

Audit Report

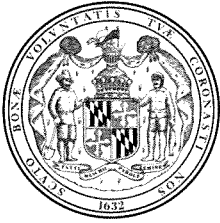
**Department of Health and Mental Hygiene
Office of the Secretary and Other Units**

February 2015



OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

-
- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.
 - Electronic copies of our audit reports can be viewed or downloaded from our website at <http://www.ola.state.md.us>.
 - Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.
 - The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.
-



DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

February 19, 2015

Thomas J. Barnickel III, CPA
Legislative Auditor

Senator Guy J. Guzzone, Co-Chair, Joint Audit Committee
Delegate Craig J. Zucker, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Office of the Secretary and other units of the Department of Health and Mental Hygiene (DHMH) for the period beginning October 15, 2009 to February 26, 2013. DHMH is responsible for promoting the health of the public and strengthening partnerships between State and local governments, the business community, and all health care providers in Maryland regarding health care.

Our audit disclosed issues with two information technology development projects. Specifically, DHMH did not formally communicate certain aspects of the Medicaid Enterprise Redevelopment Project (MERP) procurement process, including certain potential risks, when it sought Board of Public Works approval of the contract. The MERP contract, awarded in January 2012, is a \$171 million contract to replace the current system used to process Medicaid payments. As of September 2014, the contractor had been paid \$27.4 million. Amid a number of development issues, the Department of Information Technology (DoIT) and DHMH suspended work on MERP in August 2014. Additionally, DHMH did not adequately plan the Long Term Supports and Services project, nor was DoIT approval obtained when the project was initiated. Furthermore, the use of an arrangement with a State university resulted in the project development work not being subject to competitive procurement. Over a three-year period, the costs of the project have increased to more than \$20 million.

We also found that DHMH's Office of Inspector General had not been completing local health department and certain provider grant audits timely and in accordance with professional standards. In addition, DHMH's Division of Cost Accounting and Reimbursements did not adequately pursue collection of delinquent patient accounts from third parties or send the accounts to the State's Central Collection

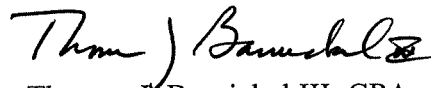
Unit as required which could result in the State unnecessarily absorbing the cost of care provided to patients admitted to State hospitals.

Our audit also disclosed that DHMH had not established sufficient security and controls over its information systems and network. For example, intrusion detection prevention system coverage and controls were not in place to protect all DHMH computers.

There were a number of other findings involving the preparation of federal reimbursement requests, the monitoring of corporate purchasing card transactions, the processing of settlement checks for capital grant projects, and the accounting for equipment.

An executive summary of our findings can be found on page 5. DHMH's response to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by DHMH.

Respectfully submitted,

A handwritten signature in black ink, reading "Thomas J. Barnickel III". The signature is written in a cursive, flowing style with a large initial "T" and a stylized "B".

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

Executive Summary	5
Background Information	7
Agency Responsibilities	7
Organizational Changes	7
Federal Audit Disallowance for Personal Care Services	8
Status of Findings from Preceding Audit Report	8
Findings and Recommendations	9
Medicaid Enterprise Restructuring Project (MERP)	
Finding 1 – Potential Risks of the MERP Project and Key Aspects of the Procurement Process Were Not Formally Disclosed to BPW	11
Long Term Supports and Services (LTSS) Tracking System	
Finding 2 – The LTSS Project Was Not Adequately Planned, Initially Subject to DoIT Oversight, Nor Competitively Procured	15
Office of Inspector General	
Finding 3 – Written Policies Were Not Established for Conducting Grant Audits Timely and in Accordance With Professional Standards	18
Finding 4 – Grantee Compliance with Sub-Vendor Audit and Oversight Requirements Were Not Verified During Grant Audits as Required	19
Division of Cost Accounting and Reimbursements (DCAR)	
Finding 5 – Records for Open Patient Financial Investigations Were Not Properly Maintained and Investigations Were Not Always Timely Conducted and Reviewed	20
* Finding 6 – Delinquent Accounts Receivable Were Not Adequately Pursued and Denied Insurance and Medicare Claims Were Not Timely Resolved	21
Finding 7 – DCAR Lacked Appropriate Procedures to Ensure All Cash Receipts Were Deposited	22
* Denotes item repeated in full or part from preceding audit report	

Federal Funds	
Finding 8 – Supervisory Oversight of Federal Fund Reimbursement Requests Was Not Always Effective	23
Corporate Purchasing Cards (CPC)	
Finding 9 – CPC Transactions Were Not Thoroughly Reviewed and Supported, Which Allowed Certain Improper Purchases to Go Undetected	23
Information Systems Security and Control	
Finding 10 – Intrusion Detection Prevention System Coverage and Controls for the DHMH Network Were Insufficient	25
* Finding 11 – Network Access to Critical Internal Network Devices Was Not Properly Restricted and Monitoring of Certain Security Events Was Not Adequate	26
Finding 12 – Malware Protection on DHMH Workstations and Servers Needs Improvement	27
* Finding 13 – Controls Over the National Electronic Disease Surveillance System Database and the Hospital Management Information System Application Were Not Sufficient	28
Capital Grant Project Checks	
Finding 14 – Proper Controls Were Not Established Over the Processing of Settlement Checks Issued for Capital Grant Projects	29
Equipment	
Finding 15 – Record Keeping and Physical Inventory Procedures Were Not in Compliance with Certain DGS Requirements	30
Audit Scope, Objectives, and Methodology	33
Agency Response	Appendix

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

Executive Summary

Legislative Audit Report on the Department of Health and Mental Hygiene (DHMH) Office of the Secretary and Other Units February 2015

- **DHMH had not formally communicated to the Board of Public Works (BPW) certain aspects of the Medicaid Enterprise Restructuring Project (MERP) procurement process, including the potential risks regarding the award decision, when it sought BPW's approval of the contract. For example, evidence was lacking that the BPW was apprised that the successful bidder had past performance issues, such as significant cost overruns and project implementation delays, on similar projects in other states. The MERP contract, awarded in January 2012, is a five-year, \$171 million contract to replace the current system used to process Medicaid payments. In August 2014, the Department of Information Technology (DoIT) and DHMH suspended development work on the project (Finding 1).**

DHMH should, in the future, ensure that all pertinent circumstances regarding significant procurement award decisions, including potential risks, are clearly documented and conveyed to the BPW for consideration when seeking contract approval.

- **DHMH did not adequately plan the development of the Long Term Supports and Services (LTSS) tracking system nor was DoIT approval obtained when the project was initiated. Additionally, the use of an arrangement with a State university resulted in the project not being subject to a competitive procurement as would normally be required by State procurement regulations had the services of the information technology (IT) contractor used on the project been obtained directly by DHMH. Over a three-year period, the cost of the project increased to more than \$20 million (Finding 2).**

DHMH should ensure that all significant IT projects are adequately planned and approved by DoIT as appropriate. Additionally, DHMH should evaluate arrangements with State agencies to ensure required services should not otherwise be obtained through a competitive procurement process.

- **DHMH had not established formal written policies for conducting local health department (LHD) and certain provider grant audits to ensure completion in a timely manner and in accordance with established professional standards (Finding 3). In addition, DHMH did not adequately verify that LHDs and private providers complied with sub-vendor audit and oversight requirements (Finding 4).**

DHMH should establish formal written policies for conducting grant audits, complete the audits in a timely and professional manner, and ensure the LHDs and private providers comply with the sub-vendor audit and oversight requirements.

- **Sufficient controls were not established over the reimbursements sought and received for the cost of care provided to patients admitted to State hospitals. Records for patient financial investigations were not properly maintained and approved (Finding 5), delinquent accounts were not properly pursued (Finding 6), and deposit verification procedures were inadequate (Finding 7).**

DHMH should take the recommended actions to ensure that the records related to cost recoveries for patients admitted to State hospitals are properly maintained, delinquent accounts are properly pursued, and the deposit of collections is properly verified.

- **DHMH had not established sufficient security and controls over its information systems (Findings 10 - 13). For example, intrusion detection prevention system coverage and controls over the network were not sufficient, and network access to critical internal network devices was not properly restricted.**

DHMH should take the recommended actions to ensure that proper security and controls are established over its information systems.

- **Effective controls were not established over federal funds, corporate purchasing cards, grant settlement checks, and equipment (Findings 8, 9, 14, and 15).**

DHMH should ensure appropriate controls are established and followed.

Background Information

Agency Responsibilities

The Department of Health and Mental Hygiene (DHMH) is responsible for promoting the health of the public and for strengthening partnerships between State and local governments, the business community, and all health care providers in Maryland regarding health care. This audit report includes the operations of the following five units:

- Office of the Secretary
- Deputy Secretary for Operations
- Deputy Secretary for Public Health Services (excluding Vital Statistics Administration)
- Deputy Secretary for Behavioral Health and Disabilities
- Deputy Secretary for Health Care Financing

These units provide an administrative infrastructure and oversight to DHMH and other health providers throughout the State. Additionally, the units are responsible for policy formulation and program implementation and for providing executive oversight to certain DHMH administrations including the Maryland Medicaid program. As part of the administrative support provided by the units, certain support services (for example, payroll processing, maintenance of accounting records, and purchasing) are provided by DHMH's Office of the Secretary and Deputy Secretary for Operations to the other units of DHMH.

According to the State's records, during fiscal year 2014, expenditures for these five units totaled approximately \$53.6 million.

Organizational Changes

Effective July 1, 2011, certain duties and responsibilities within DHMH were reorganized. Specifically, the Vital Statistics Administration was transferred via budget amendment from the Deputy Secretary for Operations to the Deputy Secretary for Public Health Services. The Vital Statistics Administration (VSA) issues certified copies of birth, death, and marriage certificates. The activities of VSA through October 14, 2009 were included in our preceding audit report on DHMH – Office of the Secretary, dated August 9, 2011. The subsequent activities of VSA were addressed in a separate audit report dated May 27, 2014.

Federal Audit Disallowance for Personal Care Services

The United States Department of Health and Human Services issued an audit report in April 2013 that disallowed Medicaid expenditures totaling \$10.9 million. The audit reviewed personal care and nurse monitoring services costs claimed under Maryland's Medicaid Home and Community-Based Services Waiver for Older Adults from July 1, 2008 to June 30, 2010. The audit identified 20 unallowable personal care service claims where documentation did not meet State and federal requirements.

Maryland's Medicaid Home and Community-Based Services Waiver for Older Adults authorizes services for individuals with low incomes who are aged 50 or older and who need the level of care provided by a nursing facility. The waiver provides for personal care services and other services that help participants avoid institutionalization. In Maryland, DHMH is the State agency that administers the Medicaid program. During the period covered by the audit, the Maryland Department of Aging administered the waiver program through an interagency agreement with DHMH.

DHMH agreed with the federal audit report findings and repaid the disallowed expenditures in May 2013 with State general funds. DHMH also agreed to improve controls over claims for personal care services provided under the waiver to ensure compliance with federal and State requirements.

Status of Findings from Preceding Audit Report

Our audit included a review to determine the status of seven of the ten findings contained in our preceding audit report dated August 9, 2011, the other three findings related to VSA which, as previously mentioned, were addressed in a separate report. We determined that DHMH satisfactorily addressed four of the seven findings reviewed. The remaining three findings are repeated in this report.

Findings and Recommendations

Medicaid Enterprise Restructuring Project

Background and Project Status

The Department of Health and Mental Hygiene (DHMH) is the single State agency responsible for administering the Medicaid Program in the State of Maryland. The Program provides medical services to eligible recipients under Title XIX (Medicaid) of the Social Security Act through enrolled providers. The State reimburses providers for the medical services provided to eligible recipients. The services are provided through a combination of fee-for-service and prepaid arrangements with a variety of medical and managed care providers. Claims for payment received from medical providers are processed, adjudicated, and paid through a federally certified Medicaid Management Information System (MMIS).

DHMH has begun the process of replacing its existing MMIS (MMIS II) with a modernized MMIS called the Medicaid Enterprise Restructuring Project (MERP). DHMH worked with the Department of Information Technology (DoIT) to develop the MERP request for proposals (RFP) for MMIS replacement and full fiscal agent (claims processing) services. With the approval of the federal Centers for Medicare and Medicaid Services (CMS), the responsibilities of being the developing contractor and the subsequent fiscal agent (FA) were combined into this one RFP. This approach has reportedly been taken by the majority of other states that have replaced their MMIS within the last 10 years. The RFP for MERP was issued May 20, 2010 and proposals were due September 7, 2010.

DHMH awarded a five-year contract in January 2012 totaling approximately \$171 million for the period from March 1, 2012 to February 28, 2017, with three two-year renewal options. The contractor is to design, develop, implement, and operate MERP and also provide FA services. The federal funding participation percentage for the MMIS development costs is 90 percent and for the FA operating costs is 75 percent.

The MERP project has encountered certain development problems, including disagreements with the contractor over the scope of work and the inability of the contractor to submit certain acceptable deliverables. As a result, the contractor was unable to meet the original projected completion date of MERP (September 29, 2014) and the actual date that MERP may be completed is uncertain. MERP has not yet progressed beyond the design phase, and DHMH has continued to use MMIS II to process its Medicaid claims.

There were a number of disagreements between DHMH and the contractor regarding the scope of the work included under the terms of the contract. In September 2013, the contractor submitted a contract claim for approximately \$62 million in relation to alleged delays on the part of DHMH and work the contractor claims falls outside the original scope of the contract. The contractor subsequently reduced its contract claim to approximately \$34 million. DHMH rejected the claim in April 2014, and the contractor filed an appeal with the Board of Contract Appeals on May 28, 2014, which as of December 11, 2014 had not yet been ruled upon.

Due to the lack of completed deliverables, DHMH issued a directive letter, or cure notice, on January 31, 2014 detailing certain specific actions that needed to be corrected for the project to move forward. The notice required the contractor to cure its failure to submit an acceptable project schedule as obligated under the contract or show cause why the contract should not be terminated for default. DHMH found that the existing project schedule and related documents contained pervasive logical errors and factual inaccuracies. For example, tasks were marked as completed on the project schedule that had not been completed according to other project documents. Further, the contractor had made numerous unexplained and unapproved changes to project schedules without notifying DHMH which, according to DHMH, created a shifting and fundamentally unreliable account of the progress of the project. DHMH further clarified that the contractor's other performance failures would not be addressed in this cure notice, but in future correspondence.

On March 14, 2014, DHMH issued a second cure notice to the contractor. The notice set forth the major deficiencies in work submitted after a previous corrective action plan (CAP) was put in place and describes the required steps the contractor needed to take. Although the CAP was submitted in May 2013, according to the second cure notice, the quality of the contractor's deliverables continued to be deficient and the CAP has proved to be "an ineffective tool for remediating the problematic performance." Additionally, DHMH identified a lack of attention to and commitment from the contractor's FA operations unit as one major root cause of multiple problems, including a stalled design process and significant delays. According to the second cure notice, this lack of participation constituted a significant departure from contractually required industry best practices and it continued to be a major barrier to completing the system design.

DoIT reported to the General Assembly that, as of August 15, 2014, the contractor had failed to submit a satisfactory response to either cure notice, and DHMH has been working with the contractor to find a suitable path forward without success. According to DoIT, the project remained high-risk and, on August 22, 2014, with

the support of DoIT, DHMH suspended development work on the project for a period of 90 days to resolve outstanding issues and to develop an acceptable path forward to continue MERP. We were advised that the work stop order was subsequently extended indefinitely. While the contractor had been paid \$27.4 million (net of \$3.0 million retainage) for 50 approved deliverables, as of September 8, 2014, there were 17 deliverables with a contract value totaling \$10.9 million that were 9 to 15 months past due. It is unlikely that MERP will meet its revised completion date of December 15, 2015 due to the suspension of work on the project. If an acceptable resolution cannot be agreed upon, DHMH advised it will evaluate other available remedies.

Finding 1

DHMH did not formally communicate certain pertinent aspects of the MERP procurement process and the potential risks regarding the award decision when it sought Board of Public Works (BPW) approval of the contract.

Analysis

DHMH did not formally communicate certain pertinent aspects of the MERP procurement process and potential risks regarding the award decision when it sought BPW approval of the contract. There was a lack of evidence that the BPW or its staff were fully apprised that the RFP qualifications were changed to obtain bidders, that the successful bidder had past performance issues involving similar projects, and that a change was made to the contractor liability provisions after the successful bidder was notified of the award. According to the results of its bid evaluation process, DHMH selected the contractor with the best technical evaluation and lowest price; however, the evaluation committee's results did not include a complete assessment of the potential risks involving its selection. We believe that in view of the project's complexity, cost, and significance to State operations, all pertinent aspects of the procurement process and potential risks should have been clearly identified and conveyed to the BPW for its consideration.

Although eight contractors expressed interest in the procurement, some of the contractors had questioned the prior experience qualifications established in the RFP. Consequently, the first addendum (ultimately there were eight addendums) to the May 20, 2010 RFP was issued on June 7, 2010 (prior to the bid submission date) to change the experience requirements. Initially, the RFP required bidders to have fiscal agent and MMIS implementation experience for a state MMIS certified by CMS within the last 5 years. The first addendum changed the qualifications so that the experience of a bidder's subcontractor would also be considered, and the period for prior system certification was extended to 10 years. After this addendum, DHMH determined that two interested contractors, which

subsequently submitted bids, were potentially qualified with respect to the prior experience requirements. As noted later, it is questionable as to whether one of these contractors, who was the losing bidder, had actually met the revised qualifications.

The June 2011 contract award recommendation memorandum from DHMH's eight-member bid evaluation committee did not provide a complete and objective assessment of the proposals, including a description of the potential risks involving its selection of the successful bidder. The memorandum included overall technical and financial rankings that indicated the bidder recommended for the award had received an overall technical proposal rating of excellent as compared to the other bidder whose proposal was determined to be poor. Also, the selected bidder's proposed cost was considerably lower. While the memorandum commented upon many of the strengths identified by the committee based on its evaluation of the selected bidder's technical proposal, it did not comment on any weaknesses pertaining to past performance issues that would have provided a more complete disclosure of the possible risks.

For example, one of the "key strengths" identified in the memorandum was that the selected bidder's subcontractor had developed an MMIS in two other states that were awaiting federal certification. (CMS certifications were subsequently obtained for both systems.) However, the memorandum did not mention that both of these systems had taken considerably longer (up to three years) than originally planned and had significant cost overruns (up to 300 percent) beyond the original projects' budgets. There was also no mention that this same subcontractor also had MMIS development contracts cancelled in two other states due to disputes arising from significant cost increases and numerous work defects. For example, according to public sources, the subcontractor was hired in June 2008 to develop an MMIS in one of these states, but two years later, after reportedly being paid \$50 million, the work was halted due to disputes over cost overruns. As of August 2013, the situation had not been resolved, and the project was on hold for more than three years. Several of these issues were noted in some of the individual committee members' bid evaluation documents, but were not disclosed in the contract award recommendation memorandum.

DHMH pointed out to us that under its technical evaluation scoring methodology, a bidder's past experience only constituted eight percent of the total score; this seems to suggest that even if evaluators had been more critical of the successful bidder's experience or if more weight was given to this category, the award outcome would not have changed given the disparity in the two bidders' total technical evaluation scores. While we acknowledge this likelihood, we nevertheless believe that past performance on similar work can be indicative of

future experience and risks and, at a minimum, the award recommendation memorandum should have provided a more complete and objective assessment of the bidder's experience and performance.

After DHMH notified the successful bidder in July 2011 that it had been selected for award, but prior to signing the contract, the contractor requested that DHMH change, what was at the time of the original RFP, standard State information technology contract language providing unlimited liability for breach of contract. According to DHMH, the contractor requested a \$20 million cap on its liability. At this stage, DHMH believed it had two options – either cancel the current procurement and pursue an entirely new procurement or change the liability clause and ask both bidders to submit a last Best and Final Offer (BAFO). It should be noted that in June 2011, the DHMH evaluation committee had discussed the risks of not awarding or rebidding the procurement. The committee concluded that the result of a new procurement would likely be the same, but the State would expend significant time and fiscal and operational resources, delay the contract award for one and one-half years, and potentially lose key State subject matter experts due to attrition.

DHMH chose to change the liability clause and ask the two bidders to submit a last BAFO. This decision was based on legal advice that concluded that State regulations prohibited an agency from making a significant contract change after selection of the successful contractor, but that RFP terms could be amended if the agency allowed all qualified bidders to revise their proposals based on the amended terms. Consequently, after consulting with DoIT, DHMH issued an eighth and final RFP addendum in October 2011 that reduced the contractor liability requirements from “unlimited” to “three times the value of the contract” (which is currently the standard liability provision for State information technology contracts) and requested both bidders to submit a last BAFO. The course of action taken by DHMH provided a way to address the successful bidder's late concern for its contract liability without jeopardizing the procurement award decision.

However, at this late stage of the procurement process, we question whether there should have been any realistic expectation of receiving a viable BAFO proposal from the second bidder. Specifically, the second bidder had previously been notified by DHMH (in July 2011) that it had not been selected for award, and it had been advised by DHMH in an August 2011 debriefing meeting that it was not selected, in part, because it lacked fiscal agent experience and had no recent MMIS implementation experience – two key RFP requirements. (Considering the second bidder's lack of MMIS experience, it is questionable whether the contractor met the revised RFP qualifications and should have been considered a

qualified bidder.) Ultimately, this bidder, in a November 2011 letter, informed DHMH that it declined to submit a last BAFO. In that letter, the bidder stated that its original proposal had been based on the assumption that standard State contract clauses were not subject to negotiation.

When the contract was submitted to BPW for its approval in February 2012, evidence was lacking that all pertinent considerations pertaining to DHMH's award decision had been formally communicated. Specifically, neither DHMH's formal presentation materials for the BPW meeting when the contract was presented for approval nor the pre-meeting briefing held with various State officials identified the significant risks associated with this project. There was no mention of the changes to the experience qualification to allow for potentially qualified bidders, the prior negative system development experiences of the successful bidder and its subcontractor, and the late change in the contractor breach of contract provision.

We were advised by a number of individuals who attended the pre-meeting briefing that there was a discussion of topics beyond those contained in the formal presentation material. However, other than the issue involving the change in contractor liability, the actual topics discussed could not be recalled with clarity due to the age of the event and the fact that no formal notes were taken.

In our opinion, given the project's complexity, cost, and significance to State operations, DHMH should have clearly conveyed all pertinent matters and risks involving the MERP procurement and selection process to BPW for its consideration.

Recommendation 1

We recommend that, in the future, DHMH ensure that all pertinent circumstances regarding significant procurement award decisions, including potential risks, are clearly documented and conveyed to BPW for its consideration of contracts submitted for approval.

Long Term Supports and Services Tracking System

Background

After the passage of the federal Affordable Care Act in June 2010, DHMH decided to modify its web-based tracking system for services provided to the elderly. These services are provided through Medicaid's Home and Community-Based Services Waiver programs and are coordinated with a number of State agencies. The revised tracking system would fully integrate with other agencies'

existing waiver tracking systems and become a single Long Term Supports and Services (LTSS) tracking system with new added functions and capabilities, including linking with the Maryland Health Benefit Exchange.

Since 1994, DHMH has entered into memorandums of understanding (MOU) with a unit of a State university to perform research and analysis on the Medicaid program as requested by DHMH. For example, the university develops capitation payment rates for managed care providers, provides program status reports, and provides consultation on issues such as federal health care reform. Provisions for developing and implementing the LTSS tracking system were initially included in the fiscal year 2011 MOU.

Finding 2

The LTSS information technology (IT) project was not adequately planned nor was DoIT approval obtained when the project was initiated. The use of the MOU resulted in the project work not being subject to competitive procurement as would normally be required by State procurement regulations.

Analysis

The LTSS IT project was not adequately planned nor was the required DoIT approval obtained when the project was initiated. Furthermore, DHMH's use of the MOU resulted in the project not being subject to a competitive procurement as would normally be required by State procurement regulations had the services of the IT contractor used on the project been obtained directly by DHMH. Over a three-year period, the cost of the project increased to \$20.1 million as of October 31, 2013.

DHMH did not establish a comprehensive plan for the development and implementation of the LTSS tracking system project, as it did not identify all user needs, the timeline for implementation, and estimated costs prior to the start of the project. Rather, the scope of work was determined as the system developed, and funding authorization under the MOU was obtained, as needed, as the work was completed. The project was assigned to the university which had previously performed tracking system development under the provisions of the MOUs between the entities. However, given the extent of the LTSS project, the university did not desire to take primary responsibility for its development but, rather, subcontracted the majority of the work to an IT company without a competitive solicitation.

Only limited funds for LTSS tracking system development (\$188,000 each year) were included in the budgets for the fiscal year 2011 and 2012 MOUs. However, the fiscal year 2012 MOU, as well as the fiscal year 2013 MOU, were modified a number of times, increasing the project budget by an additional \$8.8 million, bringing the total project award to \$9.2 million through fiscal year 2013. The deliverables were somewhat broad in scope, and the due date for the completion of the system (originally July 2012) was repeatedly extended (to January 2014) as the MOUs were modified.

Since services provided between State agencies are not subject to the State procurement regulations, DHMH's use of the MOU arrangement allowed for the LTSS subcontractor to be selected without a competitive solicitation process. If DHMH had sought to obtain the services directly from a vendor, the State procurement regulations would have applied and a competitive solicitation process would have been required. Without competition, DHMH lacked assurance that these services were received at the best value to the State. The university paid \$7.4 million to its subcontractor during fiscal years 2012 and 2013.

DHMH never formally approved the selection of the subcontractor as required by the fiscal year 2012 MOU (as modified), although the subcontractor was named in a modification of the 2013 MOU that DHMH approved in January 2013. The fiscal year 2012 MOU modifications stipulated that DHMH review and approve all subcontracts related to the work described in the modification prior to implementation. The university executed its agreement with its subcontractor in October 2011.

After development had begun, DHMH realized that the LTSS project met the \$1 million criteria for a Major Information Technology Development Project and, in January 2013, submitted an out-of-budget-cycle information technology project request for the LTSS project to DoIT. DHMH explained in its request that the original scope of the work was smaller but, after the project scope expanded, DHMH realized it required DoIT oversight and approval. DoIT advised DHMH that it should have been involved from the start of the project.

In accordance with fiscal year 2014 budget law language, the project was designated as a Major Information Technology Development Project subject to DoIT oversight. On July 24, 2013, BPW approved, as an emergency procurement, a contract between DHMH and the university's former LTSS subcontractor for an additional \$8.4 million to complete the LTSS project. The contract extended the project through June 30, 2014, with a one-year operations and maintenance option for \$2.5 million. In total, \$20.1 million has been awarded

for the LTSS project (\$9.2 million awarded to the university under MOUs plus a total of \$10.9 million under the contract awarded to the former university subcontractor). As of October 31, 2014 DHMH had paid a total of \$16.3 million on the project, which was subject to federal funding of 50 percent. We were advised by DHMH personnel that the LTSS tracking system had been implemented and was functioning at that time.

Recommendation 2

We recommend that DHMH ensure that, in the future,

- a. all information technology projects are properly planned, with their full scope and anticipated funding needs identified prior to implementation;**
- b. all qualifying projects are submitted to DoIT for review and oversight prior to their initiation;**
- c. formal arrangements with state agencies are closely evaluated to ensure that the required services should not otherwise be obtained through a competitive procurement process; and**
- d. all MOU provisions requiring the review and approval of significant subcontracts are complied with.**

Office of Inspector General

Background

The DHMH Office of Inspector General's (OIG) Division of Audits (DOA) performs audits of state grant funds paid to Local Health Departments (LHDs) and private non-profit providers who are reimbursed for the cost of care for eligible individuals. State law requires DHMH to examine the grant accounts of LHDs and these providers, determine the amount of allowable costs, and collect any excess reimbursements or pay any unreimbursed costs. DHMH has also established regulations and policy manuals to govern the use of these grants. There are 24 LHDs and 68 private non-profit providers that received grant awards subject to audit totaling \$1.8 billion and \$891 million, respectively, during fiscal years 2008 to 2013. The grant audits performed by the DOA are the primary mechanism for ensuring the propriety of the use of these funds and recovering unallowable expenditures.

Finding 3

The OIG had not established formal written policies for conducting provider grant audits in a timely manner and in accordance with established professional standards.

Analysis

The OIG had not established a formal written policy governing the timely completion of grant audits nor was there a policy to ensure the audits were conducted in accordance with established professional standards. We were advised by the management employee responsible for grant audits that the DOA still followed the policy established by the Fiscal Service Administration when it was responsible for these audits. (DOA assumed this function in December 2007.) The policy required each provider to be audited on a four-year cycle (based on the date since the last audit).

At the time of our review, we noted that 9 of the 24 LHDs and 36 of the 68 private providers had not been audited for at least five years. The LHDs and private non-profit providers that had not been audited received qualifying grant awards totaling \$217.6 million and \$83.7 million, respectively, during fiscal years 2008 and 2009. The untimely review of these grants results in the risk that the grants may not be able to be audited since State regulations do not require grantees to retain grant records beyond five years following the close of the fiscal year. We were advised by OIG management that it had sent letters to the providers in question requesting that they retain the records until audited, although such a request is not provided for in the aforementioned regulations.

Additionally, the OIG had not established a formal policy requiring grant audits to be performed in accordance with established professional auditing standards and did not always conduct the audits in accordance with such standards. For example, our review of the work papers supporting three audits disclosed that no written audit plans were prepared and that audit work papers and programs were generally not initialed by supervisory personnel to document their supervision of audit staff; these procedures are generally required by professional auditing standards.

Recommendation 3

We recommend that the OIG

- a. establish a written policy to govern the timely completion of its grant audits,**
- b. complete its grant audits on a timely basis, and**
- c. establish a formal policy requiring LHD and private non-profit provider grant audits to be conducted in accordance with professional standards.**

Finding 4

The OIG did not adequately verify LHD and private non-profit provider compliance with sub-vendor audit and oversight requirements.

Analysis

The OIG did not adequately verify LHD and private non-profit provider compliance with sub-vendor audit and oversight requirements. Our review of the grant audits for three LHDs disclosed that, for one LHD, the DOA had not verified adequate controls and monitoring procedures had been established over its sub-vendors, or that the LHD had conducted or contracted for audits of significant sub-vendors. For the other two LHDs, a listing of all sub-vendors was not obtained by DOA to enable it to conduct audit procedures to verify that the LHDs were properly monitoring their sub-vendors.

In accordance with applicable State laws and regulations, DHMH has established standards for LHDs and private non-profit providers that receive DHMH awards and then award all or a portion of those awards to sub-vendors to provide services to third parties. At a minimum, LHDs and private non-profit providers are required to have adequate controls and monitoring procedures over their sub-vendors and are responsible for conducting or contracting for regular audits of sub-vendors who receive funds of \$100,000 or more. The OIG, in turn, is required to oversee implementation of these standards by the LHDs and private non-profit providers and verify compliance as part of its regular audits of these entities.

Recommendation 4

We recommend that the OIG properly verify LHD and private non-profit provider compliance with sub-vendor audit and oversight requirements during its audits of these entities in accordance with established DHMH standards.

Division of Cost Accounting and Reimbursements**Background**

In accordance with State law, DHMH's Division of Cost Accounting and Reimbursements (DCAR) conducts financial investigations of all patients admitted to the State's mental health, intellectual disability, and chronic disease facilities to determine their ability to pay for the cost of care and/or to identify other liable parties (such as Medicaid, Medicare, third party insurers, or other legally responsible persons). DHMH policy requires DCAR's financial agents at the various State facilities to complete these investigations within six months after

the first date of service, in part, because State regulations generally only allow DHMH to bill certain parties for services retroactively for six months.

Based on the completed financial investigations, DCAR establishes an accounts receivable on the DHMH Hospital Management Information System (HMIS) and bills and collects the amounts due. According to DCAR's records, cost recoveries for fiscal year 2012 totaled approximately \$66 million and consisted primarily of Medicaid and Medicare collections, with \$4.1 million being collected from patients, legally responsible persons, and private insurers. For the same period, DCAR determined that services valued at \$227.7 million were provided to recipients for which the related costs were not recoverable from any source and consequently were paid by the State. During fiscal year 2012, 1,923 patients were admitted to the State's mental health, intellectual disability, and chronic disease facilities.

Finding 5

Records for open patient financial investigations were not properly maintained and monitored. In addition, investigations were not always timely conducted and reviewed by supervisory personnel.

Analysis

Records for open patient financial investigations were not properly maintained and monitored. In addition, investigations were not always timely conducted and reviewed by supervisory personnel. According to a March 31, 2013 report on the status of open investigations provided by DCAR management, there were 185 patient accounts for which DCAR had not determined the amount due and/or had not billed for the services provided that were more than six months old (including 107 over a year old). Our review of 10 of these accounts, as of May 30, 2013, disclosed the following conditions:

- For 8 accounts, including 4 listed as being more than 3 and one-half years old, the accounts had been investigated timely and did not belong on the open investigations report. As a result of the report including accounts that actually had been investigated, the report was not entirely reliable and its effectiveness as a monitoring tool was diminished.
- For 2 accounts, DCAR had not completed a financial investigation 12 and 18 months after the patient had been admitted, respectively. As a result, a financially responsible party was not identified and any potential recoveries could be in jeopardy.

Recommendation 5

We recommend that DHMH ensure that

- a. open patient financial investigation records are properly maintained and monitored, and**
- b. financial investigations are timely conducted.**

Finding 6

DHMH did not adequately pursue collection of delinquent DCAR accounts receivables. Furthermore, denied insurance and Medicare claims were not timely resolved.

Analysis

Delinquent accounts receivable were not always adequately pursued for collection and/or transferred to the Department of Budget and Management's Central Collection Unit (CCU), as required. Furthermore, claims which were originally denied by an insurance company or Medicare were not researched and timely resolved to determine if the insurance company or Medicare should pay the claim.

Our test of 10 accounts totaling \$3.5 million that were outstanding for more than 120 days disclosed that the collection efforts for 9 accounts totaling \$3.2 million were not sufficient. Four accounts with outstanding claims that were owed by either the patient or another individual totaling \$2.1 million were delinquent from 8 to 18 months. DCAR generally sent CCU referral warning letters to the patient or other responsible individuals, but did not refer these accounts to CCU as required. No account collection actions had been made on these accounts for 9 months to 3 years. In addition, DCAR had not sufficiently followed up on 5 outstanding accounts for which Medicare or insurance companies had denied claims totaling \$1.1 million from 6 months to over 5 years earlier. For example, for the 3 claims denied by Medicare, 2 of the claims had not been corrected and resubmitted 18 months after their denial. The other claim had been corrected and resubmitted, but no follow-up actions had been taken for 7 months after resubmission. Medicare claims are not accepted by CCU for collection. Similar conditions were commented upon in our preceding audit report.

According to DHMH accounts receivable records as of March 31, 2013, there were 1,615 outstanding accounts totaling approximately \$22 million, of which 1,072 accounts totaling approximately \$16 million were outstanding for more than 120 days. CCU regulations, as amended for DHMH, provide that delinquent balances be referred 120 days after the first billing except estate and insurance accounts; insurance accounts should be referred, regardless of age, when the claim is valid and once the insurer denies DHMH's initial request for payment.

Recommendation 6

We recommend that DHMH ensure

- a. delinquent accounts receivable are adequately pursued for collection and transferred to CCU as required (repeat); and**
- b. denied insurance and Medicare claims are timely resolved.**

Finding 7

DCAR lacked appropriate procedures to ensure all cash receipts were deposited.

Analysis

DCAR lacked appropriate procedures to ensure all cash receipts were deposited. Specifically, the cash receipts procedures provided that the initial recordation documents be routed to several employees without ensuring that a copy was forwarded directly to and retained by the employee responsible for verifying collections to deposit. Additionally, the employee responsible for the deposit verification also had access to the related collections. Under these conditions, the daily collection records are subject to possible manipulation and receipts could be lost or misappropriated without detection.

According to DCAR's records, collections received during fiscal year 2013 totaled approximately \$3.3 million. The Comptroller of Maryland's *Accounting Procedures Manual* requires that an employee independent of the cash receipts function ensure that all collections were subsequently deposited.

Recommendation 7

We recommend that DHMH ensure that

- a. the employee who prepares the initial record of collections forwards a copy of that record directly to the employee responsible for the deposit verification, and**
- b. the employee performing the deposit verification not have access to the related cash receipts.**

We advised DHMH on accomplishing the necessary separation of duties using existing personnel.

Federal Funds

Finding 8

Supervisory oversight of federal fund reimbursement requests was not always effective.

Analysis

Supervisory oversight of federal fund reimbursement requests could be improved. Specifically, although supervisory reviews of reimbursement requests were performed, the reviews were not always effective as the accuracy of supporting schedules and memorandums were not always thoroughly verified, resulting in certain errors that were either not detected or not detected timely. For example, expenditures totaling \$20.4 million that could have been submitted for reimbursement in February 2012 were included on a drawdown that was processed in May 2013. As a result of the delay in processing the reimbursement request, the State lost interest income of approximately \$233,000.

During fiscal year 2013, DHMH processed federal fund reimbursement requests totaling approximately \$4.6 billion.

Recommendation 8

We recommend that DHMH ensure that federal fund reimbursement requests are properly reviewed, along with supporting schedules and documents, and the reviews are documented.

Corporate Purchasing Cards

Finding 9

Corporate purchasing card transactions were not always thoroughly reviewed and supported, which allowed certain improper purchases to go undetected.

Analysis

Corporate purchasing card (CPC) transactions were not always thoroughly reviewed and supported, which allowed improper purchases totaling \$45,640 to go undetected. According to the issuing bank's records, as of February 2013, corporate purchasing cards had been issued to 325 DHMH employees, and the related expenditures totaled approximately \$22 million during fiscal year 2012. Our test of 169 credit card purchases totaling approximately \$122,000 made during our audit period disclosed the following conditions:

- For 18 of the purchases tested totaling approximately \$15,000, there were no itemized receipts to support the transactions. The five monthly activity logs that included the unsupported purchases had all been approved by the employees' supervisor and fiscal officer. As a result of the missing receipts, there was a lack of assurance that the expenditures were properly reviewed and represented legitimate purchases. In addition, monthly purchasing cardholder statements from the bank were not always approved as required. We noted that 7 of the 20 monthly statements tested were not signed by the cardholder's immediate supervisor. These seven logs included purchases totaling approximately \$44,000. The Comptroller of Maryland's *Corporate Purchasing Card Program Policy and Procedures Manual* requires a receipt showing the price of the item purchased. The *Manual* also requires the monthly activity log and monthly cardholder statement be approved by the cardholder's supervisor.
- Supervisory personnel did not always perform a documented review of available Level-3 purchasing card data to help determine the propriety of CPC transactions. Level-3 data, which are provided by certain merchants, provide detailed descriptions of items purchased. Specifically, for 11 logs tested where Level-3 data were available for certain purchases, there was no evidence that the data were reviewed for transactions on 8 of the logs. The review of the Level-3 data would help supervisors readily detect questionable purchases. For example, as previously disclosed in our March 26, 2014 performance audit report on the State's Corporate Purchasing Card Program, using Level-3 data, we identified inappropriate purchases (such as guitars and guitar accessories) totaling \$45,640 made by one cardholder at a LHD between January 2008 and February 2012. The cardholder indicated on the CPC activity logs that these purchases were for legitimate items and provided corresponding fictitious computer-generated receipts to avoid detection. In response to this performance audit, we were advised by DHMH management that it implemented a monthly OIG CPC Level-3 review procedure.

Recommendation 9

We recommend that DHMH

- ensure that all corporate card purchases are supported by appropriate documentation and thoroughly reviewed by supervisory personnel,**
- ensure that purchasing card activity logs and the related monthly cardholder statements are signed as required, and**
- incorporate and document the use of Level-3 purchasing card data in the supervisory review of the activity logs to help ensure the propriety of CPC activity.**

Information Systems Security and Control

Background

DHMH's Office of Information Technology (which is under the Deputy Secretary for Operations) is responsible for the overall management and direction of DHMH information systems. These systems include, but are not limited to, the Hospital Management Information System (HMIS – which is used to record information for patients of State hospitals such as admissions, billings, and collections), the National Electronic Disease Surveillance System (NEDSS – which is used to track and transmit sensitive information related to certain infectious diseases), and the mainframe-based MMIS. These systems, and many more, are supported by DHMH's network infrastructure. DHMH operates a wide area network with approximately 9,000 user connections across the State. This wide area network has connections to local health departments, State hospitals, health clinics, DHMH headquarters facility, the Statewide Government Intranet, and the Internet.

Finding 10

Intrusion detection prevention system coverage and controls for the DHMH network were not sufficient.

Analysis

Intrusion detection prevention system (IDPS) coverage and controls for the DHMH network were not sufficient.

- Although DHMH used both a network-based IDPS and protective software installed directly on servers, based on our inquiry, DHMH determined that 130 servers within DHMH's neutral network zone were not protected by network or server based IDPS. The servers without any form of IDPS protection are at a greater risk of being compromised than servers with IDPS protection. Furthermore, any of the servers that are compromised could be used to launch attacks against other servers in the internal network.
- Administrative access to the device providing network-based IDPS was not adequately controlled. Over 500 addresses had network-level administrative access to this device; however, only three network addresses required such access. Furthermore, certain password and account controls over accounts which could administer this device were not enabled. Specifically, password complexity, password history, and account lockout were not enabled. Accordingly, these password and account controls were not in accordance with the requirements specified by DoIT's *Information Security Policy*.

Complete IDPS coverage includes use of properly configured network-based IDPS to aid significantly in the detection/prevention of and response to potential network security breaches and attacks.

Recommendation 10

We recommend that DHMH

- a. provide adequate IDPS coverage for all servers in the aforementioned neutral network zone,**
- b. limit network-level administrative access to the network-based IDPS device to only those users requiring such access, and**
- c. ensure that password and account controls over the network-based IDPS device comply with DoIT requirements.**

Finding 11

Network access to critical internal network devices was not properly restricted and monitoring of security events over a critical firewall was not adequate.

Analysis

Network access to critical internal network devices was not properly restricted and monitoring of security events over a critical firewall was not adequate.

- Numerous rules on several DHMH's firewalls allowed unnecessary access to critical devices on the internal network. Specifically, rules on the firewalls protecting NEDSS and the firewalls protecting the internal network from the Internet and DHMH's disaster recovery alternate site allowed numerous unnecessary connections to internal network devices. In addition, many outdated rules existed on these firewalls. Similar conditions were commented upon in our preceding audit report.
- The device used to aggregate security logs from numerous DHMH network devices for review and analysis was not configured to report security-related activities on the Internet firewall. Specifically, firewall activities such as firewall configuration changes and failed login attempts were not reported for review and analysis. As a result, unnecessary or unauthorized changes could be made to this firewall without detection by management.

Recommendation 11

We recommend that DHMH

- a. configure its firewalls to properly protect all critical network devices; (repeat)**

- b. configure the aggregation device to include Internet firewall security-related activities such as configuration changes and failed logon attempts; and**
- c. review and analyze the reports of Internet firewall activity from this aggregation device, document these reviews, and retain the documentation for future reference.**

Finding 12

Malware protection on DHMH workstations and servers needs improvement.

Analysis

Malware protection on DHMH workstations and servers needs improvement.

- Our test of 10 computers disclosed that sufficient protection for malware was not established. Specifically, the anti-malware software used to protect DHMH computers was not properly configured to limit users' capabilities. In this regard, settings on 6 computers tested allowed users to exclude any files or folders from malware scans and to disable the anti-malware features rendering the software unable to protect against attacks. Additionally, 9 of the 10 computers were running an outdated version of the installed anti-malware software, and the remaining computer did not have anti-malware software protection enabled. The anti-malware vendor updated its software on a regular basis to fix operating problems identified with the software and to introduce new features.
- Certain workstations were configured with users having administrator rights. Administrator rights represent the highest permission level that can be granted to users and allow users to install software and change configuration settings. Our testing of seven workstations disclosed that, for five of the workstations, employees' user accounts were defined with administrator rights rather than with user rights and did not need these administrative rights. As a result, if these workstations were infected with malware, the malware would run with administrative rights and expose these workstations to a greater risk of compromise than if the employees' user accounts operated with only user rights.
- The computers we tested had not been updated with the latest releases for software products that are known to have significant security software related vulnerabilities. Although the vendors for these software products frequently provide software patches to address these vulnerabilities, DHMH had not

updated its workstations for these patches. For example, 7 of 10 computers tested for one of these software products were running older versions of this software.

Best practice guidance from the DoIT *Information Security Policy*, states that agencies should configure security settings of information technology products to the most restrictive mode consistent with operational requirements.

Recommendation 12

We recommend that DHMH

- a. disable the settings which allow users to exclude files from malware scans and override and modify default security controls established by management,**
- b. automatically update all computers for the latest versions of the anti-malware software and verify that the anti-malware software is enabled on all computers,**
- c. limit administrative rights on user workstations to only personnel who require such rights for their job duties, and**
- d. ensure that all computers are kept current for all critical security-related updates to potentially vulnerable installed software.**

Finding 13

Controls over the NEDSS database and the HMIS application were not sufficient.

Analysis

Controls over the NEDSS database and HMIS application were not sufficient.

- The NEDSS database was not configured to log any database security activity. Examples of database activities which should be logged and analyzed include, but are not limited to, direct changes to critical data tables, changes to database security settings, and use of certain critical privileges. This condition could result in unauthorized or inappropriate activities (affecting the integrity of the production database information) going undetected by management.
- Passwords for 11 NEDSS database system, user, and application accounts had no requirements with respect to length or complexity. Furthermore, two active default accounts still used their default passwords which were widely known. The DoIT *Information Security Policy* requires passwords to be a

minimum of eight characters and meet certain complexity requirements and further requires that all default system passwords be changed.

- Several critical security-related reports for the HMIS system either were not reviewed or were only reviewed for certain types of events (for example account deletions) but not for more significant changes, such as account additions and modifications. Accordingly, errors or unauthorized changes affecting HMIS data (such as patient hospital billings and receivables) could occur without detection by management. A similar condition has been commented upon in our three preceding audit reports.

Recommendation 13

We recommend that DHMH

- a. configure the NEDSS database to log all critical database security activity;**
- b. ensure that NEDSS database passwords comply with the DoIT *Information Security Policy* requirements with respect to length, complexity, and default values; and**
- c. review on a regular basis, all HMIS critical security-related reports for all significant security events (repeat).**

Capital Grant Project Checks

Finding 14

Proper internal controls were not established over the processing and handling of settlement checks issued for capital grant projects.

Analysis

Proper internal controls were not established over the processing and handling of settlement checks issued for capital grant projects. One Office of Capital Projects (OCP) employee had unilateral control over the disbursement process, and OCP did not perform an independent verification to ensure the proper disposition of these checks.

Specifically, the same employee submitted the payment request documentation, which was not approved by the OCP Director or any other supervisory personnel before submission; picked up the applicable check from the Comptroller of Maryland's General Accounting Division; and distributed the check to the grantee at settlement. Furthermore, OCP did not perform an independent verification of the disposition of each check requested to ensure that a settlement actually occurred and that the grantee acknowledged receipt of the check. Finally, this

employee was also responsible for reconciling the project grant expenditures to the State's accounting records. As a result, there is a lack of assurance as to the proper disposition of capital project grant settlement checks returned to DHMH for distribution.

Grants provide funding to eligible counties, municipalities, and nonprofit agencies for the acquisition, design, construction, renovation, and equipping of approved facilities that provide direct care services to certain individuals. OCP is responsible for the oversight of these capital project grant programs and the grant settlement process. During fiscal years 2012 and 2013, grants awarded totaled \$13.6 million and grant settlement checks returned for distribution totaled \$2.6 million.

Recommendation 14

We recommend that DHMH establish adequate internal controls over capital project checks issued for grant projects. Specifically, we recommend that

- a. grant payment requests submitted for processing be properly authorized by independent supervisory personnel,**
- b. the proper disposition of the checks be verified by independent personnel by sighting the grantee acknowledgment of receipt of the check at settlement, and**
- c. grant expenditures be reconciled to State records by personnel independent of the check processing functions.**

Equipment

Finding 15

DHMH record keeping and physical inventory procedures were not in compliance with certain DGS requirements.

Analysis

DHMH record keeping and physical inventory procedures were not in compliance with certain provisions of the Department of General Services' (DGS) *Inventory Control Manual*. DHMH's Office of the Secretary provides various support services to certain units of DHMH, including the maintenance of equipment records. According to DHMH's records, as of June 23, 2013, the value of the equipment for these units totaled approximately \$45.8 million.

- Equipment items purchased by DHMH were not always recorded in the detail equipment records and tagged as required. Specifically, our test of 76 equipment items purchased during fiscal years 2012 and 2013, totaling \$1.1

million, disclosed that 62 items costing a total of \$791,000 were not properly recorded in the detail records as of July 1, 2013, and 60 of those 62 items did not have property tags affixed.

- Physical inventories at three DHMH units, with equipment totaling \$4.3 million, were not certified in writing by the property officer who completed them, as required. In addition, as of July 15, 2013, the required annual physical inventory for one of the units, with \$1.9 million of sensitive inventory, had not been performed in three years.

DGS' *Inventory Control Manual* requires the recordation of all capital equipment items in the detail records for identification and control purposes and that proper identification be placed on each equipment item. In addition, the *Manual* requires that periodic physical inventories be conducted (annually for sensitive inventory), that variances be investigated and resolved, and that related documentation, including a certification in writing regarding the accuracy of the physical inventory, be retained for audit and verification purposes.

Recommendation 15

We recommend that DHMH comply with the requirements of the Department of General Services' *Inventory Control Manual*.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Office of the Secretary and other units of the Department of Health and Mental Hygiene (DHMH) for the period beginning October 15, 2009 to February 26, 2013. 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 DHMH'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 federal funds, audits of local health departments and private providers, grants, procurement and disbursement activities, corporate purchasing cards, cash receipts, payroll, financial investigations and related accounts receivable records for patients in State facilities, information system security, and equipment. We also determined the status of the findings contained in our preceding audit report.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of DHMH's operations, and tests of transactions. We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data), as well as from the contractor administering the State's Corporate Purchasing Card Program (credit card activity). 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 these various sources were sufficiently reliable for the purposes the data were used during this audit. We also extracted data from various key DHMH internal systems, such as the Hospital Management Information System for the purpose of testing accounts receivable for patients in State facilities. 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 objectives. The reliability of data used in this report for background or informational purposes was not assessed.

Our audit included a review of certain support services (for example, payroll, purchasing, maintenance of accounting records, and related fiscal functions) provided by DHMH's Office of the Secretary and related units to the other units of DHMH.

Our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of DHMH's compliance with federal laws and regulations pertaining to those programs because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including DHMH.

DHMH's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider significant deficiencies in the design or operation of internal control that could adversely affect DHMH'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, and regulations. Other less significant findings were communicated to DHMH that did not warrant inclusion in this report.

DHMH'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 DHMH regarding the results of our review of its response.



STATE OF MARYLAND

DHMH

Maryland Department of Health and Mental Hygiene

Lawrence J. Hogan, Jr., Governor - Boyd K. Rutherford, Lt. Governor - Van T. Mitchell, Secretary

APPENDIX

February 12, 2015

Mr. Thomas J. Barnickel, III, CPA
Legislative Auditor
Office of Legislative Audits
301 West Preston Street
Baltimore, MD 21201

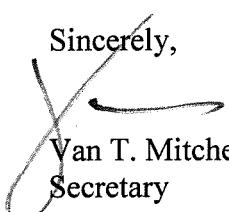
Dear Mr. Barnickel:

Thank you for your letter regarding the draft audit report for the Department of Health and Mental Hygiene – Office of the Secretary and Other Units for the period beginning October 15, 2009 through February 26, 2013. Enclosed you will find the Department's response and plan of correction that addresses each audit recommendation.

I will work with the appropriate administration directors, program directors and deputy secretary to promptly address the audit exceptions. In addition, the Office of the Inspector General's Division of Internal Audits will follow up on the recommendations to ensure compliance.

If you have any questions or require additional information, please do not hesitate to contact me at 410-767-4639 or Thomas V. Russell, Inspector General, at 410-767-5862.

Sincerely,


Van T. Mitchell
Secretary

Enclosure

cc: Thomas Kim, Deputy Secretary for Operations, DHMH
Charles Lehman, Director of Information Technology, DHMH
Thomas V. Russell, Inspector General, DHMH
Elizabeth Morgan, Acting Assistant Inspector General, DHMH
Shawn Cain, Chief of Staff, DHMH

Department of Health and Mental Hygiene, Office of the Secretary

Finding 1

DHMH did not formally communicate certain pertinent aspects of the MERP procurement process and the potential risks regarding the award decision when it sought Board of Public Works (BPW) approval of the contract.

Recommendation 1

We recommend that, in the future, DHMH ensure that all pertinent circumstances regarding significant procurement award decisions, including potential risks, are clearly documented and conveyed to BPW for its consideration of contracts submitted for approval.

Administration's Response

The Administration does not concur with the finding. The procurement was fully compliant with State law and regulations, and DHMH identified and explained to BPW and other staff the legal issue that arose at the end of the procurement. On February 15, 2012, prior to the meeting of the BPW in which the contract was approved, DHMH made a presentation to all key BPW staff concerning the legal issue. Counsel to DHMH later sent to BPW's legal counsel the cases that support DHMH's position on the issue.¹

Finding 2

The LTSS information technology (IT) project was not adequately planned nor was DoIT approval obtained when the project was initiated. The use of the MOU resulted in the project work not being subject to competitive procurement as would normally be required by State procurement regulations.

¹**Auditor's Comment:** DHMH's response indicates that it does not agree with the finding because the MERP procurement was fully compliant with State laws and regulations. Our report did not state that any State laws or regulations were violated. Rather, the report stated that DHMH did not formally communicate certain matters to the BPW or its staff. Specifically, there was a lack of evidence that the BPW or its staff were apprised that RFP qualifications were changed to obtain bidders, that the successful bidder had past performance issues involving similar projects, and that a change was made to the contractor liability provisions after the successful bidder was notified of the award. DHMH stated in its response that the contractor liability issue was explained at a pre-meeting to BPW staff, which we noted in the audit report. However, other than this issue, the actual topics discussed could not be recalled by a number of individuals who attended the pre-meeting. Furthermore, there was no evidence that this issue, as well as the other matters pertaining to this contract, were clearly identified and conveyed to the BPW at its meeting when contract approval was being sought.

Recommendation 2

We recommend that DHMH ensure that, in the future,

- a. all information technology projects are properly planned, with their full scope and anticipated funding needs identified prior to implementation;**
- b. all qualifying projects are submitted to DoIT for review and oversight prior to their initiation;**
- c. formal arrangements with state agencies are closely evaluated to ensure that the required services should not otherwise be obtained through a competitive procurement process; and**
- d. all MOU provisions requiring the review and approval of significant subcontracts are complied with.**

Administration's Response

- a. The Administration concurs and every effort will be made to ensure all information technology projects are planned, with the full scope and funding needs identified prior to implementation. We note however, that this goal may not always be possible to attain, as some information technology projects change after they are started. When this occurs, the Department will disclose the change and follow the appropriate procedure, as it did in this case.²
- b. The Administration concurs and will make every effort to ensure all qualifying projects are submitted to DoIT for review and oversight prior to initiation. We note however, some projects start when they are not qualifying as a Major IT Project, as in this case. In December 2012, DHMH voluntarily and immediately sought DoIT oversight when it recognized that the expansion of the Hilltop-led LTSS project had caused that project to become a “major IT development project” for purposes of the law requiring DoIT oversight.²
- c. The Administration concurs and will ensure that formal arrangements with state agencies are closely evaluated to ensure that the required services should not otherwise be obtained through a competitive procurement process.
- d. The Administration concurs and will ensure that all MOU provisions requiring the review and approval of significant subcontracts are complied with.

² **Auditor's Comment:** While DHMH agrees with the recommendations, its response indicates that it may not always be able to plan the full scope and funding needs of all IT projects and submit major projects to DoIT prior to implementation. Specifically, DHMH states that some projects may change after they are started and may not initially qualify as a major IT project. However, comprehensive project planning and oversight, as discussed in the finding, would minimize such instances and would provide DHMH with the opportunity to readily identify major IT projects so that the full benefits of DoIT oversight could be obtained. In addition, DoIT advised DHMH that it should have been involved from the start of the project.

Finding 3

The OIG had not established formal written policies for conducting provider grant audits in a timely manner and in accordance with established professional standards.

Recommendation 3

We recommend that the OIG

- a. establish a written policy to govern the timely completion of its grant audits,**
- b. complete its grant audits on a timely basis, and**
- c. establish a formal policy requiring LHD and private non-profit provider grant audits to be conducted in accordance with professional standards.**

Administration's Response

- a. We concur in part. While it is our intention to develop a written policy to govern the timely completion of its grant audits, the division does not concur with the finding that audits be completed within an "established 4 year audit cycle." The Fiscal Services Administration, (FSA), policy requiring a 4 year grant audit cycle plan was in effect when the Division was under the control of the FSA. Subsequent to the Division being moved to the Office of Inspector General (OIG), the policy was not considered to be in effect. In addition, the FSA policy was not mandated by regulation or statute. Once the Division was placed under the OIG, and after reviewing the deficiencies in the previous audit reports, a new audit chief was hired to re-engineer the audit process in effect at the time. Thus, the division is currently in the process of working to eliminate the audit "backlog", at which time a specific policy governing the timely completion of the grant audits will be implemented.
- b. We concur. An audit plan will be developed in conjunction with the recent hiring of a new audit chief. It is our objective to establish and annually update the audit schedule based upon funding levels and risk assessments which will also take into consideration expiring record retention periods. The plan and any updates will also take into account the exigent needs for investigations, as the Department is often asked to review and investigate various issues requiring the OIG to prioritize audits and investigations accordingly.
- c. We concur. The Division's goal is for every audit to meet generally accepted auditing and government auditing standards. Within the last several years, the Division has increased the quality of its audits with improvements to the following areas:
 - Audit Planning
 - Internal Controls and Risk Assessment
 - Testing Procedures
 - Supervisory Oversight

Finding 4

The OIG did not adequately verify LHD and private non-profit provider compliance with sub-vendor audit and oversight requirements.

Recommendation 4

We recommend that the OIG properly verify LHD and private non-profit provider compliance with sub-vendor audit and oversight requirements during its audits of these entities in accordance with established DHMH standards.

Administration's Response

We concur with the recommendation. As a result of recent improvements in the audit process, the Audit Division's Internal Control Questionnaire, audit programs and testing procedures now address the issues noted.

Finding 5

Records for open patient financial investigations were not properly maintained and monitored. In addition, investigations were not always timely conducted and reviewed by supervisory personnel.

Recommendation 5

We recommend that DHMH ensure that

- a. open patient financial investigation records are properly maintained and monitored, and**
- b. financial investigations are timely conducted.**

Administration's Response

- a. We concur that the open patient financial investigation records were not properly maintained and monitored.

The Division will be working with the HMIS project team to review current protocols and determine a more effective way to ensure all completed investigations are sent to the HMIS team are successfully cleared from the report.

Additionally, the staff at the field offices will continue to review the report monthly to determine which accounts need to be removed due to completion and which accounts need further investigation before completion. The Financial Agent Supervisor at each office will now be advised that they must review, on a monthly basis, all open investigations with each

agent in an attempt to expedite the completion of the investigations. For more effective controls, each Financial Agent Supervisor will be advised that he/she must forward the completed report each month to the Financial Agent Operations Chief for review.

- b. We concur that the financial investigations should be timely conducted.

The Financial Agent Supervisor and the Field Chief will conduct monthly reviews of all open investigations with all of their subordinate agents to determine why investigations are incomplete and what can be done to expedite the completion of the investigation in a timely manner. There are many valid reasons that an investigation may be incomplete and ongoing and more aggressive monitoring of each of these categories will be included in the supervisory responsibilities. All accounts without a valid reason to be open will continue to be pursued and investigated until resolved and rated for billing. If the account cannot be rated due to the failure on the part of the patient or their family to provide the required financial information, the account will be rated at the full per diem cost in accordance with regulations, billed for the required number of billings, and then transferred to CCU for action. Again, administrative action with our HMIS team will be taken to remove all accounts that have been completed and rated but remain on the open accounts list.

Finding 6

DHMH did not adequately pursue collection of delinquent DCAR accounts receivables. Furthermore, denied insurance and Medicare claims were not timely resolved.

Recommendation 6

We recommend that DHMH ensure

- a. **delinquent accounts receivable are adequately pursued for collection and transferred to CCU as required (repeat); and**
- b. **denied insurance and Medicare claims are timely resolved.**

Administration's Response

- a. We concur with the recommendation and will ensure delinquent account receivables are adequately pursued for collection and transferred to CCU as required.
In addition to the supervisory controls instituted as a result of the prior audit recommendation, DCAR will implement another level of supervisor review. For delinquent accounts determined by the financial agent offices, the Chief for Field Operations will conduct a monthly review of accounts to determine which accounts to transfer to CCU within the 120 day statute. In addition, procedures are being instituted for each Financial Agent Supervisor to review and complete the private pay aging report and the unrated aging report

at the 90 day period to ensure proper review in advance of the 120 day statutory limit. These reports will be forwarded to the Financial Agent Operations Chief each month for review. For Insurance accounts, the Fiscal Services Manager will perform a review of all accounts that remain denied by the insurer after all claim appeals, and transfer subject accounts to CCU. DCAR will be exploring the feasibility of developing tools to automate some of the manual steps required in this process.

- b. We concur that denied insurance and Medicare claims were not timely resolved. Denied insurance will be addressed upon denial and corrected or referred to the hospital for medical care response where appropriate. Late filing and coding errors pertaining to Medicare claims were due to the improper training of staff. The Division has had to rebuild its Medicare billing unit as a result of retirements of its senior Medicare supervisors. The remaining staff had not been trained properly to resolve denied claims in the timeliest manner. In FY 2013 new staff were hired and properly trained in Medicare billing and claims resolution. As a result of the hiring and training, there has been a significant decrease in Medicare claim errors and the denied claims are being addressed upon denial. As a result of the new staff, Medicare denials have decreased and revenues increased.

Finding 7

DCAR lacked appropriate procedures to ensure all cash receipts were deposited.

Recommendation 7

We recommend that DHMH ensure that

- a. the employee who prepares the initial record of collections forwards a copy of that record directly to the employee responsible for the deposit verification, and
- b. the employee performing the deposit verification not have access to the related cash receipts.

We advised DHMH on accomplishing the necessary separation of duties using existing personnel.

Administration's Response

We concur that the deposit verification procedures were inadequate.

- a. We concur with the recommendation. However, due to the limited number of staff at the time, it was necessary to utilize the DCAR's former Auditor to deposit the collections in a timely manner. That issue has been resolved because the former Auditor is no longer

employed at DCAR and the hiring of additional staff has helped with appropriately assigning these functions to different staff.

- b. We concur with the recommendation to separate the duties of processing receipts and deposit. As a result, DCAR has implemented the following procedure in accordance to the Auditor's recommendation as of July 28, 2013:
- The Office Secretary opens and date stamps all mail.
 - The Office Secretary runs 2 tapes; photocopies the tapes, and the checks.
 - The checks and 1 tape are given to the Cashier.
 - The Office Secretary files one original tape in a binder along with the check copies and gives the other tape to the DCAR Auditor for reconciliation.
 - The Cashier performs regular deposit duties.

Through these changes, the current DCAR Auditor does not handle the checks, nor does he have HMIS access.

Additionally the Division will be testing scanning equipment to improve this process. We anticipate this equipment will allow for the scanning of checks for direct deposit. After testing, a determination will be made regarding any additional policies, training and resources needed to implement this new process.

Finding 8

Supervisory oversight of federal fund reimbursement requests was not always effective.

Recommendation 8

We recommend that DHMH ensure that federal fund reimbursement requests are properly reviewed, along with supporting schedules and documents, and the reviews are documented.

Administration's Response

We concur with the auditor's recommendation.

Effective August 2014, as a federal draw request is received from an agency, Fiscal Services personnel ensures that two signatures/initials (requestor and supervisor) are present. In turn, before Fiscal Services submits a federal drawdown request to the State Treasurer, it will be signed / initialed by preparer and a supervisor.

Finding 9

Corporate purchasing card transactions were not always thoroughly reviewed and supported, which allowed certain improper purchases to go undetected.

Recommendation 9

We recommend that DHMH

- a. ensure that all corporate card purchases are supported by appropriate documentation and thoroughly reviewed by supervisory personnel,**
- b. ensure that purchasing card activity logs and the related monthly cardholder statements are signed as required, and**
- c. incorporate and document the use of Level-3 purchasing card data in the supervisory review of the activity logs to help ensure the propriety of CPC activity.**

Administration's Response

We concur with the auditor's recommendation.

- a.,b. Due to DHMH's size, assurance that certain corporate credit card program requirements (i.e. supervisory review to ensure adequate supporting documentation for purchases, presence of required signatures, etc.) is decentralized. However, both Fiscal Services Administration and the Office of the Inspector General perform monthly audits of select CPC transactions and documentation. In addition, each month the Purchasing Card Program's designated fiscal officers and administrators certify that the aforementioned has been performed. CPC fiscal officers are responsible for maintaining corporate purchasing card documentation for audit. Therefore, Fiscal Services Administration will send them a monthly reminder that they must ensure that all transactions are supported by adequate documentation and forms/statements are properly signed.
- c. On a monthly basis, Fiscal Services Administration sends Level 3 purchasing card data to the Office of the Inspector General, each agency's Chief Fiscal Officer, along with their designated fiscal officer and administrator for the Corporate Purchasing Card Program. To comply with auditors' recommendation, when Fiscal Services sends Level 3 data, fiscal officers are instructed that they are required to review and share the Level 3 data with all of their reviewers (Authorized Reviewer Agreement - Exhibit H). In addition, we have added Level 3 review requirements to the certification statement at the bottom of the Activity Log which reads: "... The authorized reviewer per the cardholder's Exhibit H must review the Activity Log and bank statement, along with documentation (original invoices and electronic Level 3 report) detailing each charge/credit to ensure their propriety. To document the above, the cardholder and authorized reviewer must sign and date all pages of the Activity Log and the monthly bank statement..."

Additionally, DHMH believes that based on the monthly reviews performed by the Office of Inspector General, a performance best practice is in effect as it relates to Level 3 data.

Finding 10

Intrusion detection prevention system coverage and controls for the DHMH network were not sufficient.

Recommendation 10

We recommend that DHMH

- a. provide adequate IDPS coverage for all servers in the aforementioned neutral network zone,**
- b. limit network-level administrative access to the network-based IDPS device to only those users requiring such access, and**
- c. ensure that password and account controls over the network-based IDPS device comply with DoIT requirements.**

Administration's Response

The Administration concurs with the findings and we have already implemented the recommendations in March 2014. We have therefore:

- a. implemented IDPS coverage for the specified zones,
- b. limited sources for administrative access as recommended, and
- c. configured IDPS authentication to appropriately comply with DoIT requirements.

Finding 11

Network access to critical internal network devices was not properly restricted and monitoring of security events over a critical firewall was not adequate.

Recommendation 11

We recommend that DHMH

- a. configure its firewalls to properly protect all critical network devices; (repeat)**
- b. configure the aggregation device to include Internet firewall security-related activities such as configuration changes and failed logon attempts; and**
- c. review and analyze the reports of Internet firewall activity from this aggregation device, document these reviews, and retain the documentation for future reference.**

Administration's Response

The Administration concurs with the findings and we have already implemented the recommendations in March 2014. We have therefore:

- a. configured firewalls to protect critical network devices and established a semi-annual rule review process by security staff,
- b. configured the aggregation device to include the recommended security related activities, and
- c. established procedures for daily log review and documentation which is archived for future reference.

Finding 12

Malware protection on DHMH workstations and servers needs improvement.

Recommendation 12

We recommend that DHMH

- a. disable the settings which allow users to exclude files from malware scans and override and modify default security controls established by management,**
- b. automatically update all computers for the latest versions of the anti-malware software and verify that the anti-malware software is enabled on all computers,**
- c. limit administrative rights on user workstations to only personnel who require such rights for their job duties, and**
- d. ensure that all computers are kept current for all critical security-related updates to potentially vulnerable installed software.**

Administration's Response

The Administration concurs with the findings and we have already implemented the recommendations in March 2014. We have therefore:

- a. automated the recommended settings via a centralized management server,
- b. likewise automated the recommended settings via a centralized management server,
- c. established procedures for identifying and authorizing users for administrative workstation access, and implemented controls to limit access,
- d. automated critical security-related updates to computers via a centralized management platform.

Finding 13

Controls over the NEDSS database and the HMIS application were not sufficient.

Recommendation 13

We recommend that DHMH

- a. configure the NEDSS database to log all critical database security activity;**
- b. ensure that NEDSS database passwords comply with the DoIT *Information Security Policy* requirements with respect to length, complexity, and default values; and**
- c. review on a regular basis, all HMIS critical security-related reports for all significant security events (repeat).**

Administration's Response

- a. The Administration concurs with this finding and recommendation. The NEDSS database has been configured to log all critical database security activity. Logs will be reviewed on a weekly basis by a third party who has been trained on what to search for.
- b. The Administration concurs with this finding and recommendation. Database passwords strengthening are being worked on with CDC contractor. The solution is currently being tested on the NEDSS test system. It is expected that by March 2015 the evaluation and testing will be completed and the new solution will be implemented on the production and failover servers.
 - Passwords implemented on test and eventually production servers are required to have at least 1 or more capital letters, at least 1 or more special characters, at least 1 or more numbers and at least 8 characters in length.
 - Default accounts have been disabled on all servers.
- c. The Administration concurs with this finding and recommendation. The HMIS security work flow has been updated to include the review of all HMIS critical security-related reports on a regular basis. As of early October 2014, all reviews are being documented. The HMIS Security Policy & Procedures manual has been revised to clarify this audit control responsibility. Similarly, report reviewing guidelines have been updated.

Finding 14

Proper internal controls were not established over the processing and handling of settlement checks issued for capital grant projects.

Recommendation 14

We recommend that DHMH establish adequate internal controls over capital project checks issued for grant projects. Specifically, we recommend that

- a. grant payment requests submitted for processing be properly authorized by independent supervisory personnel,**
- b. the proper disposition of the checks be verified by independent personnel by sighting the grantee acknowledgment of receipt of the check at settlement, and**
- c. grant expenditures be reconciled to State records by personnel independent of the check processing functions.**

Administration's Response

- a. The Administration concurs that the internal controls over the processing and handling of capital project grant checks returned for distribution at settlement were inadequate and has established adequate internal controls over its Capital Project check disbursements. Specifically, OCPBES has implemented processes that require grant payment requests submitted to DGA to be properly authorized by independent management personnel. Once the BPW approves the project:
 - The Payment Request form is completed and electronically sent by the OCPBES to the grantee for signature.
 - After the responsible person for the grantee signs the Payment Request it is returned electronically to OCPBES.
 - The Payment Request Form, Payment Block Form and the General Accounting Memo are prepared. The General Accounting Memo is signed by independent management personnel for proper authorization. The forms are sent to General Accounting for processing.
 - The check, once ready, is picked up from the Comptroller's Office and signed for by an authorized person from OCPBES
 - In the OCPBES a copy of the check is made and signed by a supervisor and the person picking up the check indicating the date the check was received in OCPBES.
 - The check is deposited in the General Accounting safe until settlement date.
 - Independent management personnel signature indicating the removal of the check from the safe on the day of settlement to be delivered to Grantee.
- b. The Administration concurs. Effective immediately, proper disposition of the checks will be verified by independent personnel by sighting the "right of recovery" form signed by the vendor at settlement acknowledging receipt of the check. OCPBES utilizes a tracking log to verify proper disposition of checks consisting of the following information:
 - Grantees Name

- Property Address
- Settlement date
- Check number
- Amount of the check
- Signature of the OCPBES representative delivering the check to Settlement.
- Signature and title of the responsible Grantee/representative receiving the check at settlement.
- Signature of OCPBES representative at settlement indicating the Right of Recovery (ROR) was received at Settlement.
- Supervisor's review and signature for Disposition of Check and Right of Recovery.
- The check tracking log and the copy of the check are put in a folder for record keeping.

c. The Administration concurs. We are currently performing the independent invoice verification process but we will strengthen our procedures by adding a signature sheet for documenting the independent personnel that performs the reconciliation process.

Finding 15

DHMH record keeping and physical inventory procedures were not in compliance with certain DGS requirements.

Recommendation 15

We recommend that DHMH comply with the requirements of the Department of General Services' *Inventory Control Manual*.

Administration's Response

The Administration concurs. The majority of the items identified in the audit was a part of the OPR equipment inventory and have been since added to the inventory records. Also, the Department performs an audit of the corporate credit purchases to ensure that required items are added to the physical records and properly tagged. All future equipment will be properly certified in writing by the Department's Property Accountable Officers.

In FY13, OPR took steps to secure the services of a vendor to assist us in conducting a complete inventory of items purchased through the federal grant programs that OPR administers. The vendor was initially secured for our Health and Medical Regions 1 and 2 in Western Maryland as a phase I test. That process was completed and through a larger contract, a vendor was secured to complete a similar inventory process in the other three Health and Medical Regions. The process should be completed by the end of this calendar year having accounted for every health and

medical region in the state- all 24 local jurisdictions. While the current process is a physical inventory to ensure that reportable items are accounted for and appropriately tagged, it will also encompass the OPR sensitive audit requirements. In addition, OPR met with the DHMH Central Services Division to clarify the inventory accounting requirements, establish procedures for accountability of items that may be directly shipped to the end user and clarify procedures and documentation for the transfer of items to the appropriate administration, agency, or healthcare facility inventory. OPR will meet again with the DHMH Central Services Division when the physical inventory is completed to review the results and ensure that the documentation is complete. OPR should then be prepared to meet all the requirements of the sensitive audit and the physical audit going forward.

AUDIT TEAM

William R. Smith, CPA

Audit Manager

Richard L. Carter, CISA

Stephen P. Jersey, CPA, CISA

Information Systems Audit Managers

Raymond G. Burton, CPA, CFE

Senior Auditor

Michael K. Bliss, CISA

Edwin L. Paul, CPA, CISA

Information Systems Senior Auditors

Daniel R. Brann

Timothy S. Rice

Tu N. Vuong

Staff Auditors

Matthew D. Walbert

Information Systems Staff Auditor