted during the period from May 2010 to September 2010. 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. 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 the Comptroller's wireless connectivity. ITD's fiscal operations are audited separately as part of our audit of the ITD; the latest report that covered ITD's fiscal operations was issued on May 29, 2008. We also determined the status of the findings included in our preceding audit report on ITD dated September 13, 2006.

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 general controls and security controls over operating systems, databases, firewalls, routers, and virtual private networks. Our audit procedures included inquiries of appropriate personnel, inspection 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. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

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 audit did not disclose any significant instances 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

John T. Salmon
Director
Information Technology Division

December 21, 2010

Mr. Bruce Myers, CPA
Legislative Auditor
Department of Legislative Services
301 West Preston St., Room 1202
Baltimore, MD 21201

Dear Mr. Myers,

We are in receipt of your letter dated December 6, 2010 with the attached Legislative Auditor's report. The report covered the examination of the operations of the Information Technology Division of the Comptroller of Maryland.

We have reviewed the recommendations of the Legislative Auditor and now submit to you the actions being taken regarding the recommendations.

Mainframe Software

Finding 1 - Mainframe security software access and password controls were not adequate.

Auditor's Recommendation:

We recommend that ITD
a. restrict access to critical production programs to only those individuals requiring such access and log all such accesses,
b. enforce appropriate password lifetimes and restrict direct user logon with system/application accounts, and
c. request sufficient information to adequately verify the legitimacy of individuals requesting password resets.

Information Technology Division Response:

The Information Technology Division agrees with the auditor's recommendations.
a. ITD is working with the data owners to ensure that access to critical production programs is restricted to only those individuals requiring such access. All access to critical production programs will be logged. To be completed by December 31, 2010.
b. ITD is working with the agencies who own the Logon IDs in question to ensure that all Logon IDs capable of direct user logon have passwords that expire. To be completed by December 31, 2010.
c. A Personal Identification Number (PIN) procedure has been implemented to verify the identification of authorized individuals.

Mainframe Software

Finding 2 - Monitoring of security software reports and controls over changes to critical production procedure programs were not adequate.

Auditor's Recommendation:

We recommend that ITD
a. review the aforementioned security software logs and reports for all users,
b. perform an independent verification of the propriety of changes to security rules, and
c. generate and retain a change request form for all changes to critical production procedure programs and retain evidence of the review and approval of these forms (repeat).

Information Technology Division Response:

The Information Technology Division agrees with the auditor's recommendations.
a. The security logs are now reviewed and investigated for all users.
b. An employee who cannot make security changes has been designated to perform independent verification of the propriety of changes to security rules, and will take over this function by December 31, 2010.
c. As a result of the last audit, ITD established a procedure to ensure that all changes made to production JCL libraries by the applications development staff are subject to review and approval by appropriate supervisory personnel; however, review and approval for changes to production JCL programs made by ADC Technical Services staff and ADC Security Officers was not performed. Procedures for the ADC Technical Services staff and ADC Security Officers have been developed and implemented. The documentation will be stored for subsequent audit verification.

Network Security

Finding 3 - The ITD internal network was not properly secured.

Auditor's Recommendation:

We recommend that ITD
a. restrict contractors' network level access to only those systems to which they require access,
b. perform a documented review and assessment to identify how IDPS coverage should be applied to its network and implement such coverage (including installing the previously-purchased IDPS device on the aforementioned data line) for all critical segments of its network.

Information Technology Division Response:

The Information Technology Division agrees with the auditor's recommendations.
a. Contractors' access is restricted to only those systems to which they require access. Additional network level restrictions, as recommended, will be implemented by June 30, 2011.

b. An IDPS module has been installed and configured on the aforementioned data line. A security risk review to determine the need for additional IDPS coverage will be performed on all critical segments of the network by January 31, 2011.

Thank you for bringing these items to our attention. If our office can be of further assistance, or if there are additional concerns, please let us know.

Very Truly Yours

Linda L. Tanton
Deputy Comptroller

John T. Salmon,
Director, Information Technology Division

AUDIT TEAM

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

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

Michael K. Bliss
John C. Venturella
Information Systems Staff Auditors