Audit Report

Department of Information Technology

August 2013

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

Thomas J. Barnickel III, CPA
Legislative Auditor

August 1, 2013

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 Department of Information Technology (DoIT) for the period beginning February 9, 2009 and ending February 8, 2012. DoIT provides technical assistance, advice, and recommendations concerning information technology (IT) to the Executive Branch agencies and commissions of State government. DoIT also oversees the procurement of IT and telecommunications services and products for these agencies and commissions, and manages the State's IT network.

Our audit disclosed certain deficiencies in DoIT's contract management and oversight of the One Maryland Broadband Network (OMBN), a construction project creating a statewide fiber optics network linking government and private broadband networks. The total budgeted cost for the project was $158.4 million with $115.2 million to be obtained from a federal grant. Specifically, DoIT did not timely execute a comprehensive task order modification for the addition of OMBN project management services to the scope of an existing task order that increased the value by $11.8 million. Additionally, controls were not adequate over DoIT's approval and monitoring of certain OMBN engineering and construction services and the related payments. Furthermore, DoIT had not established a process to adequately monitor the expenditure of funds it provided to a grant sub-recipient that was responsible for a significant portion of the OMBN project.

Our audit also disclosed issues related to the procurement of statewide information technology contracts. Specifically, DoIT did not ensure that State agencies' complied with State regulations and DoIT policy requiring a minimum number of days for the receipt of competitive bids when procuring certain IT

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

services and did not have safeguards in place to secure electronic bids for DoIT's own procurement of such contracts. Additionally, DoIT did not ensure that required monitoring of major information technology development projects was documented.

Our audit disclosed control deficiencies over DoIT's information systems security. Specifically, controls did not exist to ensure that information placed on a file storage service was appropriate or adequately secured. In addition, backup copies of several critical network devices did not exist.

An Executive Summary of our findings can be found on page 5. DoIT's response 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,

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

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

Executive Summary

Legislative Audit Report on the
Department of Information Technology (DoIT)
August 2013

- **DoIT did not execute a task order modification for the One Maryland Broadband Network (OMBN) project management responsibilities with an estimated cost of $11.8 million until approximately 20 months after deciding to use an existing contractor. The modification did not include certain provisions to help protect the State.**

  DoIT should evaluate its arrangement with the project management contractor to ensure the contractor's responsibilities are adequately defined and the State's investment is adequately protected. In the future, DoIT should ensure the timely execution of comprehensive task order modifications.

- **Controls were not adequate to ensure that payments for certain OMBN engineering and construction services were properly approved and supported. Additionally, expenditures by a consortium of local jurisdictions related to $71.5 million in funding provided by DoIT from a federal grant for OMBN construction were not adequately monitored.**

  DoIT should ensure that payments are properly approved and supported by appropriate documentation. Additionally, DoIT should ensure that payments are approved by appropriate personnel and comply with contract provisions. Finally, DoIT should establish procedures to monitor its grant sub-recipients.

- **DoIT did not ensure compliance with its established policy regarding the minimum time period for soliciting competitive bidding by State agencies and DoIT under statewide computer master contracts. Furthermore, DoIT did not adequately secure bids received electronically for its procurements of statewide information technology contracts.**

  DoIT should allow a competitive bid period for a minimum of 20 days as required by its policy and establish procedures to properly restrict access to competitive sealed bid proposals received electronically prior to the due date.

- **DoIT did not always document its monitoring of major information technology development projects, such as maintaining documentation substantiating its performance of quarterly portfolio reviews of each project's scope, schedule, budget, expenditures, and risks.**

  DoIT should document its project monitoring for major information technology development projects.

- **DoIT did not have controls to ensure that State agency information placed on a vendor's file storage, cloud-based system by State agencies was appropriate or adequately secured.**

  DoIT should assess the security control issues and develop appropriate solutions to protect against improper data disclosure or modification.

- **DoIT did not maintain offsite backup files of several critical *network*Maryland devices and did not have an up-to-date disaster recovery plan.**

  DoIT should store backup files of critical network device configurations at an offsite, secure, and environmentally controlled location. DoIT should also maintain a complete and comprehensive disaster recovery plan which is updated at least annually.

Background Information

Agency Responsibilities

The Department of Information Technology (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 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, during fiscal year 2012 DoIT's expenditures totaled approximately $96 million, which included approximately $46 million for the One Maryland Broadband Network (OMBN) capital project. The OMBN is a construction project to create a statewide fiber optics network by providing additional fiber optic lines that will link government and private broadband networks. The OMBN project is expected to be completed by August 2013 and has an estimated cost totaling approximately $158.4 million, of which approximately $115.2 million is funded by a federal American Recovery and Reinvestment Act grant.

Telecommunication Settlement Agreements

DoIT is currently in various stages of legal proceedings with certain telecommunication vendors to resolve overbillings identified through five audits of these vendors. For example, three audits resulted in claims totaling approximately $18.6 million. As of June 2012, the claims were under review by

[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.

the Maryland Board of Contract Appeals, and DoIT could not provide a reasonable estimate for when the legal proceedings would be finalized due to the probability of appeals or how much of these claims could be recovered from the vendors.

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 November 10, 2009. We determined that DoIT satisfactorily resolved two of these findings; the remaining finding is repeated in this report. Our audit also included a review to determine the status of one of the four findings contained in our preceding audit report, dated April 21, 2009, on the Department of Budget and Management – Office of the Secretary and Other Units since it pertained to DoIT prior to DoIT becoming a separate State agency in July 2008. We determined that DoIT satisfactorily addressed this finding which related to the improper retention of excess funds obtained from State agencies for the reimbursement of telecommunication costs.

Findings and Recommendations

One Maryland Broadband Network

Background

The One Maryland Broadband Network (OMBN) is a construction project to create a statewide fiber optics network by providing additional fiber optic lines that will link existing government and private broadband networks. The total approved project budget is approximately $158.4 million, of which approximately $115.2 million is to be funded by a federal American Recovery and Reinvestment Act grant awarded to the Department of Information Technology (DoIT) in September 2010. The grant requires that the $43.2 million difference between the approved project cost and the federal grant be funded with matching funds from State and local jurisdictions.

The goal of the completed project is to have a network that will connect lines to over 1,000 "community anchor institutions" (such as, schools, libraries, hospitals, and public safety agencies) by adding more than 1,300 miles of fiber optic cable lines to existing networks in all 24 Maryland jurisdictions. This goal will be achieved by expanding *network*Maryland (a State-owned statewide high-speed network for public sector use) and connecting it to the following other independent networks:

- the Inter-County Broadband Network (ICBN), a collaborative inter-governmental consortium consisting of eight counties and one city;

- the Maryland Broadband Cooperative network (MdBC), a member-owned and operated universal access, fiber optic network designed to deliver broadband network across the rural communities in Eastern, Southern, and Western Maryland;

- the Mid-Atlantic Crossroads, which designs and deploys a high performance networking infrastructure to universities, federal agencies, government laboratories, and non-profit institutions in Maryland, the District of Columbia, and Northern Virginia; and

- the Maryland Research and Education Network, which connects the many segments involved in Maryland education including the University System of Maryland members, other Maryland public and private universities, community colleges, and kindergarten through grade 12 local education agency institutions and provides connections to the Internet and the national research network "Internet2" using its own fiber core infrastructure.

As the recipient, DoIT is responsible for administering the federal grant and for overseeing the OMBN project, including monitoring grant sub-recipients (ICBN, MdBC, and one county) and ensuring that all fiscal, compliance, and programmatic responsibilities are fulfilled. To accomplish these responsibilities, DoIT relies on a project management contractor (PMC) to manage many aspects of the OMBN project.

Based on grant and DoIT financial records the $115.2 million in grant funds was awarded or allocated as follows:

- $71.5 million to one county government on behalf of, and representing, the ICBN,
- $700,000 to one other county government upon its withdrawal from ICBN in March 2012,
- $3.4 million to MdBC to primarily provide equipment for the project, and
- $39.6 million to DoIT for managing the project and providing construction in the remaining 15 jurisdictions.

According to the federal grant, DoIT has until August 31, 2013 to complete the project or the State is at risk of losing federal funds. DoIT currently anticipates that the project will be completed on schedule by August 31, 2013. The project's progress as of December 31, 2012 was as follows:

One Maryland Broadband Network Project Status as of December 31, 2012

Project Status Category	Budgeted/ Planned Amount	Actual Amount to Date	Percentage of Budgeted/ Planned Amount
Total Project Costs	$158.4 million	$115 million	72.6%
Fiber Mile Installations	1,368 miles	999 miles	73.0%
Community Anchor Institution Connections	1,006	294	29.2%

Source: DoIT's Federal Grant Report for the Fourth Quarter of 2012

Finding 1
DoIT used an existing information technology contractor for project management services related to the OMBN project without the timely execution of a comprehensive task order modification.

Analysis

DoIT used an existing contractor to provide project management services for the OMBN project, without the timely execution of a comprehensive task order modification. Specifically, DoIT did not execute a task order modification covering the scope of the work to be performed and the estimated costs until approximately 20 months after deciding to use the contractor as the project management contractor (PMC). Furthermore, the modified task order did not contain provisions regarding liability for cost overruns or for not meeting project deadlines.

Although DoIT decided in September 2010 to use its existing network*Maryland* contractor as the PMC at an estimated cost of $11.8 million, DoIT did not obtain any formal documents regarding extending the original task until it requested, based on our inquiry, certain information from the PMC. In this regard, in a May 23, 2012 letter, the PMC accepted its management role for the OMBN project and stated its recognition that the OMBN project had a completion date of August 31, 2013 and committed to providing the necessary management and engineering resources to ensure the State met the project deadline. The letter also confirmed the $11.8 million cost to provide the PMC services (based on estimated hours and existing contract rates) and a planned start date in September 2010. On June 28, 2012, DoIT executed a task order agreement modification to increase the maximum value of the original task order contract to $29.1 million to cover the additional PMC responsibilities for the OMBN project and additional tasks related to *network*Maryland. However, the modification did not include provisions providing for legal recourse if the OMBN project was not completed as required.

The timely execution of a comprehensive task order modification would help ensure that senior management's intentions with respect to work scope and costs were established. However, we identified a billing practice that had been arranged with the PMC for certain work performed on the OMBN without being documented in a task order modification or without the knowledge of DoIT senior management. Specifically, a DoIT management employee and the PMC verbally agreed to increase the cost of subcontracted services by eight percent, although there was no formal authorization for this increase. Beginning in July 2011, this markup fee was invoiced by the PMC to DoIT for subcontracted engineering services (including services that in some cases were performed by companies

affiliated with the PMC) in order to compensate the PMC for monitoring the work of the subcontractors. DoIT senior management was not aware of this verbal agreement until we brought the matter to its attention. DoIT management agreed that DoIT generally does not permit such arrangements and, as of March 2013, it was working with the PMC to resolve the markup fee issue under the advice of its legal counsel. According to DoIT's records, as of July 2012, the value of the eight percent markup fee totaled approximately $102,600 and was included in payments for subcontracted OMBN engineering work totaling approximately $1.4 million.

The PMC is directly responsible for project management and engineering work related to the 15 jurisdictions under direct DoIT responsibility and assists DoIT in overseeing the entire OMBN project statewide. DoIT's original $11.4 million task order with this contractor was awarded in February 2010. It required the contractor to provide management, operations, and maintenance support of the State-owned *network*Maryland, as well as hosting responsibilities for the State's official website. We were advised by DoIT that its September 2010 decision to use this contractor for the OMBN project was based in part on the contractor's responsibilities for *network*Maryland and its assistance to DoIT in applying for the federal grant for the OMBN project. Board of Public Works (BPW) approval was not necessary for the addition of the OMBN project work to the original *network*Maryland contract since it was procured under the statewide Consulting and Technical Services (CATS) contract, which was subject to BPW approval. In accordance with State procurement regulations, CATS task orders, which are required to be issued to preapproved contractors via competitive proposal procedures, and any modifications do not require BPW approval.

During the period of July 27, 2010 to May 1, 2012, DoIT paid approximately $8.5 million to the contractor, including $3.4 million for PMC responsibilities on the OMBN project.

Recommendation 1
We recommend that DoIT

a. evaluate its arrangement with the PMC to ensure that the contractor's responsibilities are adequately delineated and that the State's investment in the OMBN project is adequately protected against additional costs in the event the project is not completed timely and properly;
b. ensure the aforementioned billing issue is appropriately resolved; and
c. in the future, ensure task order modifications are timely executed and contain appropriate terms and conditions.

Finding 2
Controls were not adequate over the approval and monitoring of certain OMBN engineering and construction services and the related payments.

Analysis
Controls were not adequate over the approval and monitoring of engineering and construction services and the related payments for the work performed on the OMBN project in the 15 jurisdictions under DoIT's direct responsibility. According to DoIT's records as of July 2012, the budget for engineering and construction services totaled approximately $45.4 million and the related payments totaled approximately $15 million. We noted the following:

- Work orders authorizing the commencement of agreed-upon engineering and construction work under the PMC's management were not signed by either DoIT or PMC management personnel. We were advised that DoIT and the PMC meet frequently to discuss the scheduling of work on the multiple segments of the project in each jurisdiction. When work is ready to proceed, the scope and cost is detailed in a written work order. Without signatures on the work orders, there is a lack of assurance that both parties had reached an agreement on the work scope and cost.

- DoIT did not always obtain required documentation to verify the accuracy of engineering and construction services invoices. Our test of seven construction services payments totaling approximately $2.8 million disclosed that DoIT did not obtain a milestone acceptance form, which documents the PMC's inspection and progress of the construction work, for five payments totaling approximately $2.2 million. To support project progress and invoice costs, DoIT requires the submission of critical documentation such as the milestone acceptance form, which is to be signed by applicable DoIT and/or PMC personnel.

- The responsibilities for the selection of contractors to perform construction services and for the final approval of the related invoices for payment were not properly separated. Specifically, for each project segment authorized by a work order for construction, one DoIT employee was responsible for requesting, receiving, evaluating, and selecting contractors from a pool of contractors that had been previously pre-approved by DoIT as qualified to work on the OMBN. This employee was also responsible for reviewing and approving the related invoices for payment. Consequently, this employee had almost unlimited control over the process, which increased the risk that contractor selection and payment improprieties could occur and remain undetected.

Recommendation 2
We recommend that DoIT

a. ensure all work orders are signed by appropriate DoIT and PMC management personnel,

b. ensure proper supporting documentation for monitoring the progress of engineering and construction services work is obtained and reviewed prior to approving the invoices for payment, and

c. separate the responsibility for selecting the contractors to perform construction services from the responsibility for reviewing and approving the related invoices for payment. We advised DoIT on accomplishing the necessary separation of duties using existing personnel.

Finding 3
DoIT did not adequately monitor one grant sub-recipient that was responsible for a significant portion of the OMBN project.

Analysis
DoIT did not adequately monitor the Inter-County Broadband Network (ICBN) portion of the OMBN project. According to its *Sub-recipient Manual*, DoIT's monitoring of sub-recipients should be documented and accomplished through office-based and on-site monitoring. Specifically, we noted the following:

- DoIT did not document its review of invoices supporting ICBN expenditures submitted to DoIT for federal fund reimbursement to ensure the invoice costs were proper and conformed to contract requirements. We were advised that, prior to February 2012, DoIT's invoice review process consisted of determining that each invoice related to the ICBN project without verifying compliance with related contract provisions. Also, we were advised that the review ensured that an ICBN employee approved the invoice for payment. However, our test of 10 ICBN invoices totaling approximately $1.8 million disclosed that 3 invoices totaling approximately $700,000 were not approved by an ICBN employee. We were advised that DoIT implemented a procedure effective in February 2012 requiring a documented review of the ICBN expenditures to ensure their propriety.

- During the audit period, DoIT employees had not conducted any documented site visits to independently verify the completion of ICBN work performed as reported by its PMC.

- DoIT had not made arrangements with the ICBN to schedule an independent audit or agreed-upon procedures review to ensure that federal funds were only used for authorized purposes in accordance with federal grant requirements. Such an audit or review is required by DoIT's *Sub-recipient Manual*.

As of March 31, 2012, according to DoIT's records, of the $71.5 million allocated from the federal OMBN grant to ICBN, DoIT had transferred federal funds totaling approximately $20 million to the ICBN as reimbursement for its OMBN-related expenditures. Approximately $17 million of the funds were transferred to ICBN prior to the implementation of the aforementioned documented review procedure implemented by DoIT in February 2012.

Recommendation 3
We recommend that DoIT monitor its sub-recipients in accordance with the aforementioned *Manual* by

a. documenting its review of ICBN invoices and ensuring that the invoice costs were proper and were approved by ICBN personnel, and that such costs conform to contract requirements;
b. conducting periodic on-site visits to independently verify the completion of work performed as reported; and
c. ensuring that an independent audit or review is conducted of the ICBN expenditures to ensure that federal funds were only used for authorized purposes in accordance with federal grant requirements.

Statewide Contract Procurements

Finding 4
DoIT did not ensure compliance with its established policy regarding the minimum time period for competitive bidding and did not adequately secure bids received electronically.

Analysis
DoIT did not ensure compliance with its established policy regarding the minimum time period for soliciting competitive bidding by State agencies and DoIT. Additionally, DoIT did not adequately secure bids it received electronically when procuring statewide contracts.

- DoIT approved State agency procurements under its statewide computer software and hardware master contracts without ensuring compliance with the minimum time period established for competitive bidding from eligible contractors. Our test of 14 procurements totaling approximately $11 million

disclosed that, for 13 procurements totaling approximately $10 million (including 3 procurements by DoIT itself totaling approximately $1.7 million), the competitive bidding time period established by agencies ranged from 2 to 10 days, which is under the 20-day minimum established by policy. For example, a procurement totaling approximately $1.8 million had a competitive bidding time period of 6 days in which only 3 bids were received from 21 eligible contractors. The limited bidding period could have resulted in a lack of competition from eligible contractors and not obtaining the best value for the State.

- For Statewide contracts that it procured, DoIT did not secure competitive bids received electronically via email prior to the bid due date, as required. As directed by the related request for proposals, vendors routinely sent competitive sealed bid proposals for statewide contracts directly to either a DoIT employee's work email account or a group email account designated to receive such proposals. These bid proposal files were not password protected and access to open emails sent to the group account was not properly restricted prior to the bid due date. We were advised that at least three employees had access to the group email account. Our test of eight statewide contract awards totaling approximately $57 million related to computer service, software, and/or hardware services disclosed that the emailed competitive bid proposals for all eight contract awards were not properly secured. Consequently, there is a risk that confidential competitive bid information could be accessed and disclosed without detection to other prospective bidders prior to the bid due date.

According to DoIT's policy, State agency procurements from DoIT's statewide computer software and hardware master contracts are required to be in accordance the competitive sealed proposals process under State procurement regulations. These regulations require a minimum 20-day competitive bidding time period. Additionally, State procurement regulations require that competitive sealed bid proposals be secured until the established bid due date.

Recommendation 4
We recommend that DoIT

a. ensure compliance with its established policy regarding a competitive bid period for a minimum of 20 days as referenced in State procurement regulations, and

b. establish procedures to properly restrict access to competitive sealed bid proposals received electronically.

Major Information Technology Development Project Fund

Finding 5
DoIT could not provide certain documentation of its monitoring of major information technology development projects.

Analysis
DoIT could not provide certain documentation to substantiate that it actively monitored the status of the major information technology development projects (MITDP) it oversees. These are generally large IT projects typically financed by the MITDP Fund, with significant impact on State operations within Executive Branch agencies and commissions.

Our test of five projects, with approved MITDP Fund disbursements totaling approximately $43 million during fiscal years 2009 to 2012, disclosed that DoIT could not provide sufficient evidence of its project monitoring efforts. Although DoIT advised us that it conducted quarterly portfolio reviews in fiscal year 2011 for each project tested (a total of 20 reviews), DoIT was only able to provide documentation for the results of 2 reviews. For the remaining 18 reviews, DoIT was only able to demonstrate that the reviews were scheduled with the agency, and in some instances, meeting attendance sheets were maintained. Documentation of the project matters discussed at those meetings was not maintained. DoIT policy requires quarterly portfolio reviews of each major project that address the status of each project's ongoing scope, schedule, budget, expenditures, and risks. A similar condition was commented upon in our preceding audit report.

In addition, for two of the five projects with disbursements totaling $12.5 million, an independent verification and validation assessment (IV&V) was conducted to determine the status of the project and identify areas for improvement. However, DoIT could not provide documentation supporting how the related recommendations for improvement identified in the IV&V were addressed. Prior to fiscal year 2012, an IV&V was required for each project. Subsequently, such assessments are performed at DoIT's discretion.

During fiscal year 2012, there were 41 MITDPs involving 13 State agencies with DoIT approved funds totaling approximately $23.8 million from the MITDP Fund. MITDP Fund disbursements during fiscal year 2009 to 2012 totaled approximately $64.5 million.

Recommendation 5
We recommend that DoIT document its project monitoring for the major information technology development projects it oversees (repeat).

Cloud Messaging and Collaboration Services

Background

During September 2011, DoIT entered into a contract for cloud messaging and collaboration services for State of Maryland agencies. The contract term was for five years, with a not to exceed price of $18,719,250.

The contractor provides a cloud based software platform that is used by numerous State of Maryland agencies for electronic messaging services, collaborative tools, and support. DoIT maintains and administers these services for the State of Maryland in a Maryland.gov domain, and assists agencies that migrate their existing email service to the Maryland.gov domain's cloud messaging service.

According to DoIT schedules, state agencies are adopting the cloud messaging and collaboration services on a gradual basis. As of April 26, 2012, there were 885 state agency employees utilizing the cloud messaging services. The Maryland.gov domain is divided into sub-organizations (one for each state agency) that participate in the cloud messaging and collaboration services. The individual software services provided though the cloud services can be enabled or disabled for each participating State agency. One core collaboration service that DoIT has enabled for all participating state agencies provides a single place to store, create, access, edit, and share documents, files, and folders of all types.

Finding 6
Controls did not exist to ensure that information placed on the file storage service was appropriate or adequately secured.

Analysis

Controls did not exist to ensure that information placed on the file storage service was appropriate or adequately secured. Specifically, we noted the following control issues associated with the DoIT rollout and implementation of the file storage service:

- File owners (State employees who saved files on the file storage service) had virtually unrestricted ability to share files and set access permissions on these files.

- File owners could designate editors (that is, any other individual with a cloud messaging account, including those outside of State government) who had virtually unrestricted ability to share the file owner's files and set access permissions on these files.

- There was no electronic enforcement of what data (for example sensitive personal identifiable information – PII) was placed on files in the file storage service.

- The capability did not exist for agency management or DoIT personnel to monitor what information had been placed on the file storage service.

- The capability did not exist for agency management or DoIT personnel to monitor or modify what access permissions exist for files on the file storage service.

As a result of these conditions, agency management and DoIT personnel lack assurance that information (for example, PII) that should not be saved on the file storage service has not been saved there. In addition, for critical and sensitive information that has been placed on the file storage service, agency management and DoIT personnel lack assurance that access to this information has been properly restricted.

The cloud messaging and collaboration services' features can be enhanced through the use of third party utilities. These utilities can be purchased from the contractor, or the State could develop its own utilities to address certain of the aforementioned control concerns.

Recommendation 6
We recommend that DoIT

a. assess the aforementioned security control issues involving the State of Maryland's implementation of the file storage service,
b. develop solutions to mitigate the security issues, and
c. consider disabling the use of the file storage service until adequate controls can be implemented to protect against improper data disclosure and/or modification.

Information System Security and Control

Background

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 *network*Maryland and the State's wireless infrastructure and telecommunications systems. In addition, DoIT provides its own information technology services and support, as well as support for the Department of Budget and Management and the Executive Department – Governor. Our audit of DoIT included a review of

the security controls over DoIT's statewide responsibilities and agency specific responsibilities. Key information technology resources include systems that support many Statewide functions, such as the Financial Management Information System, the State's personnel system, the State's capital budgeting system, and cloud messaging and collaboration services.

Finding 7
Offsite backup of several critical network devices and an up-to-date disaster recovery plan for *network*Maryland did not exist.

Analysis
Offsite backup for several critical network devices and an up-to-date disaster recovery plan for *network*Maryland did not exist. Specifically, we noted the following conditions:

- Backup configuration files for four critical firewalls did not exist. Accordingly, if the configurations for these devices were to be destroyed or corrupted, a prolonged interruption of computer operations could occur.

- DoIT did not have an up-to-date information technology disaster recovery plan (DRP) for recovering from disaster scenarios (for example, a fire). Specifically, we were advised by DoIT personnel that, although the *network*Maryland architecture and operations had significant changes since 2007, the DRP had not been updated since October 2007 to reflect any of these changes. In addition, the DRP had not been tested since June 2007. Without an up-to-date and tested DRP, a disaster could cause significant delays (for an undetermined period of time) in restoring information systems operations beyond the expected delays that would exist in a planned recovery scenario. The State of Maryland Information Technology (*IT) Disaster Recovery Guidelines* provide information on the minimum required elements needed for a complete information system DRP and also include provisions for periodic testing.

Recommendation 7
We recommend that, for *network*Maryland, DoIT
a. store backup files of critical network device configurations at an offsite, secure, environmentally controlled location;
b. maintain a complete and comprehensive disaster recovery plan, which is updated at least annually, in accordance with the aforementioned *IT Disaster Recovery Guidelines*; and
c. test the DRP on a periodic basis in accordance with these *Guidelines* and document the results.

Audit Scope, Objectives, and Methodology

We have audited the Department of Information Technology (DoIT) for the period beginning February 9, 2009 and ending February 8, 2012. 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 DoIT's financial transactions, records and internal controls, and to evaluate its compliance with applicable State laws, rules, and regulations. 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 financial-related areas of operations based on assessments of materiality and risk. The areas addressed by the audit included monitoring of DoIT's statewide information technology contracts, the monitoring of the One Maryland Broadband Network project, the administration of the Universal Service Trust Fund and the Major Information Technology Development Project Fund, information systems security and controls, and DoIT's operating expenses including payroll. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of DoIT'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.

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 relating 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

July 23, 2013

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

Dear Mr. Barnickel:

The Department of Information Technology (DoIT) has reviewed your draft audit report for the period beginning February 9, 2009, and ending February 8, 2012. 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@maryland.gov.

Sincerely,

Elliot Schlanger
Secretary

cc: Mr. Douglas Carrey-Beaver, Principal Counsel
Ms. Stacia Cropper, Chief Operating Officer
Mr. Gregory Urban, Chief Technology
Mr. Charles Ihrie, Compliance Auditor, Department of Budget and Management (DBM)
Ms. Joan Peacock, Manager, Audit Compliance Unit, DBM

Findings and Recommendations

One Maryland Broadband Network

Finding 1
DoIT used an existing information technology contractor for project management services related to the OMBN project without the timely execution of a comprehensive task order modification.

Recommendation 1
We recommend that DoIT

a. evaluate its arrangement with the PMC to ensure that the contractor's responsibilities are adequately delineated and that the State's investment in the OMBN project is adequately protected against additional costs in the event the project is not completed timely and properly;
b. ensure the aforementioned billing issue is appropriately resolved; and
c. in the future, ensure task order modifications are timely executed and contain appropriate terms and conditions.

DoIT Response:

a. PARTIALLY CONCUR
When DoIT issued the RFP for network managed services in October 2009, DoIT asked for a broad range of services to meet the historical needs of all operations within the agency. When the contract was awarded, the contract value was based on the historical spend and actual approved budgets experienced at the time of award.

When the ARRA BTOP grant was released, a requirement of the grantees was that each would have existing contracts available to perform the work in the grant. DoIT, through a variety of contracts, including the Hardware Master Contract, Network Managed Services (NMS) Contract, and Cable and Wiring Contract, was able to perform the required work in the One Maryland Broadband Network (OMBN) proposal. The only new significant contract required was a contract to purchase fiber optic cable and related materials, mostly to gain the benefits of volume pricing and guaranteed delivery schedules.

The work required to execute the OMBN project was not unique to the project. DoIT and the networkMaryland™ program have performed this type work in prior projects. What made OMBN unique was the scale of the project. Essentially, instead of projects connecting 5-20 sites, this project would connect 1,000 sites. The skills and scope available under the NMS contract were the required skills and scope to execute the project. Since the volume of work provided by the project was not conceived when the contract ceiling was set, the contact ceiling needed to be increased to accommodate the additional work now funded via the federal grant.

DoIT and the PMC worked closely together to establish a program team that would manage the overall project, as well as the specific areas where DoIT would be responsible for the execution of the grant work. Work orders in the IT Service Management System (ITSMS) were created to task and track the

work related to the project. Since the work of the project is of the same type as the work envisioned when the NMS RFP was released, a contract modification for scope was not required.

At the time of this response, approximately six weeks remain in the period of performance of the grant. The portion of the project DoIT was responsible for executing against (15 counties) has already been completed. We have achieved 118% of the original sites in the grant and 105% of the original fiber mileage. The overall project has completed 91% of the sites and 99% of the fiber miles. During the period of performance of the grant, DoIT has increased the scope to achieve greater benefit to the State without increasing the project budget or grant amount. The revised scope of the project will connect an additional 81 locations (8% increase).

DoIT has evaluated the arrangement with the PMC, in consultation with our AAG, to ensure that the contractor's responsibilities are adequately delineated and that the State's investment in the OMBN project is adequately protected against additional costs, in the event the project is not completed timely and properly. No additional modifications to the task order, or any other procurement action, was deemed necessary. As confirmed by the AAG, the current language in the Master Contract and related Task Order documents is adequate to protect the State's investment, in the event the project is not completed timely or properly.

b. CONCUR
One element of the project is the engineering work required to be completed prior to installing fiber optic cable, either underground or on utility poles. This work traditionally was handled in the work packages provided in the Cable and Wiring Master Contract. Given the scale required by this project, DoIT decided to centralize this function with the PMC. Since a large percentage of work would be performed by subcontractors, and the industry standard billing method for this service is fixed price, based on the distance of the fiber optic segment being engineered (price/foot), DoIT sought to align the best practices of the industry with the existing NMS contract. Again, using industry standard markups for SG&A public sector engineering contracts, DoIT's Chief Technology Officer and the PMC's President agreed to an 8% markup on the direct costs of the subcontract engineering costs. DoIT agrees that this arrangement was not fully socialized through the senior management organization. Additionally, although this arrangement saved in excess of $200,000, based on direct Time and Materials billings for the labor used to perform the engineering work, the NMS contract did not have provisions for this type of billing arrangement. DoIT and the PMC have engaged in a formal process to resolve all billing issues and reconcile all costs billed for the engineering work under the contract.

c. CONCUR
In the future, DoIT will ensure that task order modifications are timely executed and will work with legal counsel, as necessary, to make sure task orders contain appropriate terms and conditions.

Finding 2
Controls were not adequate over the approval and monitoring of certain OMBN engineering and construction services and the related payments.

Recommendation 2
We recommend that DoIT
a. ensure all work orders are signed by appropriate DoIT and PMC management personnel,

b. ensure proper supporting documentation for monitoring the progress of engineering and construction services work is obtained and reviewed prior to approving the invoices for payment, and

c. separate the responsibility for selecting the contractors to perform construction services from the responsibility for reviewing and approving the related invoices for payment. We advised DoIT on accomplishing the necessary separation of duties using existing personnel.

DoIT Response:

a. CONCUR
DoIT will ensure that all work orders are properly signed by DoIT and the PMC management personnel.

b. CONCUR
DoIT concurs that supporting documentation is necessary before approving invoices for engineering and construction services. DoIT and the PMC developed the Milestone Acceptance Form early in the construction phase of the project in order that the PMC, who had resources in the field monitoring construction progress, could provide DoIT with concurrence that activities being billed were actually performed. DoIT will ensure the properly signed and completed forms are retained on file.

c. PARTIALLY CONCUR
DoIT does not concur that an individual involved in the selection process should be excluded from the review and approval process. A detailed knowledge of the activities being performed and invoiced is necessary for approval of such expenditures. DoIT does concur, however, that some process modification was necessary. As a result, DoIT has better separated the responsibilities of procurement and invoice acceptance/processing to better segregate these duties among the project team, procurement, and Fiscal Services staff.

Finding 3
DoIT did not adequately monitor one grant sub-recipient that was responsible for a significant portion of the OMBN project.

Recommendation 3
We recommend that DoIT monitor its sub-recipients in accordance with the aforementioned *Manual* by

a. documenting its review of ICBN invoices and ensuring that the invoice costs were proper and were approved by ICBN personnel, and that such costs conform to contract requirements;

b. conducting periodic on-site visits to independently verify the completion of work performed as reported; and

c. ensuring that an independent audit or review is conducted of the ICBN expenditures to ensure that federal funds were only used for authorized purposes in accordance with federal grant requirements.

DoIT Response:

a. CONCUR
DoIT concurs that its responsibilities as primary recipient under the Grant includes reviewing and documenting the review of grant expenditures. As identified in the above finding, DoIT initiated a detailed review of all ICBN expenditures in February 2012, due to deficiencies identified by DoIT prior to this audit. That review included all expenditures since the beginning of the grant and a reconciliation of those expenditures to all amounts drawn from the NTIA. Following this review, DoIT modified its processes to include a monthly review of each subsequent draw request. DoIT's review includes a visual inspection of all invoices for approval and conformance. DoIT also added another independent verification of selected invoices by DoIT personnel prior to drawing federal funds.

b. CONCUR
DoIT has tasked both personnel within the agency, and members of the team of inspectors that are monitoring DoIT construction contractors, to validate that work has been performed as instructed.

c. CONCUR
In the fourth quarter of 2012 DoIT, selected an audit contractor to perform an Agreed Upon Procedures (AUP) review for compliance with grant requirements. That review included DoIT, as well as all sub-recipients under the grant, including the ICBN. That review began and was completed during by the second quarter of 2013. No material deficiencies were discovered.

Statewide Contract Procurements

Finding 4
DoIT did not ensure compliance with its established policy regarding the minimum time period for competitive bidding and did not adequately secure bids received electronically.

Recommendation 4
We recommend that DoIT

a. ensure compliance with its established policy regarding a competitive bid period for a minimum of 20 days as referenced in State procurement regulations, and

b. establish procedures to properly restrict access to competitive sealed bid proposals received electronically.

DoIT Response:

a. PARTIALLY CONCUR
DoIT concurs that all procurements, including Competitive Sealed Proposals, must be open for proposal submission at least 20 days and will abide by that requirement. Other solicitations, using DoIT's master contracts, which are not subject to the 20 day COMAR requirement, but are subject to DoIT's review before issued, will be reviewed by DoIT to ensure that agencies issue the solicitation for a period that is reasonable for allowing Master Contractors to propose. Because Master Contractors have already agreed to the provisions of the Master Contract, and also because several of the Master Contracts require that the Master Contractor submit little more than prices, it is not always necessary or useful to provide Master Contractors several weeks to respond. Per DoIT's current policy, the competitive proposal period for solicitations that use DoIT's master contracts is evaluated on a case-by-case basis to determine

what is reasonable. At minimum and per DoIT's policy, solicitations that use a DoIT master contract will be open for proposal submission at least 5 days.

b. CONCUR
DoIT is exploring procedures and plans to establish a process to restrict access to competitive sealed proposal bids received electronically.

Major Information Technology Development Project Fund

Finding 5
DoIT could not provide certain documentation of its monitoring of major information technology development projects.

Recommendation 5
We recommend that DoIT document its project monitoring for the major information technology development projects it oversees (repeat).

DoIT Response: CONCUR

DoIT agrees to document the Portfolio Review process to capture the dates and attendees of each Review. Further, DoIT is now requiring that the agencies subject to Portfolio Reviews prepare an Action Item document, as a result of the Review, for distribution to DoIT and also to the agency's project team, business sponsor and executive sponsor. DoIT will maintain copies of those Action Item documents in the project files.

Cloud Messaging and Collaboration Services

Finding 6
Controls did not exist to ensure that information placed on the file storage service was appropriate or adequately secured.

Recommendation 6
We recommend that DoIT
a. assess the aforementioned security control issues involving the State of Maryland's implementation of the file storage service,
b. develop solutions to mitigate the security issues, and
c. consider disabling the use of the file storage service until adequate controls can be implemented to protect against improper data disclosure and/or modification.

DoIT Response: PARTIALLY CONCUR

The ability to share and collaborate on documents is a new and important capability that is made possible by the collaboration software suite. This capability has many uses in the operations of the State. One of the new features is the ability to share and collaborate on documents with people outside of a document owner's agency, and even outside of the domain of the State of Maryland. Although this may appear, at a glance, to increase the risk of releasing non-public data via this avenue, sharing documents in this fashion has fewer risks than other methods in use by agency personnel, with or without sanctioning from a given agency.

With the implementation of the collaboration software suite, DoIT modified the State's security policy, and restricted the placement of non-public data on the file storage service. One of the benefits of this document sharing system is that all users that access a document must first log into the vendor's site to view the document. Unlike other methods of sharing documents, this control greatly increases the ability to determine how data was shared outside of an agency or the domain.

Since the implementation of the collaboration software suite, DoIT has continuously looked for ways to enhance and improve the service. DoIT has identified a way to modify share settings for a document, and has administratively changed the share permissions for documents when required. Determining if a given file has non-public data is a difficult task. DoIT continues to search for ways to review documents on the file storage service to determine if non-public data is present, and if so, remove any permitted sharing of that document. At this point, a suitable tool to interrogate the data within the files has not been identified, but the program team continues to research solutions.

Information System Security and Control

Finding 7
Offsite backup of several critical network devices and an up-to-date disaster recovery plan for *network*Maryland did not exist.

Recommendation 7
We recommend that, for *network*Maryland, DoIT

a. store backup files of critical network device configurations at an offsite, secure, environmentally controlled location;
b. maintain a complete and comprehensive disaster recovery plan, which is updated at least annually, in accordance with the aforementioned *IT Disaster Recovery Guidelines*; and
c. test the DRP on a periodic basis in accordance with these *Guidelines* and document the results.

DoIT Response:

The State's high speed data network, in aggregate, has a different risk profile than a computer system or software application, which is the focus of the typical disaster recovery plan (DRP). The design of the network, with the goal of high availability and resiliency, has multiple layers of redundancy built into it. The loss of any single facility, no matter how critical, would not impact services other than those solely terminating in that facility. The carrier network, networkMaryland™, does not rely on periphery systems such as firewalls and operational support systems to serve its mission. The loss of the aforementioned firewalls would not stop the network from providing high speed data transport for the subscribers, and would not trigger activation of the DRP.

a. CONCUR
It is DoIT's policy to maintain a backup copy of all device configurations using a configuration management/repository system. Key elements of the configuration are also stored off site using a secure cloud data storage. Any devices that were identified as not having a copy of their configuration have been addressed and their configurations have been captured.

b. CONCUR
networkMaryland™ will update the DRP and review the DRP on an annual basis. This is expected to be completed in 2013. Although the network has changed since the DRP was authored in 2007, the key elements addressed in the DRP have not changed. The critical networkMaryland™ locations are still the same as in 2007, and the recovery strategies for the loss of any critical networkMaryland™ facility are, essentially, unchanged.

The most applicable element of the *Guidelines* is the requirement to maintain an inventory of equipment in the relevant facilities. An inventory of services and devices at each facility is better captured in an electronic format and referenced in the DRP, so that it will not become outdated over time. The equipment in the critical facilities had not significantly changed until the major upgrade brought about by the OMBN program, which is still in the implementation phase. A comprehensive updated inventory will be a product of the project, and this data will be stored in an asset management module of DoITs Customer Relationship Management system, which is operated from an environmentally-controlled off-site facility. The DR plan will reflect these changes.

c. CONCUR
DoIT agrees to periodically test the DRP. Testing procedures and schedule will depend on the updated DRP. Testing documentation will be maintained.

AUDIT TEAM

Matthew L. Streett, CPA, CFE
Audit Manager

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

Jonathan H. Finglass, CPA
Joel E. Kleiman, CPA
Senior Auditors

R. Brendan Coffey, CPA
Information Systems Senior Auditor

Brian S. Han
Henry H. Startzman, IV
Tu N. Vuong
Staff Auditors

Jeffrey T. Zankowitz
Information Systems Staff Auditor