Audit Report

# Department of Information Technology

September 2016

**OFFICE OF LEGISLATIVE AUDITS**
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

## For further information concerning this report contact:

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

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

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

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

**Warren G. Deschenaux**
Executive Director

**Thomas J. Barnickel III, CPA**
Legislative Auditor

September 12, 2016

Senator Guy J. Guzzone, Co-Chair, Joint Audit Committee
Delegate C. William Frick, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Department of Information Technology (DoIT) for the period beginning February 9, 2012 and ending June 30, 2015. DoIT is responsible for the State's information technology policies, provides information technology technical assistance, and oversees the implementation of major information technology projects for the State's Executive Branch agencies. DoIT also oversees the procurement of information technology and telecommunications services and products for these agencies and manages the State's information technology network.

Our audit disclosed certain deficiencies with DoIT's processes for overseeing the State's 33 major information technology development projects (MITDPs) valued at $850 million that existed as of June 2015. DoIT lacked documentation that it effectively monitored MITDPs through its review of annual status reports and quarterly portfolio review meetings. Our test of 20 quarterly portfolio reviews pertaining to five projects disclosed that documentation of the meetings was not maintained for 3 reviews. For 10 other reviews, DoIT did not document the matters discussed, whether significant corrective actions for the applicable projects were required, and if so, what these actions entailed.

DoIT had not established a process to independently evaluate the performance of the vendor-supplied project managers (OPMs) who were tasked to oversee the 33 MITDPs, nor developed specific documentation and reporting requirements for the OPMs' project management activities. Furthermore, DoIT had not established a means to ensure that the vendor assigned sufficient OPM resources to monitor MITDPs on its behalf.

Policies were lacking to guide decisions and define recordkeeping requirements pertaining to changes in project scope, schedule, and costs (referred to as rebaselining). DoIT, therefore, did not maintain records to identify the reasons and impact for any of the 12 such changes made on projects during fiscal year 2014. Furthermore, a policy was not established to govern the use of Independent Verification and Validation assessments (IV&V) of MITDPs as a means to assess their health and to identify areas that need improvement to help the projects be successful. An IV&V had been initiated on only one MITDP as of November 2015.

Our audit also disclosed certain security control deficiencies relating to the networks and computer resources under DoIT's responsibility. For example, certain contractors had been provided unnecessary network level access to workstations and servers, and numerous workstations were not appropriately protected from malware.

Finally, DoIT did not recommend a reduction in the Universal Service Fee in fiscal year 2015 in recognition of excess funds in the Universal Service Trust Fund, which is used exclusively to fund the Telecommunications Access of Maryland (TAM) program. The fee is assessed to customers of communications companies. We estimated that the fiscal year 2015 Fund balance could support TAM expenditures for at least three years without a fee being assessed to communications subscribers.

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,

TJ Barnickel III

Thomas J. Barnickel III, CPA
Legislative Auditor

# Table of Contents

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

**Statewide Contract Procurements**

**Universal Service Trust Fund**

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

# Background Information

## Agency Responsibilities

The Department of Information Technology (DoIT) is responsible for the State's information technology policies, procedures, and standards, and for overseeing the implementation of major information technology projects for the State's Executive Branch agencies and commissions.[1] DoIT also 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 with others through TTY (text telephone) using a standard phone; this program is supported by the Universal Service Trust Fund.

According to the State's records, during fiscal year 2015, DoIT's operating expenditures totaled $99.2 million.

## Status of Findings From Preceding Audit Reports

Based on our assessment of significance and risk relative to our audit objectives, our audit included a review to determine the status of five of the seven findings contained in our preceding audit report dated August 1, 2013. We determined that DoIT satisfactorily addressed three of the five findings. The remaining two findings are repeated in this report. We did not follow up on the remaining two findings that pertained to the One Maryland Broadband Network since this project was completed shortly after our preceding audit report was issued.

Our audit also included a review to determine the status of 5 of the 12 findings contained in our performance audit report, dated September 27, 2012. The performance audit report assessed DoIT's information system data security

[1] According to State law, DoIT does not have authority over or responsibility for the University System of Maryland, Morgan State University, and St. Mary's College.

policies and selected State agencies' compliance with certain policies. We determined that DoIT satisfactorily addressed these 5 findings.

# Findings and Recommendations

## Major Information Technology Development Projects

### Background

State law provides the Department of Information Technology (DoIT) with the responsibility for overseeing the development and implementation of major information technology development projects (MITDPs). MITDPs are defined as any information technology development project that meets one or more of the following conditions:

- The project's estimated total cost is at least $1 million.
- The project supports a critical business function associated with the public health, education, safety, or financial well-being of the citizens of Maryland.
- DoIT's Secretary determines the project requires special attention.

State law requires DoIT to approve funding for MITDPs only when projects are supported by an approved system development life cycle (SDLC) methodology. The SDLC assists agencies through the planning and execution of successful information technology projects. DoIT's oversight responsibilities generally include (1) reviewing critical project documents, including the management plan, functional requirements documents, procurement documents, and system testing plan; (2) conducting quarterly portfolio review meetings with agencies implementing MITDPs; and (3) initiating Independent Verification and Validation assessments. Since December 2013, DoIT has contracted with a vendor to provide personnel for project oversight services. However, DoIT retains ultimate oversight responsibility.

According to DoIT's records, as of June 2015, there were 33 MITDPs valued at approximately $850 million. More than 75 percent of the value of these projects was related to agencies responsible for providing services in the health, education, financial, and public safety sectors of State government. MITDPs are funded from multiple sources including the State's Major Information Technology Development Fund, which DoIT administers. According to DoIT's records, Fund expenditures totaled approximately $27.3 million during fiscal year 2015, including $1.7 million for project oversight.

**Finding 1**
**DoIT lacked sufficient documentation supporting its reviews of annual MITDP status reports and system development documents, and that quarterly portfolio reviews were conducted.**

**Analysis**
DoIT lacked sufficient documentation to support that it effectively monitored MITDPs through its reviews of information technology project annual status reports and system development documents, and its quarterly portfolio review meetings for MITDPs. We noted the following issues based on our test of five MITDP projects valued at $355.5 million.

Information Technology Project Requests
DoIT was not ensuring that agencies' annual project status reports, known as Information Technology Project Requests (ITPRs), were current prior to approving them. An ITPR includes a summary of the project scope, the needs addressed, potential risks, possible alternatives, estimated costs, and funding sources, and describes how the project meets the goals of the Statewide Information Technology Master Plan. State law requires agencies to annually complete and submit an ITPR for DoIT's review and approval throughout the MITDP life cycle. DoIT submits the approved ITPRs to the Department of Budget and Management (DBM) and the Department of Legislative Services[2] for budget analysis purposes.

Our test of the ITPRs submitted for the aforementioned five projects during fiscal year 2015 (for fiscal year 2016) disclosed that DoIT approved the ITPRs even though certain information on ITPRs for three projects valued at $163.6 million had not been updated from the prior year's ITPR. For example, explanations of the risks and the milestones achieved for two MITDPs were not updated. For one of these two projects, although the ITPR indicated certain phases of the project had been completed, the completion dates for 13 of the 17 milestones required to be completed during these phases were not reported. Consequently, the accuracy, completeness, and reliability of the information included on the ITPRs was not assured.

[2] ITPRs involve a two-step approval process to ensure State agencies follow a standardized approach to requesting approval and funding for MITDPs. Step one is in the form of a Project Planning Request and step two is in the form of a Project Implementation Request. An agency initially submits a Project Planning Request each year until the project has completed the required planning and requirements analysis phases, including a baseline project budget and schedule. Once these phases are completed, the agency submits a Project Implementation Request each year until the project has completed the design, development, testing, implementation, and operation phases.

### System Development Life Cycle

DoIT did not document its approval when agencies completed each system development life cycle (SDLC) phase, as reported on the ITPR. Although not required by State law, approval of each SDLC phase of the MITDP is critical because these projects are often large and complicated, involve high costs, and support a critical business function for the State. The SDLC is intended to reduce the risk of project failure through the application of a proven and incremental project development process performed in a logical manner. Currently, DoIT documents its approval from general project planning to project implementation but not for each phase within the SDLC. Generally, the SDLC involves nine phases, such as planning, design, testing, and implementation.

### Quarterly Portfolio Review Meetings

While DoIT's policies require that quarterly portfolio review meetings be conducted, specific documentation requirements were not established. In practice, DoIT generally required that each quarterly portfolio review meeting be documented with an attendance sign-in sheet and the agency's self-assessments of project status, including schedule, budget, expenditures, and risks. However, DoIT frequently did not document significant matters discussed during these meetings. Quarterly portfolio review meetings are a critical part of project monitoring and are used to determine if corrective actions are needed to address project risks.

We reviewed the most recent quarterly portfolio reviews, primarily for fiscal year 2015, for each of the five MITDP projects tested (total of 20 quarterly portfolio reviews) and noted certain issues with 13 of the reviews. For 3 reviews, DoIT could not provide any documentation that the meetings occurred. For 10 reviews, an attendance sign-in sheet was maintained, but DoIT did not document the matters discussed, nor did DoIT document whether significant corrective actions were required and, if so, what these actions entailed. One of these projects was the same one mentioned previously in which the milestone completion dates were not reported on the ITPR submitted during fiscal year 2015. In addition, agency's self-assessments of project status were only provided for 5 of the 10 reviews. Finally, DoIT did not document that it verified the accuracy of the agency self-assessments of project status for any of the reviews.

DoIT advised us that it believes it provides sufficient oversight through regular verbal communication with the agencies, including during these meetings, and relies on the agencies to record the discussed corrective actions. Nevertheless, complete documentation should be maintained by DoIT to demonstrate effective monitoring of projects. A similar condition regarding the lack of sufficient documentation of project monitoring efforts was commented upon in our two preceding audit reports.

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

**a. ensure project status information reported on the ITPR is current and complete as part of its annual review and approval process;**
**b. implement procedures to approve each SDLC phase when successfully completed; and**
**c. establish and adhere to specific documentation requirements to support that quarterly portfolio review meetings were performed, that agency project status reports were verified for accuracy, and that its recommended corrective actions resulting from the meeting were documented (repeat).**

**Finding 2**
**DoIT had not established a process to independently evaluate project managers hired through a vendor to oversee MITDPs, specific project monitoring documentation and reporting requirements, nor a means to ensure sufficient contract personnel were assigned to monitor all 33 MITDPs valued at $850 million.**

**Analysis**
DoIT had not established a process to independently evaluate the performance of the vendor-supplied oversight project managers (OPM), nor had DoIT developed specific documentation and reporting requirements for their project management activities. Furthermore, DoIT had not established a means to ensure that the vendor assigned sufficient OPM resources to monitor MITDPs on its behalf. Consequently, assurance was lacking that the vendor was effectively monitoring the development and implementation of all 33 MITDPs valued at $850 million.

DoIT had not established a formal process to independently assess whether OPMs hired by its vendor to monitor assigned MITDP projects were properly performing their duties and meeting expectations. According to the contract, the vendor's OPMs were required to follow project management methodologies consistent with DoIT's policies (such as, System Development Life Cycle) and the Project Management Institute's *Project Management Body of Knowledge (PMBOK). PMBOK* is generally recognized as a best-practice standard in the project monitoring industry by providing extensive guidance and formal methodologies. OPMs were also responsible for reviewing and assessing MITDP documentation (such as ITPRs and SDLC documentation), communicating with project teams and stakeholders, contributing to DoIT's MITDP reports, and attending quarterly portfolio review meetings.

DoIT had processes in place to direct and approve the work of OPMs, including establishing work orders, requiring the submission of bi-monthly activity reports, and verifying hours worked. However, DoIT did not specify the types of documentation that OPMs should gather while overseeing the projects nor specify the information that should be included in the OPMs' bi-monthly activity reports. Consequently, we found that when activity reports were submitted, the descriptions of the reported work performed by the individual OPMs varied in content and specificity. This could impede DoIT's ability to determine whether OPMs were effectively monitoring project status, including the cost, scope, and implementation schedule.

Additionally, DoIT did not establish a means to ensure an adequate number of OPMs were assigned commensurate with the number and complexity of MITDPs. Specifically, DoIT did not measure the workload of each OPM and determine if an appropriate number of individuals were assigned to effectively monitor each project, as recommended by *PMBOK*. Although the contract terms provided for up to 20 OPMs to be assigned to meet DoIT's project oversight needs, DoIT could not explain why only 6 OPMs were assigned to oversee the MITDPs as of June 2015.

In December 2013, DoIT executed a two-year contract (including three one-year renewal options) totaling $32.2 million with this vendor to provide OPM personnel for oversight support services, primarily for MITDPs. According to DoIT's records, payments to the vendor since the inception of the contract totaled approximately $3.8 million as of December 2015.

**Recommendation 2**
**We recommend that DoIT**

a. **establish a process to independently evaluate the performance of OPMs,**
b. **develop specific documentation and reporting requirements for OPM project monitoring activities, and**
c. **establish a process to ensure an adequate number of OPMs are assigned to meet the project oversight needs.**

## Finding 3
**DoIT had not established comprehensive policies for project changes to scope, schedule, or costs (rebaselining) and Independent Verification and Validation assessments.**

### Analysis

DoIT had not established comprehensive policies for project changes to scope, schedule, or costs (rebaselining) and for the use of Independent Verification and Validation assessments (IV&Vs). During the planning phases of the SDLC, a project's baseline for scope, schedule, and cost is established and is the measurement against which a project team manages and is held accountable. A project can be rebaselined for valid reasons (such as, changes in goals, requirements, funding, or to correct inaccuracies), but rebaselining could also be used to mask cost overruns or schedule delays. An IV&V serves as an independent assessment on the overall health of the project; it identifies strengths and areas that need improvement to help the project be successful, on time, and within the allotted budget, and serves to strengthen DoIT's routine project oversight performed by OPMs.

#### Rebaselining

Since a rebaselining policy had not been established, DoIT management advised us that it rebaselined projects based on its subjective judgment or at the request of the agency implementing an MITDP. Furthermore, historical records to readily identify all rebaselining occurrences during the life of each project, including the reasons and project impact, were not maintained. According to DoIT's records, 12 of the 42 projects it monitored in 2014 (29 percent) were rebaselined for one or more reasons, such as changes in project scope, schedule, and/or budget.

*PMBOK* recommends that project managers establish a comprehensive rebaselining policy and a formal process to track and explain the changes to the baseline for scope, schedule, and cost. A comprehensive policy should address the following elements:

- A description of valid reasons for rebaselining a project
- A description of the process for developing a new baseline
- A requirement that the new baseline be validated, and reviewed and approved by management
- A requirement that rebaselining decisions be documented, including the reasons, specific changes, and management's review and approval

### Independent Verification and Validation Assessments

Since an IV&V policy had not been established, DoIT management advised us that the decision to initiate an IV&V was generally made during the project development phase when its quarterly portfolio review meetings indicated an MITDP had unaddressed risks with budget, scope, and/or schedule. However, the lack of an IV&V policy resulted in unclear guidance and definitions of risk factors to trigger an IV&V. According to its annual report on MITDPs as of November 2015, and based on discussions with DoIT management, DoIT had only initiated one IV&V for one of the 33 MITDPs. According to DoIT's records, as of June 30, 2015, DoIT had not documented a determination as to whether to initiate an IV&V for any of the projects being monitored at that time, including 19 projects that were in the more critical implementation/development phases of the SDLC. Additionally, DoIT management could not document how IV&V results should be considered during its project oversight.

IV&Vs can be performed throughout the SDLC as an independent means to determine whether the system is being built using practices that lead to a successful implementation (verification), and whether the completed system will provide the needed functionality to satisfy the intended business purpose (validation). Establishment of an IV&V process early in the project planning phase allows the IV&V team members to have an unbiased view into the project planning, scheduling, budgeting, and resource allocation. Implementing IV&V processes during the planning phase ensures the development contractor's compliance with mandated scope and functionality of the software and helps prevent cost overruns. Based on our research, we determined that a comprehensive IV&V policy could incorporate the following elements:

- A description of the systematic methodology to be used by the IV&V vendor for periodically calculating project risk based on parameters including project significance, agency project management performance, vendor performance, funding, schedule slippage, cost overruns, and significant scope changes
- Requirements for documenting considerations for whether and when to initiate an IV&V
- Guidelines for taking corrective actions to mitigate risks when an IV&V is not performed
- Guidelines for determining the IV&V scope and whether the IV&V should be initiated at one or more points during the project, or should represent continuous monitoring throughout the project
- Guidelines for considering IV&V results and documenting follow-up efforts to determine the status of recommended actions (such as, reassessing resources and staffing, suspending, or terminating a project)

- Provisions for when the IV&V vendor should conduct a post-implementation assessment once the project has been in production for several months to determine if business and technical objectives were achieved

**Recommendation 3**
**We recommend DoIT establish and adhere to comprehensive policies, including the aforementioned suggested provisions, governing project rebaselining decisions and recordkeeping, and the use of IV&Vs.**

## Information Systems Security and Control

**Background**
DoIT has statewide Information Technology (IT) responsibilities as well as support service responsibilities on an agency-specific level as follows:

- DoIT manages the development and operations of the State's data network known as networkMaryland.

- DoIT is responsible for statewide applications such as the Financial Management Information System, personnel system, and employee benefit system. The Office of Legislative Audits separately examines controls for these statewide applications within the separate audits of the Financial Management Information System – Centralized Operations and the DBM Office of Personnel Services and Benefits.

- In addition to its Statewide role, DoIT has responsibility for IT and telecommunication services and support for DoIT, DBM, and the Executive Department – Office of the Governor (EOG). This includes infrastructure development, acquisition and maintenance, and application development and maintenance.

- During fiscal year 2015 DoIT began providing network protection termed Security as a Service (SECaaS) and managed desktop services (which included malware protection) to certain State agencies with the goal of expanding these services to numerous State agencies in the future.

Our audit of DoIT included a review of the security controls over DoIT's statewide responsibilities and agency specific responsibilities, including SECaaS and managed malware protection.

## Finding 4
## The DoIT, DBM, and EOG networks were not properly secured in that certain contractors had been granted unnecessary access and certain security capabilities were not fully used.

### Analysis

The DoIT, DBM, and EOG networks were not properly secured in that certain contractors had been granted unnecessary access and certain security capabilities were not fully used.

- Contractors had unnecessary network level access to the DoIT and DBM networks. Both DoIT and DBM were developing several systems with extensive use of third-party contractors. These contractors worked both on-site at DoIT and DBM locations and remotely. We were advised that these contractors only required access to the specific development servers involved with their projects and certain support servers. Although DoIT had implemented various controls to help secure the DoIT and DBM networks from contractors working remotely, appropriate controls were not in place for those working on-site. Consequently, we determined that 57 of 213 contractors had unnecessary network level access to DoIT and DBM workstations and numerous critical servers other than the development and support servers that they needed to access.

- Our test of advanced security appliances determined that DoIT did not fully utilize the expanded capabilities of these appliances to provide enhanced perimeter security over the DoIT, DBM, and EOG networks. Specifically, we noted that four available features (including the ability to allow or deny traffic based on the application traversing the network) that would provide enhanced network security were not used.

- Although the network-based intrusion detection prevention system (IDPS) used by DoIT for the DoIT and DBM networks had the capability to decrypt and analyze encrypted network traffic received, this feature was not enabled. Furthermore, we determined that host-based intrusion protection systems (HIPS) were not in use on DoIT and DBM servers that processed encrypted traffic. The absence of IDPS coverage for such encrypted traffic created a network security risk as such traffic could contain malicious exploits which are not detected or dropped. Complete IDPS coverage includes the use of a properly-configured, network-based IDPS that analyzes encrypted traffic, and/or the use of an HIPS on critical servers, to aid significantly in the detection and prevention of, and response to, potential network security breaches and attacks.

**Recommendation 4**
**We recommend that DoIT**

a. **restrict each DoIT and DBM contractor's network level access to only those servers and workstations that each contractor needs to access;**
b. **fully utilize the expanded capabilities of the advanced security appliances to properly secure the DoIT, DBM, and EOG networks; and**
c. **perform a documented review and assessment of its network security risks from encrypted traffic and identify how IDPS and/or HIPS coverage should be best applied to its network and implement this coverage.**

### Finding 5
### Computers covered by DoIT's managed desktop services were not properly maintained and secured with current malware protection.

**Analysis**
Computers covered by DoIT's managed desktop services were not properly maintained and secured with current malware protection. DoIT provided managed desktop services, including malware protection, for DoIT, DBM, EOG, and three other State agencies. In total, these six agencies operated approximately 1,700 computers.

- Numerous DoIT managed computers were running outdated versions of the malware protection software. We identified 188 computers that were running an outdated version of the malware protection software as of July 2015. Of these 188 computers we determined that 113 computers were using an outdated version released in December 2012. Updated versions of the software were released in May 2014 and April 2015.

- We identified 113 workstations with local administrator rights defined on these workstations. For DoIT and DBM employees (other than system and network administrators) we identified 32 workstations that had assigned local administrative rights to the user. DoIT could not provide any documentation which authorized and supported administrative rights defined for these 32 employees. Administrative rights are the highest permission level that can be granted to users and it allows users to install software and change configuration settings. Accordingly, if these computers were infected with malware, the malware would run with administrative rights and expose these workstations to a greater risk of compromise than if the workstation's user account operated with only user rights.

- Numerous workstations and servers had not been updated with the latest releases for software products that are known to have significant security-related vulnerabilities. Although the vendors for these software products frequently provide software patches to address these vulnerabilities, DoIT had not updated workstations and servers for these patches. For example, as of July 2015, we identified 662 computers that were running older versions of a commonly vulnerable application. The older versions had software release dates ranging from October 2008 to June 2015, with a majority of the release dates between January and June 2015.

The State of Maryland's *Information Security Policy* states that agencies, at a minimum, must protect against malicious code (viruses, worms, Trojan horses) by implementing anti-malware solutions that, to the extent possible, include a capability for automatic updates.

**Recommendation 5**
**We recommend that DoIT**

**a. ensure that all managed computers are running current versions of their malware protection software,**
**b. ensure that administrative rights on managed workstations are restricted to system and network administrators, and**
**c. promptly install all critical security-related software updates for commonly vulnerable applications on all managed computers.**

## Statewide Contract Procurements

**Finding 6**
**DoIT did not properly instruct State agencies procuring services from DoIT's statewide contract to secure competitive bids received electronically and DoIT did not always properly secure its own bids.**

**Analysis**
DoIT did not properly instruct State agencies that procured services from DoIT's Consulting and Technical Service Plus (CATS+) statewide information technology contract to secure competitive bids received via email. In January 2015, DoIT issued guidance to State agencies regarding competitive bids received via email. (Prior to January 2015, DoIT had not issued guidance on this topic.) The issued guidance required that financial proposals be password protected; however, it did not require that technical proposals be password protected, and it did not specify that bids be opened in the presence of two State employees. DoIT's guidance should be consistent with State procurement regulations which

require competitive bids (both technical and financial proposals) be secured and opened in the presence of two State employees. Consequently, there is a risk that confidential competitive bid information could be accessed and disclosed without detection to other prospective bidders.

Furthermore, our tests disclosed that DoIT did not properly secure its own bids. We tested two CATS+ contracts that DoIT (as user agency) solicited and awarded in April and May of 2015 for its own operations. Our test disclosed that, for one contract totaling $1 million, only the financial proposals were password protected and, for the other contract totaling $100,000, neither the technical nor the financial proposals were password protected. Also, DoIT did not document that these proposals had been opened in the presence of two State employees.

According to DoIT's records, during the period from August 2013 to July 2015, 113 contracts totaling $479.5 million were awarded through the CATS+ master contract, including 15 contracts totaling $108.2 million awarded by DoIT for its operations and responsibilities. The statewide CATS+ contract includes preapproved contractors obtained via a competitive proposal process to provide information technology consulting and technical services in 17 different functional areas (such as software engineering, information system security, and management consulting). State agencies may then issue task order requests and perform their own competitive solicitation for services through the preapproved contractors.

A similar condition was commented upon in our preceding audit report.

**Recommendation 6**
**We recommend that DoIT**

a. **revise its guidance for the CATS+ contract to require that access to competitive bid proposals received electronically be properly restricted and ensure this guidance is established for all its statewide contracts (repeat),**
b. **ensure that agencies using DoIT's statewide information technology contracts are specifically instructed to document the opening of competitive bid proposals in the presence of at least two State employees, and**
c. **properly secure its own bids consistent with this guidance.**

## Universal Service Trust Fund

**Finding 7**
**DoIT did not recommend an appropriate reduction in the Universal Service Fee in recognition of excess funds in the Universal Service Trust Fund.**

**Analysis**
DoIT did not recommend an appropriate Universal Service Fee reduction for fiscal year 2015 that considered the Universal Service Trust Fund (USTF) balance and projected expenditures for that year. According to State law, the Universal Service Fee, which is determined annually by DoIT and implemented by the Maryland Public Service Commission (PSC), is to be set at an amount that is necessary to generate sufficient revenues to fund the costs of the Telecommunications Access of Maryland (TAM) program for the following year. In the past several years, the USTF balance has increased and it currently significantly exceeds the amount needed to fund annual TAM program costs.

The TAM program provides telecommunications relay service for Marylanders who are deaf, hard of hearing, or speech-disabled so they can communicate with others through TTY (text telephone) using a standard phone. State law provides that the Universal Service Fee be collected from customers of communications companies that provide landline telephone service, wireless or cellular telephone service, or Voice Over Internet Protocol (VoIP) service in Maryland. The communications companies remit the Universal Service Fee collections to the Comptroller of Maryland for deposit into the USTF, which is used exclusively to fund the expenses of the TAM program.

During fiscal year 2013, USTF revenue totaled approximately $7.8 million and TAM program expenditures totaled $4.0 million; the USTF fund balance was $6.7 million as of June 30, 2013. Based upon DoIT's recommendation, the PSC reduced the monthly Universal Service Fee in fiscal year 2014 from the maximum allowed by law of $0.18 per subscriber account to $0.11. However, the USTF balance continued to increase to $10.3 million as of June 30, 2014, reflecting both an increase in revenue and a decrease in expenditures, and DoIT did not recommend a fee reduction for fiscal year 2015. The increase in the USTF balance is due in part to a law change (Chapters 571 and 572, Laws of Maryland 2012), effective July 1, 2012, that expanded the companies required to collect and remit the Universal Service Fee revenues from just those providing landline phone service to include companies providing wireless or cellular telephone service, or VoIP service.

According to State records, the USTF balance was $12.4 million as of June 30, 2015. Accordingly, we estimate that the fiscal year 2015 USTF balance could support the TAM program for at least three years without a Universal Service Fee being assessed by communications companies to subscribers. Subsequent to our audit, DoIT recommended a fee reduction in December 2015, and in April 2016, PSC approved a rate reduction to $0.05.

**Recommendation 7**
**We recommend that DoIT**

a. **annually determine the minimum balance needed in the USTF, considering the fund balance and projected TAM expenditure activity for that year; and**
b. **recommend a change in the Universal Service Fee, as necessary.**

# Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Department of Information Technology (DoIT) for the period beginning February 9, 2012 and ending June 30, 2015. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by 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.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. 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, information systems security and controls, and DoIT's operating expenses. We also determined the status of five of the seven findings contained in our preceding audit report and certain findings contained in our performance audit report on information system data security dated September 27, 2012.

Our audit did not include a review of certain support services provided to DoIT by the Department of Budget and Management (DBM) Office of the Secretary. These support services (such as legal, internal audit, and budgeting) are included within the scope of our audit of DBM.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of DoIT operations, and tests of transactions. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk. Unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, the results of the tests cannot be used to project those results to the entire population from which the test items were selected.

We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from this source were sufficiently reliable for the purposes the data were used during this audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

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

LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lieutenant Governor

DAVID A.GARCIA
Secretary

State of Maryland
Department of Information Technology

September 8, 2016

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 audit report for the period beginning February 9, 2012 and ending June 30, 2015. 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 410-697-9401 or David.Garcia@maryland.gov.

Sincerely,

David A. Garcia, Secretary
Department of Information Technology

cc: Mr. James Appel, Executive Financial Officer
Mr. Al Bullock, Chief of Staff
Mr. Douglas Carrey-Beaver, Principal Counsel
Mr. Gregory Urban, Chief Operations Officer

**Finding 1**
**DoIT lacked sufficient documentation supporting its reviews of annual MITDP status reports and system development documents, and that quarterly portfolio reviews were conducted.**

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

a. **ensure project status information reported on the ITPR is current and complete as part of its annual review and approval process;**
b. **implement procedures to approve each SDLC phase when successfully completed; and**
c. **establish and adhere to specific documentation requirements to support that quarterly portfolio review meetings were performed, that agency project status reports were verified for accuracy, and that its recommended corrective actions resulting from the meeting were documented (repeat).**

***Department Response***

***a. Concur***
*The Oversight Project Managers (OPMs) will work with the Agencies to ensure that all information, including project funding requests and spending, provided on the ITPRs are accurate at the time of submission and that the appropriate amount of oversight funding is budgeted in the ITPR.*

***b. Disagree***
*OPMs review the suite of documentation required for each SDLC phase and are continuously engaged with the project team to provide guidance and perform these reviews as documentation is completed. While not a formal approval transition from step to step is discussed within the program management team. Legislative approval is sought when moving an MITDP from the Project Planning Request (PPR) phase to the Project Implementation Request (PIR) phase.*
*As the current SLDC waterfall model is transforming into a Lean Agile model, the phases and suite of documentation for planning and implementation will also adjust accordingly. DoIT will become involved in the planning and project management of the work being executed. DoIT will work collaboratively with DLS when developing the model to assure the needs of the future state/process are defined, and the application of the process is logical.*

**Auditor’s Comment**: While a project’s transition between the 9 SDLC steps may have been discussed within the project management team, DoIT did not have procedures to approve each phase when successfully completed. Approval of each phase of a project is critical to help mitigate development risk for projects that are often large and complicated, involve high costs, and support critical business functions. Nevertheless, DoIT’s transition to a Lean Agile model will necessitate a new methodology for reviewing and approving project development activities, and DoIT has agreed to pursue the matter with the Department of Legislative Services.

***c. Concur***

*Standard process requires OPMs to maintain Portfolio Review documentation such as sign in sheets, project schedules, and financial information for the MITDP Portfolio Reviews. DoIT had incorporated into its process that corrective actions were the Agencies responsibility to document and submit to DoIT following the portfolio reviews. DoIT Management will put measures in place to ensure OPMs submit the appropriate documentation following each Portfolio Review.*

*Since 2016, a revision was made to the portfolio review process which adjusts the frequency of portfolio reviews based on the monthly project’s performance and health assessments identified during DoIT Executive Management meetings. This allows for continued visibility into the project’s state. At the outcome of these monthly meetings, Portfolio reviews will be held per the Secretary’s discretion based on concerns communicated from the assessments of the project.*

**Finding 2**

**DoIT had not established a process to independently evaluate project managers hired through a vendor to oversee MITDPs, specific project monitoring documentation and reporting requirements, nor a means to ensure sufficient contract personnel were assigned to monitor all 33 MITDPs valued at $850 million.**

**Recommendation 2**

**We recommend that DoIT**

**a. establish a process to independently evaluate the performance of OPMs,**

**b. develop specific documentation and reporting requirements for OPM project monitoring activities, and**

**c. establish a process to ensure an adequate number of OPMs are assigned to meet the project oversight needs.**

***Department Response***

***a. Concur***

*DoIT recognizes the need to define and measure the effectiveness of OPM performance. As part of the Department's transformation to Lean Agile development the previous waterfall methodology related metrics will no longer be applicable. DoIT will concurrently define the appropriate metrics and compile these into a performance scorecard as part of the development/transformation efforts to which the OPM's will be evaluated against.*

***b. Concur***

*Currently OPM's are to provide standard weekly status reports, monthly MITDP health assessment charts, project reporting for mid-year and end of year reports to DLS and other reports and documents as requested. As stated above in Recommendation 2a., DoIT will also identify the specific documentation and reporting requirements an OPM should adhere to in a Lean Agile development environment.*

***c. Concur***

*Current OPM assignments are made based upon level of effort required per individual project and by certain criteria (project size, visibility, health, risk factors, project phase). Additional resources for the contract are utilized for business process analysis and procurement support required to support MITDP efforts. The number of factors involved in properly balancing workloads makes it difficult to have a formula.*

*As with response 2a DoIT will develop metrics for OPM assignments concurrently with our transition to Lean Agile.*

**Finding 3**
**DoIT had not established comprehensive policies for project changes to scope, schedule, or costs (rebaselining) and Independent Verification and Validation assessments.**

**Recommendation 3**
**We recommend DoIT establish and adhere to comprehensive policies, including the aforementioned suggested provisions, governing project rebaselining decisions and recordkeeping, and the use of IV&Vs.**

***Department Response***

***Concur***
*Although there is currently no formal written policy regarding rebaselining practices, OPMs were responsible for monitoring and reporting on project rebaselining. Any baseline changes that occur are reported in Portfolio review meetings and during schedule status discussions. A rebaselining policy will be developed that fits with the transition to Agile development.*

**Finding 4**
**The DoIT, DBM, and EOG networks were not properly secured in that certain contractors had been granted unnecessary access and certain security capabilities were not fully used.**

**Recommendation 4**
**We recommend that DoIT**

a. **restrict each DoIT and DBM contractor's network level access to only those servers and workstations that each contractor needs to access;**
b. **fully utilize the expanded capabilities of the advanced security appliances to properly secure the DoIT, DBM, and EOG networks; and**
c. **perform a documented review and assessment of its network security risks from encrypted traffic and identify how IDPS and/or HIPS coverage should be best applied to its network and implement this coverage.**

*Response*
***a. Disagree.***
*Contractors on the network that use State owned devices should not be restricted any more than any other state owned device at the network layer. Contractors that use their own devices are restricted to only the devices they work on or have to VPN in from the guest network. We do however agree we should implement security rules that are based upon an individual user's role and the applications that the user is authorized to use based on that role.*
***b. Concur.***
*DoIT will look into using the application identify feature more fully as part of a comprehensive review of our security posture.*
***c. Concur.***
*We believe that DoIT should perform and document a review of network security risks from encrypted network traffic. Gartner and NIST have published best practices for addressing this concern, and DoIT has started implementing inspection of encrypted traffic for agencies with specific requirements to do so. DoIT will both complete a comprehensive analysis of the risks, and implement decryption and inspection on encrypted traffic prior to the next audit cycle.*

**Finding 5**
**Computers covered by DoIT's managed desktop services were not properly maintained and secured with current malware protection.**

**Recommendation 5**
**We recommend that DoIT**

**a. ensure that all managed computers are running current versions of their malware protection software,**
**b. ensure that administrative rights on managed workstations are restricted to system and network administrators, and**
**c. promptly install all critical security-related software updates for commonly vulnerable applications on all managed computers.**

*Response*
***a. Concur.***
*DoIT has standardized on an anti-malware platform and is in the process of deploying this centralized, enterprise quality solution- for this activity to all computers managed by DoIT.*
***b. Concur.***
*DoIT tracks the numbers of Administrative Privileged users and is actively reducing those numbers. We have, in the past 12 months, consciously engaged in the practice of limiting administrative rights on computers managed by DoIT with the intent to only provide administrative rights to system and network administrators.*
***c. Concur.***
*DoIT routinely scans servers and workstations to verify software and hardware are up to date. Patches and updates are installed regularly through a centralized enterprise software distribution server.*

**Finding 6**
**DoIT did not properly instruct State agencies procuring services from DoIT's statewide contract to secure competitive bids received electronically and DoIT did not always properly secure its own bids.**

**Recommendation 6**
**We recommend that DoIT**

a. **revise its guidance for the CATS+ contract to require that access to competitive bid proposals received electronically be properly restricted and ensure this guidance is established for all its statewide contracts (repeat),**
b. **ensure that agencies using DoIT's statewide information technology contracts are specifically instructed to document the opening of competitive bid proposals in the presence of at least two State employees, and**
c. **properly secure its own bids consistent with this guidance.**

***Department Response***
***a. Concur***
*Based on DoIT's previous audit in 2013, the OLA found that DoIT "did not secure competitive bids received electronically". Given that the word "bid" commonly means pricing, and that COMAR 21.02.01 defines a "Bid" as a statement of price, terms of sale, and description of the supplies/services, DoIT assumed that it could satisfy the audit finding by securing the financial proposals alone. However, DoIT realizes that its assumption was wrong and is revising its policies and procedures accordingly.*
***b. Disagree***
*DoIT does not have the authority to create a policy that contradicts COMAR and it does not have the discretion to waive regulatory requirements. COMAR 21.05.03.03 (G) (1) requires proposals to be opened in the presence of at least two State employees, and that is the practice at DoIT. Moreover, DoIT's policy for opening electronic proposals is not inconsistent with procurement regulation simply because it did not expressly require proposals to be opened in the presence of two employees. With that being said, DoIT agrees that proposal openings should be documented and it is revising its procedures to satisfy the recommendation.*

> Auditor's Comment: The audit recommendation does not suggest that DoIT should implement a policy that contradicts State procurement regulations (Title 21 of the Code of Maryland Regulations). Rather, DoIT should provide instructions to ensure that certain requirements of those Regulations are properly adhered to by State agency personnel using DoIT's statewide information technology contracts. Nevertheless, DoIT has agreed to revise its procedures to address the recommendation.

***c. Concur***

*With its move to a new headquarters, DoIT has identified secure holding locations to support this recommendation.*

**Finding 7**
**DoIT did not recommend an appropriate reduction in the Universal Service Fee in recognition of excess funds in the Universal Service Trust Fund.**

**Recommendation 7**
**We recommend that DoIT**

**a. annually determine the minimum balance needed in the USTF, considering the fund balance and projected TAM expenditure activity for that year; and**
**b. recommend a change in the Universal Service Fee, as necessary.**

***Department Response***
***a. Disagree***
*TAM took the following into consideration when determining the amount needed for effectively and efficiently providing services to Maryland consumers:*
*FY'14 was the first year that changed in the manner in which the USTF was assessed. Prior to FY'14, the surcharge was based on a per land-line basis only. In 2014 the General Assembly expanded the revenue base to include VoIP and Wireless/cellular and changed the surcharge from per line to per account.*
*In May, 2015 the FCC released Report and Order and Further Notice of Proposed Rulemaking (CG Docket No. 13-24) and (CG Docket No. 03-123) "In the Matter of Misuse of Internet Protocol Captioned Telephone Service (IPCTS), Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities". This Report serves as a warning to the States that the FCC may turn over responsibility for these services (no longer provide the funding). When the responsibility is turned over to the States for IP and IP CTS, it is estimated that it will cost the State an additional $9m to $11m per year. Therefore, it is imperative that the surplus remain in our account so we are prepared to take on the responsibility of this upcoming unfunded mandate from the FCC.*

> **Auditor's Comment**: While we were aware of the Federal Communications Commission (FCC) report, the report did not indicate when, if ever, FCC could decide to turn over certain responsibilities to the states. If that occurs, we assume DoIT would request a fee change at that time to cover any additional costs. Since DoIT has since requested and obtained a fee reduction, it appears that FCC's possible action is no longer a significant concern.

***b. Concur***

*In January of 2016, DoIT/TAM recommended in a letter to the PSC that the surcharge be cut in half from the current $.11 fee.  The Hearing to discuss this with the PSC has already been re-scheduled two times.  The Hearing is currently scheduled for April 6, 2016.*

## AUDIT TEAM

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

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

**Joel E. Kleiman, CPA**
**Marissa L. Eby, CPA**
Senior Auditors

**R. Brendan Coffey, CPA, CISA**
**Christopher D. Jackson, CISA**
Information Systems Senior Auditors

**Amanda M. Jones**
**Nathan H. Suffin, CPA**
Staff Auditors

**Steven D. Bryant**
Information Systems Staff Auditor