Audit Report

# Department of Information Technology

November 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

November 10, 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 Department of Information Technology (DoIT) for the period beginning July 1, 2008, and ending February 8, 2009. Our audit also included the activities of the former Department of Budget and Management – Office of Information Technology, as further discussed on page 4 of this audit report. DoIT provides technical assistance, advice, and recommendations concerning information technology to the Executive Branch agencies and commissions of State government. DoIT also oversees the procurement of information technology and telecommunications services and products for these agencies and commissions.

Our audit disclosed control deficiencies over DoIT's information systems security. We noted deficiencies regarding the security controls in place over DoIT's network, as well as over the Department of Budget and Management's network, and networkMaryland (the State's high-speed data network), for which DoIT provides services. As a result, these networks could be subject to attacks, or critical services could be disrupted. In addition, DoIT did not always obtain or document its review of critical monitoring documentation for major information technology development projects.

DoIT's response 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 DoIT.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

# Table of Contents

# Background Information

## Department Creation and Agency Responsibilities

Chapter 9, Laws of Maryland 2008, effective July 1, 2008, established the Department of Information Technology (DoIT) as a principal unit of the Executive Branch. It transferred the information technology and telecommunications functions of the Executive Branch from the Department of Budget and Management (DBM) – Office of Information Technology (OIT) to DoIT. In the past, such activities were included in the scope of the DBM – Office of the Secretary audit.

DoIT is responsible for the State's information technology policies, procedures, and standards for Executive Branch agencies and commissions of State government.[1] Additionally, DoIT provides technical assistance, advice, and recommendations concerning information technology to these agencies and commissions. Furthermore, DoIT develops the Statewide Information Technology Master Plan; manages the Major Information Technology Development Project Fund (MITDP Fund); and coordinates, purchases, and manages information technology and telecommunications services to State agencies. The MITDP Fund is the fund that supports many of the State's major information technology development projects. DoIT also administers the Telecommunications Access of Maryland program, which provides telecommunications relay service for Marylanders who are deaf, hard of hearing, or speech disabled so they can communicate through TTY (text telephone) with others using a standard phone; this program is supported by the Universal Service Trust Fund. According to the State's records, DoIT's expenditures totaled approximately $40 million during fiscal year 2009.

The most recent audit report on DBM – Office of the Secretary was dated April 21, 2009 and covered the period beginning September 1, 2005 and ending September 30, 2008; that audit excluded the activities transferred to DoIT. Consequently, the scope of this audit included the activities of the former DBM – Office of Information Technology beginning September 1, 2005 and ending June 30, 2008 when those functions were transferred to the newly created DoIT. This audit also included the activities of DoIT since its creation through February 8, 2009.

[1] According to State law, DoIT does not have authority or responsibilities related to the University System of Maryland, Morgan State University, St. Mary's College, the Maryland Judiciary, or the Legislative Branch.

## Maryland Funding Accountability and Transparency Act of 2008

Chapter 659, Laws of Maryland 2008, effective July 1, 2008, required that a searchable website be designed and operated to provide information on State funding to the public at no cost. Beginning with fiscal year 2008, the website, which, by law is operated by DoIT, lists the names of payees of the State who received, in the aggregate, monies greater than $25,000 in a fiscal year; the website also includes the locale of the payees, the amounts of individual payments, and the names of the State agencies making the payments. Payees do not include State employees or retirees. Additionally, consistent with informal advice DoIT obtained from the Office of the Attorney General, the website does not include operating payments made by the University System of Maryland, Morgan State University, and St. Mary's College. Additionally, the website does not include payments made by the Maryland Judiciary and the Legislative Branch. During our review, we noted that the website did not include a disclaimer reflecting these limitations; based on our inquiries, DoIT management advised us that these limitations would be disclosed on the website in the near future.

## Telecommunication Settlement Agreements

During fiscal years 2006 and 2007, the former DBM – OIT entered into settlement agreements or recovered overbillings totaling approximately $11.6 million from four vendors providing telecommunication services. Specifically, the former DBM - OIT contracted with a private consulting firm to perform seven audits of various telecommunication services (such as wireless, long-distance, local access). These audits encompassed the periods of the related telecommunication service contracts. The dates of services covered by the aforementioned audits ranged from December 1996 to December 2006. In addition, current ongoing audits have identified potential refunds totaling $6 million due to the State.

In several prior audit reports, we commented that the State's telecommunication vendors' invoices had not been audited since 1991, and, in the preceding report, that refunds had not been received on a timely basis. The former DBM – OIT contracted for such audits beginning in November 2001.

## Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the eight findings from our preceding audit report on DBM – Office the Secretary, dated August 30, 2006, which related to the Office of Information Technology. Furthermore, our audit

included a review to determine the status of one finding from our preceding audit report on the Executive Department – Governor dated, October 5, 2007, since DoIT performs the information technology support services for the Governor's Office. We determined that DoIT had satisfactorily resolved all of these nine findings.

# Findings and Recommendations

## Information Systems Security and Control

The Department of Information Technology (DoIT) provides services on a statewide level to numerous State and other governmental agencies (such as local governments). For example, DoIT manages the development and operations of the State's high-speed data network known as networkMaryland. In addition, DoIT provides its own information technology services and support, as well as for the Department of Budget and Management (DBM) and the Executive Department – Governor (Governor's Office). Our audit of DoIT included a review of the security controls over DoIT's statewide responsibilities and agency-specific responsibilities. Key network resources include systems that support many Statewide functions, such as major information technology projects, the State's personnel system, the State's fleet management, and the State's capital budgeting, as well as agency email systems, and websites.

**Finding 1**
**Firewalls did not adequately secure the DoIT, DBM, Governor's Office, and networkMaryland networks, and the Governor's Office network was not adequately protected by intrusion detection and prevention system software.**

**Analysis**
Firewalls did not adequately secure the DoIT, DBM, Governor's Office, and networkMaryland networks, and the Governor's Office network was not adequately protected by intrusion detection and prevention system software. Specifically, we noted the following conditions:

- Although firewalls were installed to protect the DoIT, DBM, and Governor's Office networks, deficiencies in the firewall configurations allowed unnecessary and insecure connections to network devices in the internal networks. The firewall rules were not configured to adequately secure connections to these networks from the Internet, networkMaryland, and other untrusted sources. Therefore, critical network devices for certain applications were susceptible to attacks, which could result in a loss of data integrity or the interruption of critical network services.

- Similarly, the firewalls installed to protect the networkMaryland management systems local area network in Baltimore, which served as an operations center, allowed certain unnecessary and insecure connections to network management servers and other critical devices. The firewall rules were not

configured to adequately secure these network management servers and other devices from untrusted sources, including non-administrative networkMaryland users and devices. Therefore, critical networkMaryland management servers and devices were susceptible to attacks, which could result in the interruption of critical network services.

- Intrusion detection and prevention systems were not properly utilized on the Governor's Office network to protect critical portions of the network. Specifically, while the network included both intrusion detection and prevention systems, their configurations did not help protect the internal network from threats originating from untrusted network sources, including the Internet and other State agencies. Also, the intrusion detection software had not been updated with the most current vendor software releases. Intrusion detection and prevention systems gather and analyze network traffic to identify and help prevent network security breaches and attacks, and alert network administrators of these situations.

**Recommendation 1**
**We recommend that DoIT**

**a. configure the aforementioned firewalls to adequately secure the DoIT, DBM, Governor's Office, and networkMaryland networks; and**

**b. configure the Governor's Office intrusion detection and prevention systems to provide coverage of all critical Governor's Office network devices, and maintain these systems at the most current vendor software releases.**

**Finding 2**
**Critical DoIT and DBM systems were accessible, at the network level, by the majority of the other department's users.**

**Analysis**
Critical DoIT and DBM systems were not adequately segmented on the local area network (LAN) shared by DoIT and DBM. From a network perspective, the shared DoIT/DBM LAN was not modified after the creation of DoIT in July 2008, which resulted in the two departments sharing one LAN. As a result, each department's critical systems were accessible, at the network level, to the majority of the other department's users. Accordingly, each department's users had unnecessary network level access to the other department's critical systems. DoIT and DBM employees utilize critical systems and servers such as the networkMaryland management servers.

**Recommendation 2**
**We recommend that DoIT restrict access, at the network level, to critical DoIT and DBM systems, to only those users requiring access to the systems.**

## Major Information Technology Development Projects

**Finding 3**
**DoIT did not always obtain or document its review of critical monitoring documentation for major information technology development projects, as required by its policy.**

**Analysis**
The existence and/or review of critical monitoring documentation was inadequate for major information technology development projects (MITDP) overseen by DoIT and financed by the Major Information Technology Development Project (MITDP) Fund. These projects are generally large IT projects, with significant impact on State operations, within Executive Branch agencies and commissions. Specifically, our review disclosed the following conditions:

- We tested five projects, for which DoIT approved MITDP Fund disbursements during fiscal years 2006 to 2008 totaling approximately $23.1 million. For three projects, with approved disbursements totaling approximately $14.2 million during fiscal years 2006 to 2008, although DoIT stated it reviewed certain critical system development life cycle documents, this review was not documented, and DoIT management could not provide us with all required documents. For example, for one project with approved disbursements totaling approximately $1.6 million, DoIT could not provide the project's management plan. The management plan includes components related to acquisition planning, quality assurance planning, and concept of operations. System development life cycle documents, which are required for all MITDPs, promote the development of safe, secure, and reliable systems in order to ensure information technology projects are successfully planned and executed.

- Although it was DoIT's policy to conduct quarterly reviews of project monitoring documents and costs schedules, this review process was not always formally documented. Documents subject to review address the status of each project's ongoing scope, schedule, budget, expenditures, and risks.

- DoIT did not always ensure that an independent verification and validation assessment was conducted for each project. Specifically, according to DoIT's records, as of June 30, 2009, such assessments were not conducted for 29 of the 36 projects eligible for an assessment (for example, active projects not in the operation or maintenance phase). These independent third party assessments determine the status of the project and identify areas for project improvement. DoIT requires projects to annually budget for an assessment during the project's development. Furthermore, per DoIT's fiscal year 2009 information technology project request guidelines and instructions, such assessments are required for each MITDP. We were informed by DoIT that, due to budget constraints, the funding for these assessments is sometimes subject to budgetary reductions.

During fiscal year 2008, there were 44 MITDPs involving 15 State agencies in which DoIT approved funds totaling approximately $11.5 million from the MITDP Fund.

**Recommendation 3**
**We recommend that DoIT**

**a. obtain and review system development life cycle documentation;**

**b. document its review of quarterly project monitoring documents and cost schedules, and system development life cycle documents; and**

**c. ensure annual independent verification and validation assessments for all projects are performed or document the reason for assessments that are not performed.**

# Audit Scope, Objectives, and Methodology

We have audited the Department of Information Technology (DoIT) for the period beginning September 1, 2005, and ending February 8, 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.

DoIT was created by law, effective July 1, 2008, as a principal unit of the Executive Branch, and is responsible for the information technology and telecommunication functions of the Executive Branch. Previously, the Department of Budget and Management (DBM) — Office of Information Technology was responsible for these activities. The scope of this audit included the activities of the former DBM—Office of Information Technology beginning September 1, 2005 and ending June 30, 2008 when those functions were transferred to the newly created DoIT. This audit also included the activities of DoIT since its creation through February 8, 2009.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine DoIT's financial transactions, records and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations. The areas addressed by the audit included monitoring of DoIT's statewide information technology contracts, the administration of the Universal Service Trust Fund and the Major Information Technology Development Project Fund, and information systems security and controls. We also determined the status of the findings included in our preceding audit report of the Department of Budget and Management – Office the Secretary (with respect to the Office of Information Technology), dated August 30, 2006. In addition, we determine the status of one finding from our preceding audit report of the Executive Department – Governor, dated October 5, 2007.

In planning and conducting our audit, we focused on the major financial-related 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 DoIT 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.

Our audit did not include certain support services provided to DoIT. These support services (such as payroll and maintenance of certain accounting records) are included within the scope of our audit of the Department of Budget and Management.

DoIT'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 related to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect DoIT's 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 DoIT that did not warrant inclusion in this report.

DoIT's response 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 DoIT regarding the results of our review of its response.

# APPENDIX

doit

STATE OF MARYLAND
DEPARTMENT OF INFORMATION TECHNOLOGY

*MARTIN O'MALLEY*
Governor
*ANTHONY BROWN*
Lieutenant Governor

*ELLIOT SCHLANGER*
Secretary

November 9, 2009

Mr. Bruce A. Myers, Legislative Auditor
State of Maryland
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, MD 21201

Dear Mr. Myers:

The Department of Information Technology (DoIT) has reviewed your draft audit report for the period beginning September 1, 2005, and ending February 8, 2009. As requested, our responses to the findings in the report are attached.

If you have any questions or need additional information, you may contact me at 410-260-2994 or Elliot.Schlanger@doit.state.md.us.

11/09/2009

Elliot Schlanger, Date
Secretary

cc: Mr. Douglas Carrey-Beaver, Principal Counsel
Ms. Wendy Brickus, Assistant Attorney General
Ms. Stacia Cropper, Deputy State CIO, Administration
Mr. Charles Ihrie, Compliance Auditor, Department of Budget and Management (DBM)
Ms. Joan Peacock, Manager, Audit Compliance Unit, DBM
Mr. Michael Eismeier, Director, Policy and Planning Division

# Department of Information Technology (DoIT)
# Response to Legislative Audit Findings and Recommendations
# Audit Period: September 1, 2005, and ending February 8, 2009

## Information Systems Security and Control

**Finding 1**
**Firewalls did not adequately secure the DoIT, DBM, Governor's Office, and networkMaryland networks, and the Governor's Office network was not adequately protected by intrusion detection and prevention system software.**

**Recommendation 1**
**We recommend that DoIT**

**a. configure the aforementioned firewalls to adequately secure the DoIT, DBM, Governor's Office, and networkMaryland networks; and**

**b. configure the Governor's Office intrusion detection and prevention systems to provide coverage of all critical Governor's Office network devices, and maintain these systems at the most current vendor software releases.**

DoIT Response: Agree

DoIT has implemented updated firewall policies and made the appropriate configurations, addressing the specifics of the audit finding. Also, DoIT has performed the configuration changes to the Governor's Office intrusion detection and prevention systems, addressing the coverage areas detailed in the audit finding.

**Finding 2**
**Critical DoIT and DBM systems were accessible, at the network level, by the majority of the other department's users.**

**Recommendation 2**
**We recommend that DoIT restrict access, at the network level, to critical DoIT and DBM systems, to only those users requiring access to the systems.**

DoIT Response: Agree

DoIT has restricted access to systems and network resources based on user login credentials since DoIT was officially created on July 1, 2008. Although this access restriction has been sufficient to protect against internal security breaches, DoIT will split the two departmental networks to further segregate the

two networks and their various assets. Until the physical split of the two networks occurs, the two will be secured in the same manner as has protected the entities since DoIT was created.

Due to intense budget constraints, DoIT will not be able to purchase additional equipment, if it is determined it is needed, no earlier than FY 2012 given current projections. Between now and that time, DoIT will plan and develop the procedures for the migration and produce the typical technical planning documents required for this task.

## Major Information Technology Development Projects

**Finding 3**
**DoIT did not always obtain or document its review of critical monitoring documentation for major information technology development projects, as required by its policy.**

**Recommendation 3**
**We recommend that DoIT**

**a. obtain and review system development life cycle documentation;**
**b. document its review of quarterly project monitoring documents and cost schedules, and system development life cycle documents; and**
**c. ensure annual independent verification and validation assessments for all projects are performed or document the reason for assessments that are not performed.**

DoIT Response: Partially Agree

DoIT did not obtain certain project artifacts, due to the fact that the beginning of two of the projects tested preceded the requirement for agencies to submit all system development life cycle (SDLC) documents to DoIT. Likewise, although DoIT does periodically review certain SDLC documents, those documents are not always kept on file after they have been reviewed and discussed with the agency. Most SDLC documents are living documents and therefore updated frequently. DoIT oversight does not benefit from trying to track and store the various versions reviewed as part of oversight. Regarding documentation associated with its oversight, DoIT often reviews and discusses SDLC documents orally with the agency project teams when conducting project review sessions and does not always record the comments associated with the documents referenced during the meeting.

With regard to recommendation a., DoIT will continue its current process of collaborating with agencies to review various required SDLC documents at least quarterly, as part of its oversight responsibility. It has not been, nor will it become, DoIT's intention to collect and maintain SDLC documents for all of the projects in the Portfolio. SDLC artifacts are living documents that should, if used properly, change frequently. Furthermore, there can be literally dozens of documents with dozens of iterations over the life of a project. These documents represent the agencies' project management data and tools, subject to

DoIT's periodic inspection, review and analysis. No value would be garnered in DoIT becoming a repository for these documents.

For recommendation b., DoIT has begun more formally documenting all project monitoring activities including quarterly project updates and SDLC document reviews.

With regard to IV&Vs in recommendation c, DoIT began requesting funding in FY 2008 for each MITDP expected to still be active, but not yet in the Operations and Maintenance phase. This same process of requesting IV&V funds for all projects expected to be in implementation during the next fiscal year has continued during the budget planning processes for FY 2009 and FY 2010. The same protocol will continue in FY 2011 and beyond. Due to various internal iterations of budget approvals and reductions, IV&V funding is susceptible to being cut before making the Governor's Allowance stage, where it is then subject to further cuts from the General Assembly.

## AUDIT TEAM

**Matthew L. Streett, CPA, CFE**
Audit Manager

**Stephen P. Jersey, CPA, CISA**
Information Systems Audit Manager

**Terry S. Gibson**
Senior Auditor

**R. Brendan Coffey, CPA**
Information Systems Senior Auditor

**Carey L. Harper**
**David O. Mauriello**
Staff Auditors

**Michael K. Bliss**
Information Systems Staff Auditor