Audit Report

Department of Information Technology

May 2020

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

To Obtain Further Information

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

To Report Fraud

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.

Nondiscrimination Statement

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 United States 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

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

May 1, 2020

Senator Clarence K. Lam, M.D., Senate Chair, Joint Audit and Evaluation Committee
Delegate Carol L. Krimm, House Chair, Joint Audit and Evaluation Committee
Members of Joint Audit and Evaluation Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Department of Information Technology (DoIT) for the period beginning July 1, 2015 and ending May 6, 2018. DoIT is responsible for the State's information technology policies, provides information technology technical assistance, and oversees the implementation of major information technology development projects (MITDPs) 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. Furthermore, in fiscal year 2015, DoIT began the Enterprise Technology Support Services Initiative for certain Executive Branch agencies, which supports fundamental daily agency information technology activities including Internet and Statewide Intranet access, email, computer server operations, and file sharing.

Our audit disclosed certain deficiencies with DoIT's processes for overseeing the State's 47 MITDPs valued at $1.6 billion that existed as of June 2018. DoIT lacked documentation that it effectively monitored MITDPs through its review of annual status reports and other monthly monitoring activities. For example, our test of fiscal year 2019 annual status reports for four projects estimated to cost $645.7 million disclosed that DoIT did not document its review and approval of any of these reports, and critical information had not been updated in the annual status reports from the preceding year for three of the projects estimated to cost $471.1 million. DoIT also had not established a process to independently evaluate the performance of the vendor-supplied oversight project managers (OPMs) who were tasked with overseeing the projects. For one of these projects,

the Shared Human Services Platform (MD THINK), we noted certain issues regarding project costs and timeliness. As a result of our overall observations, our Office is planning to initiate a special review of the MD THINK project in the near future, which may also include DoIT's MITDP processes.

DoIT did not adequately monitor contracts for one program. Specifically, DoIT contracted with a vendor to design and implement the Maryland First Responders Interoperable Radio System Team (Maryland FiRST) under this program, but did not ensure that the vendor complied with certain contractual requirements, such as system functionality, prior to making payments.

Our audit also disclosed certain security control deficiencies relating to the networks and computer resources under DoIT's responsibility. For example, intrusion detection and prevention system coverage did not exist for a substantial amount of untrusted network traffic flowing into the DoIT internal network. Additionally, access to personally identifiable information (PII) for State vendors stored in the State's Financial Management Information System (FMIS) was not adequately restricted, and the PII was accessible to thousands of State employees. DoIT shares responsibility for the operation of FMIS with the Comptroller of Maryland and the Department of Budget and Management.

Furthermore, our audit disclosed deficiencies in a number of other areas of DoIT responsibilities. DoIT did not sufficiently control equipment and monitoring of its contractor for the State's high-speed data network. DoIT also lacked formal written agreements with the 29 State agencies to clarify responsibilities for services it provides to them through the Enterprise Technology Support Services Initiative.

Finally, our audit included a review to determine the status of the seven findings contained in our preceding audit report. We determined that DoIT satisfactorily addressed five of these findings. The remaining two findings are repeated in this report.

DoIT's response to this audit is included as Appendix A to this report. In accordance with State law, we have reviewed the response and, while DoIT generally agrees with the recommendations in this report, we identified a number of instances in which statements in the response conflict with or disagree with the Finding 1 analysis and recommendations. In each instance, we reviewed and reassessed our audit documentation, and reaffirmed the validity of our finding. In accordance with generally accepted government auditing standards, in Appendix B we have included an Auditor's Comment to address DoIT's disagreements. We

will advise the Joint Audit and Evaluation Committee of any outstanding issues that we cannot resolve with DoIT.

Further, the Committee should be aware that the primary basis of disagreement is the extent of DoIT's responsibility for monitoring MITDPs and verifying the accuracy of data reported by State agencies which is ultimately used to report the status of IT projects to the Governor, the Department of Budget and Management and the budget committees of the General Assembly. DoIT contends that the enhanced monitoring and verification processes we are recommending are not required by State statute, nor is it its mission to verify the accuracy of the data reported by State agencies. In our opinion, effective monitoring and oversight includes ensuring the accuracy of reported project status and costs in order to ensure successful project implementation. As noted above, we will be undertaking a special review of the MD THINK project which we anticipate may result in additional insights into the process for monitoring major information technology projects, along with related recommendations for improvements to the process.

We wish to acknowledge the cooperation extended to us during the audit by DoIT and its willingness to address the majority of the audit issues and implement appropriate corrective actions.

Respectfully submitted,

Gregory A. Hook, CPA
Legislative Auditor

Table of Contents

* **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.

The Enterprise Technology Support Services Initiative was implemented beginning in fiscal year 2015. The Initiative supports fundamental day-to-day information technology operations, including internet and Statewide intranet access, email, computer server operations, and file sharing for Executive Branch agencies authorized in law who have chosen to participate.

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 2018, DoIT's expenditures totaled approximately $139.4 million.

Status of Findings From Preceding Audit Report

Our audit also included a review to determine the status of the seven findings contained in our preceding audit report, dated September 12, 2016. As disclosed in Table 1, we determined that DoIT satisfactorily addressed five of these findings. The remaining two findings are repeated in this report.

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

Table 1
Status of Preceding Findings

Preceding Finding	Finding Description	Implementation Status
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.	**Repeated** (Current Finding 1)
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.	**Repeated** (Current Finding 2)
Finding 3	DoIT had not established comprehensive policies for project changes to scope, schedule, or costs (rebaselining) and Independent Verification and Validation assessments.	Not repeated
Finding 4	The DoIT, Department of Budget and Management, and Executive Department – Office of the Governor networks were not properly secured in that certain contractors had been granted unnecessary access and certain security capabilities were not fully used.	Not repeated
Finding 5	Computers covered by DoIT's managed desktop services were not properly maintained and secured with current malware protection.	Not repeated
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.	Not repeated
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.	Not repeated

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 (also referred to in this report as "projects") 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.
- The DoIT 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 defines actions, functions, or activities to be performed for the critical stages of the project, such as planning, implementation, and operation. DoIT's oversight responsibilities generally include (1) reviewing critical project documents, including the management plan, functional requirements documentation, procurement documentation, and system testing plan; (2) reviewing agency project status reports; and (3) determining the necessity of Independent Verification and Validation (IV&V) assessments. Since December 2013, DoIT has contracted with a vendor to hire oversight project managers (OPMs) to provide project oversight services. However, DoIT retains ultimate responsibility.

According to DoIT's records, as of June 30, 2018, there were 47 MITDPs with an estimated cost at completion of approximately $1.6 billion. Seventy-five percent of the value of these projects was for agencies responsible for providing services in the health, education, financial, transportation, and public safety sectors of State government. MITDPs are funded from multiple sources including the State's Major Information Technology Development Project Fund, which DoIT administers. According to DoIT's records, Fund expenditures totaled approximately $18.7 million during fiscal year 2018, including $2.4 million for project oversight.

We reviewed DoIT's oversight of the following four MITDPs:

Table 2
Summary of MITDPs Tested
(amounts in millions)

MITDP	Agency	Estimated Cost at Completion	Cost as of June 30, 2018
Statewide Personnel System (SPS)	Department of Budget and Management	$81.2	$73.3
Shared Human Services Platform (MD THINK)	Department of Human Services	314.1	59.6
Long Term Support Services Tracking System (LTSS)	Maryland Department of Health	174.6	55.5
Unemployment Insurance Modernization (UIM)	Maryland Department of Labor	75.8	38.6
Total		**$645.7**	**$227.0**

Sources: Fiscal Year 2019 Information Technology Project Requests (ITPR) for "Estimated Cost at Completion," and Fiscal Year 2018 MITDP Annual Report for "Cost as of June 30, 2018."

Finding 1
DoIT lacked sufficient documentation that it effectively monitored MITDPs through its review of annual MITDP status reports and monthly monitoring activities. In addition, DoIT did not always accurately report estimated project costs in its annual report to State officials, as required.

Analysis
DoIT lacked sufficient documentation to support that it effectively monitored MITDPs and did not always accurately report the estimated project costs to the Governor, DBM, and the Maryland General Assembly, as required.

Information Technology Project Requests (ITPRs)

DoIT did not have a documented review and approval process for agencies' annual project status reports, known as ITPRs, and was not ensuring that ITPRs contained current information. 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. For all approved projects, State law requires an initial ITPR submission to DoIT, and DoIT requires agencies to submit subsequent ITPRs on an annual basis throughout the MITDP's life cycle. Specifically, each agency submits an ITPR to DoIT and, DoIT, in conjunction with its OPMs, is to review and approve the ITPR to ensure the accuracy of the cost data and projected spending. However, DoIT did not document its review and approval prior to submitting the agencies' annual ITPRs to DBM and the Department of Legislative Services for budget analysis purposes.

Our test of the ITPRs submitted for the four projects noted in Table 2 during fiscal year 2018 (for fiscal year 2019) disclosed that DoIT did not document its or the OPMs' review and approval of any of these ITPRs. Based on our test, the review of these ITPRs appeared deficient. Specifically, certain critical information for three projects (SPS, MD THINK, UIM), with estimated completion costs totaling $471.1 million, had not been updated from the preceding year's ITPR.

For example, for one project (MD THINK), the estimated $314.1 million cost of completion had increased by $141.1 million (81.5 percent) from the preceding year's (fiscal year 2018) ITPR, but an explanation was not provided for the increase, such as a change in the project scope. DoIT advised us that the increased project cost was primarily due to the omission in the preceding year's ITPR of costs expected to be incurred in future years, which in itself provides another example of the deficiency of DoIT's review process. In addition, DoIT also advised us that it does not always review the estimated cost of completion for project costs reported in the ITPRs.[2]

[2] During another audit, we noted certain other issues regarding MD THINK project costs and timeliness. There is also a steering committee consisting of high ranking officials from seven State agencies, including the secretaries of DoIT, DHS, and DBM, that has a significant role and responsibilities over this project. As a result, and in consideration of the increasing project costs, we are planning to initiate a special review of this project and the committee's oversight in the near future, which may include other DoIT MITDP-related processes.

Monthly Project Monitoring

DoIT did not require the OPMs, hired by a DoIT vendor, to document their review and verification of the accuracy of information provided in monthly project monitoring reports provided by the agencies. The review of these monthly monitoring reports is critical to monitoring project status including scope, schedule, cost, and risks. Also, DoIT's failure to develop specific documentation and reporting requirements for the OPMs could hinder DoIT efforts to evaluate the effectiveness of the OPMs' performance (see Finding 2 for further comments regarding evaluation of OPM performance).

DoIT advised us that it requires monthly status reports and steering committee[3] meetings, which OPMs were also responsible for attending, for certain more complex projects, at its discretion. Our review of applicable reports discussed during fiscal year 2018 meetings for two of the four tested projects (MD THINK and UIM) totaling $389.9 million disclosed that the actions to be taken to address identified risks, such as project delays, were not always included in the reports, and DoIT did not document that methods to address these risks were discussed in the related meetings. The steering committees included DoIT management and management from the agencies affected by the project.

Annual Report

In its fiscal year 2018 annual report, DoIT did not properly report total estimated project costs for the MD THINK and UIM projects. Based on our review of project documents and discussions with DoIT management, we determined that DoIT understated the total estimated project costs for those two projects by $64.4 million. DoIT advised us that it reported decreases in estimated costs because of delays in these projects; however, we determined that not all estimated future costs were included in the annual report.

State law requires an annual report to be submitted to the Governor, DBM, and the budget committees of the Maryland General Assembly on or before November 1 of each year. For each MITDP, the report is required to include (1) the status of the project; (2) a comparison of the estimated and actual costs of the project; (3) any known or anticipated changes in scope or costs of the project; (4) an evaluation of whether the project is using best practices; and (5) a summary of any monitoring and oversight of the project from outside the agency in which the project is being developed, including a description of any problems identified by an external review and any corrective actions taken.

[3] Most significant IT projects have a steering committee of relevant high level State officials established to oversee a project's development and implementation.

Similar conditions regarding the lack of sufficient documentation of project monitoring efforts have been commented upon in our three preceding audit reports.

Recommendation 1
We recommend that DoIT

a. **ensure project status information reported on ITPRs is current and complete as part of its annual review and approval process (repeat), and the approval is documented;**
b. **require the OPMs to document their review and verification of the accuracy of monthly project monitoring reports (repeat);**
c. **ensure that recommended actions to address identified risks are discussed at applicable meetings and documented (repeat); and**
d. **ensure that annual reports include accurate estimated costs to complete.**

Finding 2
DoIT had not established a process to independently evaluate OPMs hired through a vendor to oversee MITDPs.

Analysis
DoIT had not established a process to independently evaluate the performance of the OPMs supplied by its third-party vendor to monitor assigned MITDPs. Consequently, assurance was lacking that the OPMs were effectively monitoring the development and implementation of all 47 MITDPs valued at $1.6 billion as of June 30, 2018.

During the audit period, DoIT did not conduct performance evaluations of the OPMs hired by its vendor to independently assess whether OPMs 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 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 monthly project status report meetings. A similar condition was commented upon in our preceding audit report.

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 $13.7 million as of September 2018.

Recommendation 2
We recommend that DoIT conduct periodic performance evaluations of the OPMs to help ensure MITDPs are being effectively monitored (repeat).

Statewide Communications Interoperability Program

Background

The Maryland Statewide Communications Interoperability Program was established through an Executive Order issued in July 2008. The Executive Order was intended to enhance public safety communications infrastructure and interoperability throughout the State, through the implementation of several projects. Interoperable communications is the ability for first responders to transmit voice and data communications in real time, regardless of agency or jurisdictional boundary.

As provided for in the Executive Order, the State established a Statewide radio system, known as Maryland First Responders Interoperable Radio System Team (Maryland FiRST), using the 700 MHz band of frequencies to allow voice and data communications between State, county, and local users of the system for day-to-day operations and in the event of an emergency. DoIT contracted with a vendor in November 2010 to design and implement Maryland FiRST. The contract was originally valued at $485 million (eight-year base period valued at $345 million, plus seven one-year options for operations and maintenance valued at $140 million). Originally, the contract required the Maryland FiRST vendor to complete the project by November 2018. However, according to DoIT's fiscal year 2018 capital budget testimony, the project experienced delays resulting from cost containment measures as well as issues with equipment that was not performing to the State's satisfaction and was replaced by the vendor at no additional cost.

As of February 2018, as a result of various modifications, the total contract value was $406 million. This reflected a 12-year base period through November 2022 valued at $331 million; maintenance during the base period, totaling an additional $55 million; and a one-year option for operations and maintenance valued at $20 million. Costs (by cost component) for both the original and amended contracts

are reflected in Table 3. DoIT advised us that it plans to procure a separate contract for ongoing operations and maintenance costs after the current contract term.

Table 3
Maryland FiRST Original and Amended Contract Costs

Cost Components	Original Contract *(November 2010)*	Amended Contract *(as of February 2018)*
Infrastructure and Contingency	$230,135,125	$257,081,499
Subscriber Equipment	114,864,875	73,864,875
Subtotal	**$345,000,000**	**$330,946,374**
Operations and Maintenance*	140,000,000	75,053,626
Total	**$485,000,000**	**$406,000,000**

Source: Contract Documents

* The value of the Operations and Maintenance cost in the original contract was for 7 years after all phases were operational. The value of these cost in the amended contract is for 1 year, as well as for maintenance as phases became operational.

The Maryland FiRST project comprises five phases by geographical regions throughout the State. As of December 31, 2018, four phases had been completed, and work was in progress for Phase 5 - the National Capital and Southern Maryland Region. This Region is expected to be fully operational by the end of September 2020. According to State records, Maryland FiRST contract expenditures totaled $286.3 million as of January 2019.

Finding 3
DoIT did not ensure that the Maryland FiRST vendor met certain contractual requirements related to radio coverage nor did it ensure contract milestones regarding radio coverage testing were completed prior to payment.

Analysis
DoIT did not ensure that the Maryland FiRST vendor met certain contractual requirements related to radio coverage nor ensure contract milestones regarding radio coverage testing were completed prior to payment. In general, contract

payments were to be made based on completed milestones (such as, design, construction, and testing) within each phase (established geographic area). Specifically, our review of the Western Maryland phase of the contract (which was completed in December 2018) disclosed that DoIT accepted coverage levels below the contractual requirements and did not ensure all testing requirements were met prior to making payments. We tested two payments totaling $3.9 million for completion of two separate radio coverage tests (system functionality and radio frequency) in Washington County.

- For the radio frequency test, DoIT accepted the Washington County coverage testing result of 74.5 percent, even though the minimum acceptable radio communications coverage for the Western Maryland phase was 86.5 percent. DoIT management advised us that it accepted these testing results for the purpose of approving contractor performance under the assumption that the entire Western Maryland phase results, once measured, would meet the minimum coverage requirement. However, the final in-building testing reports for the entire Western Maryland phase resulted in coverage testing of 85.5 percent and the vendor was not required to take additional actions to meet the minimum acceptable coverage.

- DoIT could not document that it received one test plan and that it had approved the other test plan. The vendor was required to submit test plans to DoIT, that were specific to the region or county tested, so that DoIT could ensure the tests were appropriately designed to measure achievement of the acceptable radio communication quality.

- DoIT did not document its approval to waive radio coverage testing in certain geographic areas as required by the contract. Specifically, the vendor did not test 668 of the 3,748 one square mile units within the Western Maryland phase. DoIT advised us that certain units were not tested because the vendor deemed them to be inaccessible (for example, property owners did not grant access), but DoIT did not document its approval to waive the testing, as required by the contract. Given the large area that was excluded from testing (18 percent), there is a lack of assurance the reported coverage testing result of 85.5 percent for the phase was valid.

Recommendation 3
We recommend DoIT

a. monitor the contract to ensure that the vendor complied with contract requirements, including radio coverage, unless appropriately waived; and
b. obtain and review documentation to support that contract deliverables (milestones) were satisfactorily met prior to making related payments.

Finding 4
DoIT did not adequately monitor the construction of a tower and ensure that the related payments totaling $1.4 million were proper.

Analysis
DoIT did not adequately monitor the construction of a tower and ensure that the related payments were proper. In addition, DoIT did not require the vendor to pay liquidated damages totaling $47,600 for delays in completion of the construction as allowed by the contract. DoIT contracted with additional vendors for certain Maryland FiRST infrastructure needs. We reviewed one of these infrastructure contracts to construct a tower for which DoIT made payments totaling approximately $1.4 million.

- DoIT did not obtain tower construction inspection services and materials testing during the construction process as required. In addition, documentation of DoIT's final inspection of the completed tower site appeared questionable. Specifically, the inspection report we initially reviewed in the project file did not include information to identify the tower site, the inspection date, and the name of the inspector. After bringing this to DoIT's attention, DoIT provided us with a completed inspection report dated August 10, 2017. However, according to the vendor's documentation, the tower was completed on September 6, 2017, about one month later. As a result, there is a lack of assurance that construction of the tower was properly completed.

- DoIT did not have an adequate process to ensure that the vendor completed the required work in a timely and satisfactory manner prior to approving invoices for payment. Required notices of milestone completion and weekly detailed project schedules were not received from the vendor, and delivery acceptance forms were not prepared by DoIT for any of the 16 milestones included in the four payments tested totaling $1.4 million.

- DoIT did not require the vendor to pay liquidated damages for delays in completion of the construction as allowed by the contract. The contract required the vendor to complete all work on the contract by June 30, 2017 and also stated that completion of the tower in a timely manner was essential. According to available documentation, the vendor completed the work on September 6, 2017, which was a delay of 68 days. Since the contract provided that liquidated damages of $700 could be assessed for each day any work remained uncompleted, DoIT could have assessed liquidated damages totaling $47,600. DoIT could not explain the reasons for this delay, but stated

that liquidated damages had not been assessed since the vendor had informally been given more time to complete the project.

Recommendation 4
For all tower construction services contracts, we recommend DoIT

a. ensure all required inspections are performed and properly documented,
b. ensure work is completed in accordance with the contract prior to approval of invoices for payment, and
c. assess applicable liquidated damages when appropriate.

Information Systems Security and Control

Background

DoIT has Statewide Information Technology (IT) responsibilities as well as responsibilities for managed shared services, for numerous agencies as follows:

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

- DoIT supports statewide applications such as the Financial Management Information System, personnel system, and employee benefit system.[4] DoIT also supports a cloud computing, productivity and collaboration software service widely used by Executive Branch agencies. Additionally, DoIT manages an eGovernment service utilized by various State agencies to provide customers with web-enabled transaction processing and other supporting services.

- DoIT provides various managed shared services to numerous Executive Branch agencies involving IT security and computer hosting. These functions include managed security services for maintaining agencies networks' firewalls; end user services for supporting agencies computer workstations, providing malware protection software, encryption and host intrusion prevention system software; and Infrastructure Services for hosting agency virtual servers at a third-party service provider's hosting data center, and managing agencies' onsite and branch locations' local area networks including wireless network segments.[5]

[4] 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.

[5] The Office of Legislative Audits examined controls for these managed shared services within a separate audit conducted of DoIT as a service provider.

- DoIT operates and secures its own agency-level IT infrastructure, by making use of the same DoIT managed shared services that are applied on behalf of various other Executive Branch agencies.

Our current audit of DoIT focused on reviewing security controls over certain DoIT Statewide responsibilities, monitoring procedures for the cloud collaboration software and eGovernment software services, and DoIT's usage of its own managed services for securing its network.

Finding 5
Intrusion detection and prevention system (IDPS) coverage did not exist for a substantial amount of untrusted network traffic flowing into DoIT's internal network.

Analysis
IDPS coverage did not exist for a substantial amount of untrusted network traffic flowing into DoIT's internal network. Specifically, network device based IDPS inspection coverage did not occur for the untrusted traffic. We identified 55 firewall rules that allowed traffic from any source to 71 unique network destinations as well as a small network segment within DoIT's internal network without IDPS coverage. The absence of IDPS coverage for such untrusted traffic creates increased network security risk, as such traffic could contain undetected malicious data.

The State of Maryland *Information Technology Security Manual* requires protection against malicious code and attacks by using IDPS coverage to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information. Strong network security uses a layered approach, relying on various resources, and is structured according to assessed network security risk. Properly configured IDPS protection can aid significantly in the detection/prevention of, and response to, potential network security breaches and attacks.

Recommendation 5
We recommend that DoIT ensure that network-based IDPS protection exists for all critical portions of its internal network, by including IDPS coverage for untrusted external traffic flowing to its internal network resources.

Finding 6
DoIT lacked assurance that adequate information technology security and operational controls existed over its managed cloud collaboration and eGovernment software systems that were hosted, operated, and maintained by service providers.

Analysis
DoIT lacked assurance that adequate information technology security and operational controls existed over its managed cloud collaboration and eGovernment software systems that were hosted, operated, and maintained by service providers. Specifically, DoIT could not provide evidence that it had performed reviews of available independent security review reports related to these systems.

Our review for the cloud collaboration system determined that DoIT had obtained the service provider's most recent System and Organization Controls (SOC) 2 Type 2 report. DoIT personnel advised us that this SOC report was reviewed; however, that review was not documented. For the eGovernment system, DoIT could not provide evidence that the service provider's SOC reports for the periods ending June 30, 2016 and June 30, 2017 had been obtained and reviewed. DoIT advised us that personnel turnover had caused the responsibility for reviews of these reports to shift among its personnel, and that completion of the necessary reviews could not be verified. After our inquiries, DoIT obtained the SOC reports related to the eGovernment system. Our review concluded that none of the aforementioned SOC reports disclosed any significant control weaknesses.

The American Institute of Certified Public Accountants has issued guidance concerning examinations of service providers. Based on this guidance, service providers may contract for an independent review of controls and resultant independent auditor's report referred to as a SOC report. There are several types of SOC reports, with varying scopes and levels of review and auditor testing. One type of report, referred to as a SOC 2 Type 2 report for Service Organizations, contains the service organization's description of its system and the results of the auditor's examination of the suitability of the system design and operating effectiveness for the period under review, and can include an evaluation of system security, data availability, processing integrity, confidentiality, and privacy trust services criteria.

Recommendation 6
We recommend that DoIT, for its managed cloud collaboration and eGovernment software systems,

a. **timely obtain and review copies of SOC 2 Type 2 reports, including any needed reports for prior periods, and verify that the related service providers implement all critical report recommendations; and**
b. **document the aforementioned reviews and retain them for future reference.**

Financial Management Information System

Background

The Financial Management Information System (FMIS) is an integrated database system that runs on the Comptroller of Maryland's Annapolis Data Center's computers and supports individual agency and Statewide purchasing and accounting operations. According to the State's accounting records, expenditures processed through FMIS for fiscal year 2018, before fiscal year-end closing adjustments, totaled approximately $34.7 billion (including State agencies that use their own computer systems, but interface with FMIS).

The State implemented FMIS in 1992 to replace separate accounting systems maintained by the Comptroller and DBM. In July 2008, in accordance with State law, the Office of Information Technology was removed from DBM and established as an independent department of the State—the Department of Information Technology (DoIT). Also in July 2008, a memorandum of understanding (MOU) between DBM and DoIT established DBM as the owner of FMIS and required DoIT to provide certain support services to DBM's financial applications, including FMIS.

That MOU was superseded in 2009 by an Operating Agreement between the Comptroller, DoIT, and DBM in which it was agreed that the three control agencies would actively engage in the functional and technical support associated with the enhancement, maintenance, documentation, operation, replacement, and disposition of the State's Relational Standard Accounting and Reporting System, which is one of the two components of FMIS. That Agreement also states that DoIT is responsible for information technology standards and procedures and the management of all system development life cycle tasks, including enhancements and exhibiting control over the system security, and that the Comptroller has final approval authority for any core enhancements or modifications of accounting and/or reporting functions. To the extent that third-party reviews, such as those conducted by the Office of Legislative Audits, identify items related to the integrity of system controls, DBM and DoIT are to provide the Comptroller an action plan to resolve such issues and a monthly progress report until all issues are resolved.

Finding 7
Personally identifiable information (PII) was not adequately restricted in the State's FMIS and was visible to 5,204 employees Statewide.

Analysis
DoIT, in conjunction with DBM and the Comptroller of Maryland, did not ensure that access to vendor PII stored in FMIS was adequately restricted and that this PII was otherwise safeguarded. Specifically, certain PII was displayed in FMIS in plain text on-line or in reports generated by FMIS. While we did not perform a comprehensive review, we readily identified at least 9 FMIS screens and 13 FMIS reports containing vendor PII that were available to FMIS users throughout the State. As of August 2018, based on FMIS records, there were 5,204 State employees with access to FMIS and, therefore, depending on their access level, these users potentially had access to the sensitive PII.

As of May 2019, there were approximately 398,000 Statewide vendors in FMIS with PII, although there could be some duplication of vendors within this total number. The number of Statewide vendors excludes approximately 117,000 vendors which are State employees for which certain restrictions exist to limit access to their PII.

We believe that this situation represents a critical PII issue that requires a collective corrective action plan from the responsible agencies. Consequently, it is incumbent upon the three control agencies (the Comptroller, DoIT, and DBM) to ensure that PII in FMIS is adequately restricted and safeguarded, including determining whether practical alternatives to using PII in FMIS exist. The Comptroller of Maryland's *Accounting Procedures Manual* instructs agencies to restrict access to certain PII to the extent practical. In addition, the State of Maryland *Information Technology Security Manual* requires that agencies ensure that access to confidential information is strictly controlled and audited and that it supports the concept of "least privilege" allowing only authorized access to accomplish assigned tasks.

We were advised by DBM's legal counsel that, in accordance with the July 2008 law creating DoIT, the responsibility for changes to FMIS, including any changes required to address the PII security issue, had been transferred to DoIT. DoIT's legal counsel subsequently advised us that DoIT is required to confer with DBM and the Comptroller prior to any changes that impact FMIS accounting functions, procedures, or business operations.

Recommendation 7
We recommend that DoIT, in conjunction with the Comptroller and DBM, take the necessary steps to adequately restrict and safeguard PII in FMIS.

Contracts

Finding 8
DoIT did not adequately monitor task order payments and did not obtain support for the related invoices from its networkMaryland vendor for which payments totaled $56.8 million.

Analysis
DoIT did not adequately monitor task order payments and did not obtain documentation to support invoices received from its vendor that maintains the State's high-speed data network for public sector use, known as networkMaryland. DoIT contracted with this vendor to provide management and operations services relating to data networks and support, security, network engineering, and fiber optic construction, design, engineering, and repair for networkMaryland. The contract award and subsequent modification totaled $71.5 million for the period from April 1, 2015 through March 31, 2020. According to State records, as of November 8, 2018, DoIT had paid approximately $56.8 million to the vendor.

- DoIT did not obtain documentation to ensure that goods and services were received in a satisfactory manner and labor hours billed were accurate prior to approving invoices for payment. Specifically, DoIT did not obtain and review documentation (such as, receiving reports, written plans, and site diagrams) nor perform inspections to support that services were received as requested. In addition, DoIT did not obtain timesheets, which were required to be provided by the vendor, to verify hours billed.

- DoIT did not maintain a record of amounts spent for each task order to ensure that payments did not exceed the approved task order amount. Instead, the vendor maintained this task order payment information and provided it to DoIT periodically. We reviewed the vendor records associated with 690 time and material task orders for the period from December 5, 2016 through October 29, 2018 totaling $11.0 million. Based on our review, we identified 14 task orders totaling $551,600 for which DoIT had paid $711,000, exceeding the approved amounts by $159,400. For example, for 4 of these task orders, valued at $84,700, DoIT made payments totaling $158,000. DoIT was unable to provide

documentation for or explain why payments exceeded the approved task order amounts by $73,300.

Recommendation 8
We recommend DoIT

a. obtain documentation to ensure that goods and services are received in a satisfactory manner prior to approving invoice payments;
b. obtain timesheets from the vendor and compare them to hours billed, at least on a test basis, to ensure labor hours billed are supported;
c. maintain a record of amounts spent for each task and ensure payments do not exceed the related task order; and
d. investigate the aforementioned task order payments that exceeded the approved amounts, and take any appropriate action.

Enterprise Technology Support Services Initiative

Background

The Enterprise Technology Support Services Initiative was implemented beginning in fiscal year 2015. The Initiative supports fundamental day-to-day IT operations, including Internet and Statewide Intranet access, email, computer server operations, and file sharing for Executive Branch agencies authorized in law who have chosen to participate.

During implementation of the Initiative, numerous IT employee positions were transferred from various State agencies to DoIT. DoIT has also relied, to a significant degree, on a contractor for providing personnel and technical expertise related to varying portions of the Initiative services.

As of February 2019, according to its records, DoIT was providing services under the Initiative to 29 State agencies, with more than 9,000 employees.

Finding 9
DoIT lacked formal written agreements with the 29 participating State agencies to clarify responsibilities of technology support services performed by DoIT and the reimbursement of related costs.

Analysis

DoIT did not enter into a formal written memorandum of understanding (MOU) with any of the 29 participating State agencies whose IT services it supported through the Initiative. An executed MOU is critical to clarify and obtain

agreement regarding each agency's IT responsibilities, including the associated costs.

In particular, the MOUs should specify DoIT's support services provided, the State agencies' IT responsibilities, and how the costs for DoIT's support services should be determined, documented, and reimbursed. Additionally, a formal MOU is necessary to ensure oversight of all agency-critical systems and should specify which agency is responsible for each IT system. For example, while DoIT may be responsible for the day-to-day IT operations of an agency, certain agencies retain responsibility for unique systems that are critical for the agency's mission.

DoIT incurred unreimbursed IT service costs for software upgrades and equipment purchases it made on behalf of other State agencies. Based on our discussions with DoIT management personnel, it appears DoIT did not obtain reimbursement from these agencies because of the lack of clarity regarding financial responsibility for the costs. An MOU would have clarified this financial responsibility. As a result, DoIT requested and obtained deficiency appropriations totaling approximately $10 million for amounts spent in excess of its appropriations for fiscal years 2017 through 2019.

Recommendation 9
We recommend DoIT enter into formal MOUs with all agencies for which it provides services as part of the Enterprise Technology Support Services Initiative. The MOU should clarify DoIT and agency responsibilities, specific services to be provided by each, and a mechanism to provide for the cost of these services.

Equipment

Finding 10
DoIT did not adequately control its equipment inventory and did not maintain accurate detail records.

Analysis
DoIT did not have adequate procedures and controls over its equipment inventory and did not maintain accurate records. DoIT reported equipment valued at $51.4 million to the Department of General Services (DGS) as of June 30, 2018. A majority of this equipment value related to networkMaryland and Maryland FiRST for which the equipment records were maintained by the related vendors.

- DoIT did not ensure that equipment purchases were properly recorded in the detail records and were properly installed and tagged. For example, we reviewed DoIT's August 2017 purchases of 1,101 computers, costing $731,000, which were delivered directly to the Maryland Department of Health (MDH). We noted that DoIT did not record any of these items in its detail records and, at the time of our audit, neither DoIT nor MDH were able to locate 605 of these computers.

- DoIT did not ensure annual physical inventories of DoIT equipment were properly and timely performed as required. For example, as of July 2018, our review of the detail Maryland FiRST equipment records indicated the vendor did not conduct a physical inventory during fiscal year 2018, and only a small number of items were inventoried in fiscal year 2017. Additionally, DoIT's physical inventory of certain other IT equipment was performed by an individual who had the capability to adjust the detail records, and therefore was not independent.

- DoIT did not accurately report equipment inventory to DGS. For example, our review of the $51.1 million equipment value DoIT reported in fiscal year 2017 disclosed that DoIT did not separately report equipment additions and disposals. Rather, DoIT combined them and reported net additions totaling $523,175. Furthermore, according to the State's accounting records, DoIT purchased $8.7 million of new and replacement equipment during that period.

The DGS *Inventory Control Manual* requires State agencies to accurately report and safeguard equipment, maintain comprehensive detail records and an independent control account, and conduct a physical inventory of sensitive equipment at least once a year including investigating any discrepancies.

Recommendation 10
We recommend that DoIT comply with the requirements of the DGS *Inventory Control Manual*.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Department of Information Technology (DoIT) for the period beginning July 1, 2015 and ending May 6, 2018. 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, as well as procurement and monitoring of other contracts, information systems security and controls, the Enterprise Technology Support Initiative, and DoIT's operating expenses. We also determined the status of the seven findings contained in our preceding audit report dated September 12, 2016.

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 human resources, 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. In addition, we extracted data from other systems maintained by DoIT or its contractors for the purpose of selecting items for testing. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the 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. As provided in *Government Auditing Standards*, there are five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring. Each of the five components, when significant to the audit objectives, and as applicable to DoIT, were considered by us during the course of this audit.

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 A

See Appendix B for auditor's comment

Maryland DEPARTMENT OF INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

April 3, 2020

Gregory A. Hook, CPA
Legislative Auditor
301 W. Preston Street, Room 1202
Baltimore, MD 21201

Dear Mr. Hook:

The Department of Information Technology (DoIT) has received the fiscal compliance audit submitted by the Department of Legislative Services, Office of Legislative Audits, dated March 11, 2020. This audit included a fiscal internal control review for the period beginning July 1, 2015 and ending May 6, 2018.

DoIT acknowledges the efforts of the legislative auditors during this audit. Responses to the audit findings are attached to this cover letter.

Sincerely,

DocuSigned by:
Michael G. Leahy
7820D075CBE64C5...

Michael G. Leahy
Secretary, Department of Information Technology

Department of Information Technology

Agency Response Form

Major Information Technology Development Projects

Finding 1
DoIT lacked sufficient documentation that it effectively monitored MITDPs through its review of annual MITDP status reports and monthly monitoring activities. In addition, DoIT did not always accurately report estimated project costs in its annual report to State officials, as required.

We recommend that DoIT

a. ensure project status information reported on ITPRs is current and complete as part of its annual review and approval process (repeat), and the approval is documented;
b. require the OPMs to document their review and verification of the accuracy of monthly project monitoring reports (repeat);
c. ensure that recommended actions to address identified risks are discussed at applicable meetings and documented (repeat); and
d. ensure that its annual reports include accurate estimated costs to complete.

Agency Response	
Analysis	
General Comment	*The Department of Information Technology (Department) thanks the Office of Legislative Audits (OLA) for this review and analysis of the Department's Major Information Technology Development Project (MITDP) program, frequently called the Enterprise Program Management Office (EPMO). This analysis includes a wealth of information that will help the Department improve the quality of the service it offers to the legislature and the people of Maryland.* *The Department takes its role of overseeing, monitoring, and reporting on MITDPs very seriously. Using available resources, the Department has sufficient processes in place that fulfill its oversight responsibilities of MITDPs, consistent with statute, to monitor and properly provide insight and guidance to agencies as well as to provide effective and appropriate reporting to the applicable parties, including the legislature. Thus, the Department agrees with the auditors that it has an oversight and monitoring responsibility related to MITDPs; we disagree with the detailed level of related tasks that OLA has taken issue with and is recommending.* ***I. The "monthly project reporting" is an informal tool utilized in the MITDP process. It is a self-reporting tool provided by the unit and used by the Department for data gathering purposes on certain MITDPs.*** *The Maryland Code requires that covered units of state government submit technology requests to the Department for review. The Secretary reviews these*

	requests and may deem a request as major. When a technology initiative is officially declared by the Secretary as major, it becomes an MITDP. The statute then sets forth certain reporting and oversight requirements that the Department and covered units must follow. One of these requirements is the submission of an Information Technology Project Request (ITPR) at MITDP inception. Subsequent ITPR submissions are then required annually to provide updates. The Department compiles and transmits information concerning these ITPRs to the legislature at the commencement of each regular legislative session. Prior to approval and transmission to the legislature, the Department carefully reviews all ITPRs. This process is discussed further in the Department's response to recommendation 1a. *The Department embraces its role in MITDP monitoring as an oversight function. Certain practices, such as the "monthly project reporting" noted in the auditor's analysis, may be a tool used in MITDP oversight, but these are not instituted as a policy or official Department requirement and are not uniformly employed for all MITDPs. The cadence of information gathering is developed individually, per MITDP, based upon the oversight needs of the MITDP. The periodic meetings should be recognized as individual targeted data collection efforts, tailored per MITDP, designed to elicit information that improves the quality of the statutorily required reporting. EPMO collects a substantial body of data in many different manners as part of its ongoing efforts to monitor the MITDP portfolio. Information gathering is intended to track a unit's MITDP progress and provides inputs to other activities such as the OPM monthly health checks and the annual ITPR planning.* *Documenting their review of the monthly project reporting provided by the unit is not be the most efficient use of the EPMO resources. Furthermore, the lack of requiring such document does not hinder the Department's efforts in evaluating the OPMs' performance. (The Department has established a process to evaluate OPM performance, as noted in the response to Finding 2.)* *EPMO has adopted documentation and reporting requirements, adopting a model like other state governments and other large multi-organizational unit enterprises that employ an EPMO function. In particular, the OPMs are required to provide monthly health reports to the Secretary, that provide an assessment made by the OPM of the MITDP health based on the information gathered during that month. In the monthly health check meetings, OPMs submit reports and present an analysis of each MITDP to the Secretary. This approach keeps the Secretary fully informed of key factors, including risks and issues that affect the health of MITDPs. The monthly health checks are the main method of documenting the Department's efforts to oversee the MITDP portfolio and serves as an effective management tool in the Department's efforts to improve the health posture of the MITDP portfolio.* ***II. The Department role in financial oversight is limited.***

Agency Response Form

	The Department's role is that of a technical subject matter expert. Therefore, the Department's oversight focuses primarily on factors that influence the technical efficiency of the MITDP, including such things as spending plans and contractor performance against required deliverables. The Department does not possess access to financial records, including those maintained in the State's Financial Management Information System (FMIS), as these are maintained at the unit operating the MITDP. The state financial management processes were constructed in a manner that allows a unit operating an MITDP to expend funds without the Department's prior approval, and the Department transfers funds to the other unit after the fact. The Department sees benefits in the establishment of processes that require other units operating MITDPs to obtain approval from the Department prior to the encumbrance or expenditure of MITDP funds; however, these changes are complex, may require significant investment to implement, and require the cooperation of a number of parties outside of the Department. *The Department does perform limited examinations of financial records to ensure the technical efficiency of an MITDP. From time to time, the Department may discover inconsistencies in a unit's MITDP financial data submission. When this occurs, the Department refers the observation to appropriate parties accountable for the financial management practices of that MITDP. The EPMO does not engage in an extensive verification of financial records, does not possess the resources or access to detail information to perform such activities, and the Department does not agree that its mission includes the auditing of financial data.*		
Recommendation 1a	Agree	**Estimated Completion Date:**	Complete
	We <u>CONCUR WITH FURTHER EXPLANATION; this finding has been resolved.</u> *In July 2018, the Department implemented a system called PRISM that provides a thorough, documented review process for units' new MITDP submissions and annual project requests. PRISM provides a unit approval process that assures the unit CIO and Executive Sponsor provide their acceptance of the information being submitted. Once a new MITDP or annual update is received, PRISM provides an acknowledgement that the Department has received the unit's submission. The results of the ITPR analysis are brought forward to the Secretary. Any new projects meeting certain criteria as defined in statute are approved as MITDPs. New MITDPs and annual updates are approved by the Secretary prior to submission to the legislature. Because the core function of an EPMO is to provide a framework for program and project management and then to monitor performance to that framework, the Department depends upon units for accuracy in their reporting. Indeed, the submission of an MITDP project request, commonly known as an ITPR, must be approved by an executive of the unit who possesses appropriate authority as an attest to the accuracy of the submission. While the Department does from*		

	time to time perform targeted collections of data and analysis pertaining to MITDP submissions, which may include periodic meetings, the Department disagrees that targeted investigations are uniformly necessary, or that they should be performed in a structured manner. MITDPs vary greatly, and the application of a uniform structure to monitoring would be detrimental to the mission of the EPMO. Instead, EPMO tailors the monitoring and reporting activities to each MITDP. ***Review and Approval Steps of the ITPR process*** *Below are the steps taken in the review and approval stage of the ITPR process, demonstrating that the Department's activities are compliant with statute and meet the needs of the Department's mission.* *Activities performed by the Department's EPMO* *The EPMO is the division within the Department responsible for executing the day to day activities related to statutory requirements pertaining to MITDPs. The EPMO receives and analyzes ITPR submissions and provides advice to the Secretary. This includes, by way of example but not limitation to, activities such as calling meetings with unit IT personnel to discuss an ITPR submission, researching details pertinent to an ITPR submission, or requesting further elaboration of details contained in an ITPR submission. The EPMO does not perform project management work, such as the initiation, planning, executing, controlling, and closing of projects. The project management work is performed by a delivery project manager or delivery Program Management Office (PMO) operating within the unit whose technology request was deemed to be an MITDP.* *Activities performed by the Secretary* *While EPMO performs a variety of oversight tasks, it does not possess the authority to approve ITPR submissions. This authority remains fully vested with the Secretary. The Secretary performs two functions pertinent to review and approval. First, the Secretary reviews and approves ITPR submissions upon initial receipt and issues a declaration that an initiative is an MITDP. Information gathering that supports this review is supported via the Department's Project Request Information Systems Management (PRISM) service, located at https://prism.doit.maryland.gov/. Since the inception of PRISM, the ITPR collection and approval process has been fully automated and documented, terminating in either or both of a MITDP determination letter issued by the Secretary, or an annual MITDP submission to the legislature. Second, the Secretary receives each fully packaged annual MITDP submission to be delivered to the legislature, which comprises key elements from all ITPR submissions. This package is carefully reviewed and approved by the Secretary. This process is documented via correspondence.* ***While this finding has been labeled a repeat; the Department would like it to be acknowledged that corrective actions are already implemented, and were implemented in the most expeditious manner possible.***

Agency Response Form

	The Department received OLA's audit report dated September, 2016, in which OLA stated that the Department "lacked sufficient documentation supporting its reviews of annual MITDP status reports". Without delay, the Department embarked upon an effort to automate the approval process. This effort began in earnest in July, 2017 when funding was provided, and concluded at the beginning of the following MITDP submissions cycle in July 2018 for FY2019 ITPR submissions. The Department therefore asserts that the implementation of the 2016 audit finding was performed in the most expeditious manner possible (complete project implementation in less than twelve months), and indeed is now complete. PRISM has provided value for the State and has delivered many successful outcomes in addition to the approval process discussed here.		
Recommendation 1b	Disagree	**Estimated Completion Date:**	N/A
	The Department takes seriously its oversight and monitoring responsibility over MITDPs; however, we <u>DISAGREE</u> with the finding and recommendation that the OPMs must document their review and verification of the accuracy of the monthly project monitoring reports. Because we believe there is a process established to document the OPMs monitoring efforts, we also <u>DISAGREE</u> with the determination of this item as a repeat finding. *The Department's OPMs and EPMO do not serve as project managers for the MITDPs (as mentioned in the response to 1a), but serve an oversight role as a subject matter expert to provide guidance and insight. Through its oversight role, the Department tailors the review protocols of each MITDP. Factors that influence the Department's tailoring of MITDP review include the project management methodologies applied, project size, stage, and the nature of the work being performed.* *While the OPM does review and analyze reports as part of its oversight function, the Department does not possess a formal internal verification or audit capability. This detailed level of oversight and verification, recommended by the auditors, is not required by statute and is not the mission of the Department. The Units maintain responsibility for project management and reporting accurate data. The EPMO does, where appropriate and as funding permits, conduct research into significant risks and issues. EPMO presents findings and other outcomes of research back to the appropriate parties (i.e., unit's executive sponsor, project manager, or PMO) for further investigation and response, and where appropriate these are brought to the Secretary's attention.* *In cases where a detailed verification is deemed to be necessary, the Secretary may request the engagement of an Independent Verification and Validation (IV&V) service. The Department engages this service, typically provided by a*		

Agency Response Form

	third party not involved with the MITDP, to examine the MITDP based upon a defined scope of engagement established by the Secretary. The Department does not have the funds to provide this level of verification on all MITDPs.		
Recommendation 1c	Disagree	**Estimated Completion Date:**	N/A
	We <u>DISAGREE</u> with the finding and recommendation. *During monthly health check meetings, OPMs submit reports and present an analysis of each MITDP to the Secretary to ensure the Secretary is fully informed of key factors, including risks and issues that affect the health of MITDPs. Risks identified and recommended actions to be taken to correct them are being documented by the OPM. There is no requirement that this information must be provided in the monthly project reports. Furthermore, these reports are not a deliverable prepared by the OPMs but by the unit's project managers.* ***<u>We DISAGREE that this finding and recommendation should be considered a repeat.</u>*** *The September, 2016 audit recommended improvements to the identification and monitoring of risks at the Department's quarterly portfolio review meetings. These meetings are being held as required. Additionally, the Department supplied to OLA, during the audit, records demonstrating that the recommended improvements have been made. Thus, we do not believe this particular finding or recommendation is a repeat.*		
Recommendation 1d	Disagree	**Estimated Completion Date:**	N/A
	The Department <u>DISAGREES</u> with this finding and is unable to implement the recommendation as presented by the auditors. The Department performs limited reviews of information submitted by units that are used for reporting. These reviews are based on available information. The recommended actions proposed by OLA, which require a more detailed review, are outside the scope of the Department's statutory responsibility and available resources. *The Department relies upon the unit submitter to properly estimate total current and out year project costs. The Department carefully analyzes the budget requests that the unit submits and then, with the approval of the Secretary, submits those budget requests on the unit's behalf. Once budget requests are approved, units then receive funds from the MITDP fund and are responsible for the expenditure of the funds received. The Department monitors for variances in spending from the estimates provided and depends upon agencies to report their project costs accurately. This is because the Department does not operate the projects and is not resourced to provide detailed financial analysis; rather, these MITDPs are operated by the agencies themselves. It is the unit's responsibility to ensure that the figures reported as estimated total current and future project costs are accurate. The Department will remind units of this responsibility.*		

Department of Information Technology

Agency Response Form

	The Department has followed up with individual units found by OLA to have misrepresented facts associated with their organization's MITDP(s) to ensure the unit understands their responsibility to report accurate data and to enable these units to determine what corrective actions need to be put in place to ensure all reporting from that unit represents accurate and complete information.

Agency Response Form

Finding 2
DoIT had not established a process to independently evaluate OPMs hired through a vendor to oversee MITDPs.

We recommend that DoIT conduct periodic performance evaluations of the OPMs to help ensure MITDPs are being effectively monitored (repeat).

Agency Response			
Analysis			
Recommendation 2	Agree	**Estimated Completion Date:**	Complete
	This finding has been addressed. *Corrective actions were put in place with the new oversight support services RFP released in June, 2018 to address this finding. The new oversight support services contract was awarded in March, 2019 and included monthly Performance Evaluation Forms to be completed by each Task Order manager for each OPM supporting the contract.* *Thus, DoIT has instituted a process for performing evaluations for each OPM contractor. These monthly evaluations are being conducted and are submitted to the Contract Monitor to ensure OPMs are properly performing as well as to ensure MITDPs are being effectively monitored. Follow-up action is taken, if necessary, for any unsatisfactory performance items noted. This process is documented and will be maintained for future reference and audit purposes.*		

Department of Information Technology

Agency Response Form

Statewide Communications Interoperability Program

Finding 3
DoIT did not ensure that the Maryland FiRST vendor met certain contractual requirements related to radio coverage nor did it ensure contract milestones regarding radio coverage testing were completed prior to payment.

We recommend DoIT

a. monitor the contract to ensure that the vendor complied with contract requirements, including radio coverage, unless appropriately waived; and

b. obtain and review documentation to support that contract deliverables (milestones) were satisfactorily met prior to making related payments.

Agency Response			
Analysis			
Recommendation 3a	Agree	**Estimated Completion Date:**	December 2020
	While DoIT agrees with the auditor's recommendation, we would like to note the following: • *"DoIT could not document that it received one test plan and that it had approved the other test plan."* *The test plans used in these instances were the same as those used in all previous phases of the project, so it was felt that a new approval was not required. It should be noted that all equipment operated as expected.* • *"DoIT did not document its approval to waive radio coverage testing in certain geographical areas as required by the contract."* *The original RFP and Contract allow test "tiles" that are inaccessible to have the requirement to test them waived. An example of this is when certain coverage testing "tiles" cannot be accessed by test vehicles during coverage testing due to private land ownership or safety concerns for test teams. The contract requires the test teams to only make every effort to test tiles and acknowledges there are certain instances where tiles may be inaccessible. While we understand the auditor's position, DoIT, did not originally believe a documented, formal waiver was necessary* • *"For the radio frequency test, DoIT accepted the Washington County coverage testing result of 74.5 percent, even though the minimum acceptable radio communications coverage for the Western Maryland phase was 86.5 percent."* *In the test plan and CATP presentations, the predicted or acceptable radio communications coverage (i.e., 24db in-building coverage) was*		

Agency Response Form

	*stated to be 86.5%. The average communications coverage for Phase 4 based on the final testing is **actually 87.235%,** which surpasses the predicted, acceptable coverage requirement of 86.5%. Note, there is no requirement for 12db in building tests, so those results are not required for acceptance. The only results that are required for acceptance are the 24db tests, if applicable, and the on-street test.* *To implement the recommendation, DoIT has notified the contractor to revise, and submit for approval, any and all test plans at least 30 days prior to any scheduled testing. Revisions to the existing plans include the addition of waived test tiles supporting coverage testing, and a site by site equipment walk through supporting acceptance testing.* *DoIT has also requested the vendor review expected testing results with the State prior to testing to ensure contractual requirements for the applicable phase will be met. Any contractual variations to the expected result will be documented by the vendor and approved by DoIT staff, along with a documented mitigation plan.* *No testing has occurred on the project since these policy revisions were submitted to the vendor following these audit findings. This revised process will resolve the concerns the auditor's had as well as will help to ensure the vendor has complied with contract requirements. This new process will be implemented beginning with the Phase 5 testing, which is scheduled to begin in 4Q2020 (CY).*		
Recommendation 3b	Agree	**Estimated Completion Date:**	December 2020
	DoIT has implemented additional internal processes to ensure that all contract deliverables (milestone completions) are fully documented by the vendor and reviewed by appropriate levels of DoIT staff for contract compliance (i.e. to ensure contract deliverables were satisfactorily met) before any invoices are authorized for payment. This revised process will be implemented beginning with the Phase 5 testing, which is scheduled to begin in 4Q2020 (CY).		

Agency Response Form

Finding 4
DoIT did not adequately monitor the construction of a tower and ensure that the related payments totaling $1.4 million were proper.

For all tower construction services contracts, we recommend DoIT

a. ensure all required inspections are performed and properly documented,
b. ensure work is completed in accordance with the contract prior to approval of invoices for payment, and
c. assess applicable liquidated damages when appropriate.

Agency Response			
Analysis			
Recommendation 4a	Agree	**Estimated Completion Date:**	Completed
	DoIT has formalized inspection of work done with proper documentation that is reviewed at appropriate levels of DoIT management. These new procedures ensure all inspections are performed as per contracts. In addition, documentation of these required inspections will be maintained and available, as necessary. This corrective action began with the implementation of the Nice Bridge tower in Dec 19. These processes will continue with all subsequent tower constructions.		
Recommendation 4b	Agree	**Estimated Completion Date:**	Completed
	DoIT personnel performed on-site inspections of all work completed prior to the authorization of vendor milestone payment during the implementation of the Nice Bridge tower in Dec 19. Per DoITs request, the tower vendor provided on-going status reports to DoIT staff for review to ensure work was occurring according to contractual requirements, Site documentation was reviewed and approved by the appropriate levels of management before any invoices were authorized for payment. These processes are documented and will continue with all subsequent tower constructions.		
Recommendation 4c	Agree	**Estimated Completion Date:**	Completed
	With the implementation of the Nice Bridge tower in December 19, DoIT project managers worked closely with Procurement Officers to ensure that all work was completed per the contract, regularly reviewing the terms of the contract to ensure that completion dates were met or, if warranted, terms of the contract were modified for successful completion. These processes will continue with all subsequent tower constructions. If there should be any instances where assessing liquidating damages is appropriate, DoIT will take necessary actions.		

Agency Response Form

Information Systems Security and Control

Finding 5
Intrusion detection and prevention system (IDPS) coverage did not exist for a substantial amount of untrusted network traffic flowing into DoIT's internal network.

We recommend that DoIT ensure that network-based IDPS protection exists for all critical portions of its internal network, by including IDPS coverage for untrusted external traffic flowing to its internal network resources.

Agency Response			
Analysis			
Recommendation 5	Agree	**Estimated Completion Date:**	Completed
	DoIT agrees completely with this finding. The auditor's evaluation occurred just as the firewall baseline process for DoIT started. Specifically, the items noted in the analysis of the finding were addressed as part of the Rev.0 firewall baseline project. DoIT implemented those changes from 12/7/2017 through 11/08/2018.		

Agency Response Form

Finding 6
DoIT lacked assurance that adequate information technology security and operational controls existed over its managed cloud collaboration and eGovernment software systems that were hosted, operated, and maintained by service providers.

We recommend that DoIT, for its managed cloud collaboration and eGovernment software systems,

a. timely obtain and review copies of SOC 2 Type 2 reports, including any needed reports for prior periods, and verify that the related service providers implement all critical report recommendations; and

b. document the aforementioned reviews and retain them for future reference

Agency Response			
Analysis			
Recommendation 6a	Agree	**Estimated Completion Date:**	December 2020
	DoIT will ensure that all future and current contracts for third-party hosting services require the service provider to annually obtain a SOC 2 Type 2 audit and to provide DoIT a copy of the SOC 2 audit within 30 days of it being provided to the service provider. DoIT will follow up with the service providers to make sure all reports are received timely. In addition, for all current such contracts, DoIT will follow up with the service provider(s) to obtain any needed reports for prior periods (as appropriate). All SOC 2 audits received will be reviewed to ensure the sufficiency of controls. Appropriate action will be taken as necessary. All such reviews and follow-up actions needed will be documented.		
Recommendation 6b	Agree	**Estimated Completion Date:**	December 2020
	DoIT will conduct a documented review of the independent assessments received from the third-party service providers to ensure adequate information technology security and operational controls existed over its State enterprise services operations. These reviews and any follow-up actions needed will be documented and retained for future reference.		

Department of Information Technology

Agency Response Form

Financial Management Information System

Finding 7
Personally identifiable information (PII) was not adequately restricted in the State's FMIS and was visible to 5,204 employees Statewide.

We recommend that DoIT, in conjunction with the Comptroller and DBM, take the necessary steps to adequately restrict and safeguard PII in FMIS.

Agency Response			
Analysis			
Recommendation 7	Agree	**Estimated Completion Date:**	December 2020
	DoIT will reach out to the various agency security officers and request they review FMIS user's security level for each online screen. They will determine if access to the screen is necessary and revoke as required. Essentially, only users of FMIS that require access to the specific system components are granted access. *The replacement of eMarylandMarketplace (eMM), the State's online procurement application is in progress. The replacement application dubbed eMMA is required to adhere to the State's Cybersecurity policy including items related to protecting PII.* *It is impractical to remove PII in FMIS in its entirety given our tax reporting mandate, however DoIT will work to minimize PII exposure where ever possible. FMIS reports will be reviewed determining if masking the vendor number is an option. Masking will take into consideration report type (control, requestable), GAD concerns and not inhibit the ability of State employees to perform their job function.* *Online screens within FMIS will be reviewed to determine the screen type – data entry or inquiry - and if masking the vendor number is practical. Masking will take into consideration screen type, document status, user access, GAD concerns and not inhibit the ability of State employees to perform their job function. Any masking discussion will require a lengthy detailed walk through of all processes to gain a complete understanding of how all of the tables interact. Any programming changes made could introduce significant operational risk to daily State-wide payment functions.*		

Agency Response Form

	While we understand the risk associated with PII in FMIS, the data elements are necessary for tax reporting and liability offset capture. Vendors and their associated PII are only added into FMIS when payment is required. Hence, the vendor associated PII is necessary. Yearly processes are executed in FMIS that disable vendors after five years of inactivity and are removed from the application after 10 years of inactivity. The purge function minimizes the amount of PII captured and retained within FMIS

Agency Response Form

Contracts

Finding 8
DoIT did not adequately monitor task order payments and did not obtain support for the related invoices from its networkMaryland vendor for which payments totaled $56.8 million.

We recommend DoIT

a. obtain documentation to ensure that goods and services are received in a satisfactory manner prior to approving invoice payments;
b. obtain timesheets from the vendor and compare them to hours billed, at least on a test basis, to ensure labor hours billed are supported;
c. maintain a record of amounts spent for each task and ensure payments do not exceed the related task order; and
d. investigate the aforementioned task order payments that exceeded the approved amounts, and take any appropriate action.

Agency Response			
Analysis			
Recommendation 8a	Agree	**Estimated Completion Date:**	Complete
	DoIT and the vendor have developed and implemented a Project Acceptance Form (PAF) which is approved by the appropriate Program Manager within DoIT. As a part of this process, related documentation (such as receiving reports, written plans, and site diagrams) will be received and, if deemed necessary, inspections may be performed periodically to confirm services were received as requested. Because a number of these projects extend over many months, it is not practical to defer approval of monthly invoices until the scoped goods and services are received in full. In these cases, we will sample monthly billings against the detailed monthly reports provided to ensure there is agreement between the invoice and the detail. Prior to a final payment being made, we will require that the PAF be approved by the vendor and by DoIT indicating that the project has been completed in a satisfactory manner and all deliverables and services have been received.		
Recommendation 8b	Agree	**Estimated Completion Date:**	Complete
	DoIT is now receiving automated reports showing hours billed by employee (including the associated approvals) as well as the tasks being supported. DoIT is comparing those hours against the detailed time reporting for those specific tasks and the associated activities being performed to ensure they align with the project. DoIT is also ensuring that total billed hours are reasonable relative to the billable period and requesting explanations of hours which		

Agency Response Form

	exceed what would be expected for the billing period. This review is documented and performed prior to reviewing invoices.		
Recommendation 8c	Agree	**Estimated Completion Date:**	Complete
	DoIT is now receiving an automated report which tracks monthly spend by task order and compares that spend to the amounts authorized for each task order, prior to approving invoice payments. Amounts in excess of approved task orders which are not supported by approved change orders are being rejected.		
Recommendation 8d	Agree	**Estimated Completion Date:**	June 2020
	We will investigate the differences once the specific details are provided, and take action as deemed necessary.		

Department of Information Technology

Agency Response Form

Enterprise Technology Support Services Initiative

Finding 9
DoIT lacked formal written agreements with the 29 participating State agencies to clarify responsibilities of technology support services performed by DoIT and the reimbursement of related costs.

We recommend DoIT enter into formal MOUs with all agencies for which it provides services as part of the Enterprise Technology Support Services Initiative. The MOU should clarify DoIT and agency responsibilities, specific services to be provided by each, and a mechanism to provide for the cost of these services.

Agency Response			
Analysis			
Recommendation 9	Agree	**Estimated Completion Date:**	June 2020
	DoIT has created a standard MOU for all agencies that receive Enterprise Services, which lays out the roles and responsibilities of all parties. There are also service agreements for each service in DoIT's service catalog that an agency subscribes to which will be part of the MOU. The annual invoice provides for the cost of the services to be provided, Portfolio Officers are working with the agencies to get these documents executed.		

Department of Information Technology

Agency Response Form

Equipment

Finding 10
DoIT did not adequately control its equipment inventory and did not maintain accurate detail records.

We recommend that DoIT comply with the requirements of the DGS *Inventory Control Manual*

Agency Response			
Analysis			
Recommendation 10	Agree	**Estimated Completion Date:**	June 2020
	DoIT is moving the asset management function to DoIT Fiscal. We are currently working with DGS on a policy for DoIT asset management, which will include that all purchased equipment that meets the requirements for asset management will be tagged and accounted for appropriately when it is received. All items delivered will be compared to order sheets to ensure all equipment ordered is accounted for. *DoIT will create an independent "control account" for inventory purposes and require quarterly "change logs" from vendors so that all moves/replacement/retirements/new equipment can be accounted for. All equipment will be verified prior to acceptance and all equipment will be independently verified prior to being decommissioned to ensure the control account is accurate. This control account will be reconciled periodically to the detail records to ensure the records are up to date and all equipment has been properly tagged and accounted for.* *DoIT will ensure independent and documented annual physical inventories are conducted as required. The results will be reconciled to the related detail records. Any discrepancies will be investigated, and missing items will be reported to DGS, as appropriate.* *DoIT personnel will work with DGS to identify the requirements to accurately report inventory to DGS, per their current asset management policies.*		

APPENDIX B

Auditor's Comment on the Department of Information Technology's Response

In its response to the audit report, the Department of Information Technology (DoIT) disagreed with numerous aspects of Finding 1 as it related to its level of responsibility for monitoring Major Information Technology Development Projects (MITDPs). Appendix A represents a revised response from DoIT to the audit report, and was submitted after DoIT management requested an opportunity to further discuss Finding 1 and withdrew their initial response. While the revised response acknowledges a greater degree of DoIT responsibility for monitoring MITDPs then claimed in the initial response, we still believe additional monitoring and verification efforts are warranted beyond those accepted to by DoIT. Our comments addressing this continued disagreement are presented below. In accordance with State law, all areas of disagreement will be addressed through separate correspondence between this Office and DoIT.

Finding 1:

DoIT's response indicates numerous disagreements with our Finding 1, entitled MITDPs. We reviewed and reassessed our audit documentation and, as a result, we have reaffirmed the validity of our finding. It continues to be our position that DoIT must implement formal processes to monitor MITDPs in a comprehensive manner, including verification that the State agency prepared annual project status reports (ITPRs) are complete and accurate. Rather than address and refute the numerous DoIT's disagreements on a point-by-point basis, we will focus on some of the recurring themes from its response on a high-level basis.

For example, in response to our recommendation to document their review and verification of the accuracy of monthly project monitoring reports (Recommendation 1b.), DoIT stated it agreed that it has an oversight and monitoring responsibility related to the MITDPs, but disagreed with the detailed level of related tasks that we are recommending, citing a lack of statute requiring such efforts and asserting it is not DoIT's mission to verify the accuracy of the monthly reports. In this regard, DoIT's response refers to the monthly project reports as merely an informal information gathering tool that is not required by statute and states that it does not possess a formal internal verification or audit capability and, therefore, relies on State agencies to report accurate data. However, we continue to believe that the monitoring of MITDPs is a critical function of DoIT, regardless of State law not specifically making mention of a monthly monitoring requirement. Additionally, since State law requires DoIT to

oversee the development and implementation of MITDPs, we believe it reasonable and appropriate to conclude that it is part of DoIT's responsibility and mission to verify the accuracy of the monthly reports given the financial and operational importance of such projects to specific agencies and to the State overall.

Therefore, we continue to strongly believe that DoIT should review and verify the accuracy of the monthly project reports, including scope, schedule, cost and risk, since this was the report process initiated by DoIT to collect information on the projects. Our review of selected reports disclosed that certain critical information, such as actions to be taken to address identified risks (project delays), for large projects like MD THINK were not always included in the reports. As part of DoIT's oversight of MITDPs, DoIT should verify the inclusion of all pertinent information and the review of the reports should be documented to ensure the completion of the reviews.

Also throughout its response, DoIT maintains that certain information it reports to State agencies and officials are received from the units having MITDPs and that the units are expected to report accurate data. We share DoIT's hope that State agencies will provide correct and supportable information, but the results of our audits of State agencies have shown over the years that formal oversight processes are both a necessary and valuable control feature to ensure agency compliance. Consequently, we continue to believe that DoIT should ensure the accuracy of information that it receives and then reports to other parties responsible for making decisions over such important and expensive projects, especially when even a cursory review may disclose obvious problems such as agency-reported information not having been updated since the preceding year (as noted in Finding 1).

Finally, DoIT disputes this Finding is a repeat condition from the preceding audit report. While the frequency of the reporting may have changed since last audit (from quarterly to monthly), DoIT still has not ensured that information reported on the ITPRs is current and complete, that its reviews of the reports submitted are documented, that the ITPRs contain accurate information, and that project risks are identified and documented at applicable meetings, all of which were recommended in our preceding audit.

AUDIT TEAM

Mark S. Hagenbuch, CPA
Audit Manager

R. Brendan Coffey, CPA, CISA
Information Systems Audit Manager

Julia M. King
Lauren E. Franchak, CPA
Senior Auditors

J. Gregory Busch, CISA
Information Systems Senior Auditor

Sporthi J. Carnelio
Zain Khalid
Staff Auditors

Peter W. Chong
Joseph R. Clayton
Information Systems Staff Auditors