

Audit Report

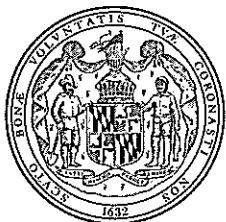
**Department of Health and Mental Hygiene
Regulatory Services**

November 2011



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

November 7, 2011

Karl S. Aro
Executive Director

Bruce A. Myers, CPA
Legislative Auditor

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

Ladies and Gentlemen:

We have audited Regulatory Services, a budgetary unit within the Department of Health and Mental Hygiene (DHMH), for the period beginning February 1, 2008 and ending August 2, 2010. Regulatory Services (hereinafter referred to as the Unit) consists of the following units:

- Health Professional Boards and Commission (comprised of 16 separate boards and one commission)
- Board of Nursing
- Board of Physicians
- Office of Health Care Quality (OHCQ)

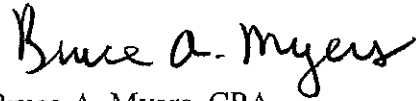
The entities comprising the Unit are responsible for licensing and regulating health professionals (such as physicians, nurses, and pharmacists) and health care facilities in the State. As further explained on page 4 of this report, the Unit was created based on certain organizational changes made within DHMH.

Our audit disclosed that certain boards had not established adequate control and accountability over licenses and related cash receipts. For example, as commented upon in our audit reports dating back to 1987, one of these boards did not reconcile the value of licenses issued to the related cash receipts. This condition contributed to the failure of the board to detect in a timely manner the apparent fraudulent sale and distribution of certain certificates.

We also noted that certain health care facilities were not inspected by OHCQ as required. For example, OHCQ had not performed inspections for 725 of the 1,367 (53 percent) licensed assisted living facilities during fiscal year 2010. Finally, we identified certain security and control deficiencies pertaining to one board's information systems.

DHMH's response to this audit, on behalf of the Unit, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by the Unit.

Respectfully submitted,

A handwritten signature in black ink that reads "Bruce A. Myers". The signature is written in a cursive, flowing style.

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

Background Information	4
Organizational Change and Agency Responsibilities	4
Status of Findings From Preceding Audit Reports	4
Findings and Recommendations	6
Licensing Controls and Cash Receipts	
* Finding 1 – Certain Boards Had Not Established Sufficient Controls Over the Accounting for Professional Licenses and Related Collections	6
Health Care Facility Inspections	
* Finding 2 – The Office of Health Care Quality Had Not Conducted Annual Inspections of Certain Health Care Facilities as Required	7
Information Systems Security and Control	
Finding 3 – An Information Technology Contract of the Board of Nursing Did Not Contain Specific Provisions Obligating the Vendor to Address Certain Risks	9
* Finding 4 – The Board of Nursing Did Not Have a Complete Disaster Recovery Plan and Certain Licensing Database Controls Were Not Sufficient	10
Audit Scope, Objectives, and Methodology	12
Agency Response	Appendix

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

Background Information

Organizational Change and Agency Responsibilities

Chapter 484, Laws of Maryland, effective July 1, 2009 (Budget Bill) created Regulatory Services as a separate budgetary unit within the Department of Health and Mental Hygiene (DHMH) consisting of

- Health Professional Boards and Commission (comprised of 16 separate boards and one commission),
- Board of Nursing,
- Board of Physicians, and
- Office of Health Care Quality (OHCQ).

Prior to this organizational change, these entities were budgeted within DHMH – Office of the Secretary.

The various boards and commission are responsible for licensing and regulating health professionals (such as physicians, nurses, and pharmacists) in the State. OHCQ is responsible for regulating health care facilities. According to the State's records, fiscal year 2010 expenditures for the Unit totaled approximately \$40.8 million.

The results of our most recent audit of the Health Professional Boards and Commission, the Board of Nursing, and the Board of Physicians were commented upon in our report dated January 21, 2009 and covered the period from June 1, 2005 through January 31, 2008. Accordingly, our current audit of the Unit included these entities for the period from February 1, 2008 through August 2, 2010.

Prior to July 1, 2009, OHCQ was included within the scope of our audits of DHMH – Office of the Secretary. Our current audit of the Unit included OHCQ for the period from July 1, 2009 through August 2, 2010.

Status of Findings From Preceding Audit Reports

Our audit included a review to determine the status of the eight findings contained in our preceding audit report on the Health Professional Boards and Commission, the Board of Nursing, and the Board of Physicians dated January 21, 2009. We have determined that the applicable boards satisfactorily addressed six of the findings. The remaining two findings are repeated in this report.

Our audit also included a review to determine the status of one of the findings in our preceding audit report, dated August 8, 2007, on DHMH – Office of the Secretary related to the Office of Health Care Quality. The finding was not satisfactorily addressed and is repeated in this report.

Findings and Recommendations

Licensing Controls and Cash Receipts

Finding 1

Certain boards had not established sufficient controls over the accounting for professional licenses and related collections.

Analysis

Adequate accountability and control over professional licenses and related collections had not been established at two of the three boards reviewed. According to Department of Health and Mental Hygiene (DHMH) records, during fiscal year 2010, cash receipts for the two boards (that is, the Boards of Nursing and Pharmacy) totaled approximately \$9 million. In addition, during fiscal year 2010 the two boards issued and renewed approximately 288,000 licenses. Our review disclosed the following conditions:

- The Board of Nursing employee who performed the deposit verification was not independent, as this employee also prepared and made the deposit. In addition, this same employee recorded bank deposits in the State's accounting records, and processed charge backs resulting from checks that were dishonored by the bank. Due to the lack of adequate controls, this employee could misappropriate cash receipts without detection. According to the Board's records, during fiscal year 2010, the Board's cash receipts totaled approximately \$6.8 million. The lack of adequate deposit verifications by certain boards has been commented upon in our audit reports dating back to 2002.
- Both boards had not reconciled the value of licenses issued with the related collections. The lack of such reconciliations by certain boards has been commented upon in our audit reports dating back to 1983, including the Board of Nursing since 1987. This control deficiency contributed to the failure to detect in a timely manner the alleged fraudulent sale and distribution of certain nursing certificates at the Board of Nursing. Specifically, in May 2009, the Board received an allegation related to the possible fraudulent sale and distribution of certificates by one of its employees. The Board referred the allegation to DHMH's Office of the Inspector General (OIG) for further review. Based on the preliminary results of the OIG's investigation, on June 5, 2009, the Board terminated the employee for misconduct. The OIG issued a report in August 2009 and concluded that the employee in question had erroneously issued at least 19 certificates using names of persons who either had not applied for certification and/or did not meet the minimum

qualifications required for certification. No funds were deposited for the licenses issued. The OIG further reported that the employee may have personally profited in the amount of \$11,400 from the sale of the 19 certificates over several years. The OIG referred this matter to the Office of the Attorney General – Criminal Division in August 2009 for further investigation. A referral to the Criminal Division does not mean that a criminal act has actually occurred or that criminal charges will be filed. In addition, the OIG recommended that the Board improve controls over license issuance and related collections and continue its investigation to ensure the legitimacy of issued certificates. While the Board instituted some corrective actions, at the time of our review, it still had not established procedures to reconcile licenses issued with collections received. As of November 1, 2011, the investigation was ongoing.

- The Board of Pharmacy did not periodically account for the pre-numbered licenses as to issued, voided, or on hand. The lack of periodic accountings for pre-numbered licenses by certain boards has been commented upon in our audit reports dating back to 1991.

Recommendation 1

We recommend that the applicable Boards

- a. establish procedures to ensure that an employee independent of the collections verifies that all amounts received are deposited and recorded in the State’s accounting records (repeat);**
- b. verify that all licenses issued were paid for and were proper (repeat); and**
- c. periodically account for all licenses as being issued, voided and/or on-hand (repeat).**

Health Care Facility Inspections

Finding 2

The Office of Health Care Quality (OHCQ) had not conducted annual inspections of certain health care facilities as required.

Analysis

OHCQ had not inspected certain health care facilities as required. OHCQ is required to conduct inspections of these facilities at least annually to ensure facility compliance with State and federal regulations regarding patient care and safety.

According to its records, which we determined to be reliable, for fiscal year 2010, OHCQ had not performed inspections for 725 of the 1,367 (53 percent) licensed assisted living facilities nor inspected 154 of the 201 (76 percent) facilities for the developmentally disabled. In addition, OHCQ had not inspected any of the 15 related resource coordination agencies (which are primarily county health departments) responsible for developing appropriate individualized plans for developmentally disabled individuals. DHMH inspections would include reviews of the adequacy of these plans.

Similar situations were commented upon in our two preceding audit reports of DHMH – Office of the Secretary. DHMH management again indicated that an increasing workload, combined with reductions in staff, have caused the delays in performing required inspections and they are continuing efforts to improve inspection processes to gain efficiencies.

Recommendation 2

We recommend that OHCQ complete inspections of the various health care facilities, as required by law (repeat).

Information Systems Security and Control

Background

Thirteen boards and one commission have licensing systems maintained by the Unit's information technology staff on a consolidated licensing application database system. The remaining five boards maintain licensing systems residing on servers located at each board's office and principally utilize application security to provide system security. Additionally, several boards provide an online license verification service to the general public and numerous boards offer online license renewals.

Our audit of these systems was limited to the review of select database system controls for the Board of Physicians, the Board of Nursing, and the Unit's consolidated licensing database. Our audit also included the review of certain other general controls (such as file backup procedures and disaster recovery planning) for the Board of Nursing.

In addition, the Board of Nursing has contracted with an information technology vendor for a document imaging system and an online web-based application required for nursing license renewals and related application processing. The vendor provides support for the Board's system and computer applications along with maintenance of data records residing on the Board's in-house databases. These databases contain certain sensitive personal information such as social

security numbers of licensees. The vendor was awarded a sole source five-year contract from July 1, 2009 through June 30, 2014 for an amount not to exceed \$2,337,479.

Finding 3

The Board of Nursing's contract with its licensing service vendor did not include provisions obligating the vendor to address certain significant information technology security and operational risks.

Analysis

The contract between the Board and its licensing services vendor did not contain specific provisions obligating the vendor to address certain significant information technology security and operational risks, including risks over sensitive client data (such as social security numbers). Furthermore, the Board did not ensure that the vendor had established proper controls to ensure security over the related data. Typically, such assurance is obtained through an independent examination of controls by an audit firm engaged by the vendor.

The contract did not establish expectations relative to significant risks in order to reduce the risks associated with outsourcing information technology operations as outlined in guidance issued by the Cloud Security Alliance. For example, we noted that the aforementioned contract lacked specific provisions addressing the following issues:

Data Security

- Migration of data both within the vendor's operating environment and to alternate service provider organizations
- Controls to prevent impermissible copying and/or removal of the Board's data

Data Segregation

- The segregation of the Board's data from data of other vendor clients when systems for multiple clients are hosted on the same server
- Periodic monitoring to ensure that vendor data segregation policies are not violated

Contract Termination and Service Exit Plan

- Upon contract termination, the process for the safe return of the Board's data

The Cloud Security Alliance, a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing, has issued *Security Guidance for Critical Areas of Focus in Cloud Computing*, dated December 2009, which addresses security best practices when using services of this nature and has been widely adopted. Cloud computing refers to the use of Internet-based services and resources to provide computing services, such as data processing and storage, to customers. These services are typically performed by vendors (service organizations). This guidance outlines the operational and security risks associated with these services and the related recommendations to mitigate these risks. Furthermore, the American Institute of Certified Public Accountants has provided detailed guidance for performing an examination to report on a service organization's controls (SOC) over its system relevant to security, availability, processing integrity, confidentiality, and privacy. Such a report on management's description of a service organization's system and the suitability of the design and operating effectiveness of the controls is referred to as a SOC 2, type 2 report.

Recommendation 3

We recommend that the Board

- a. obtain assurances from the vendor that it has addressed critical data security and operational risks, including safeguards for sensitive data;**
- b. request that the vendor periodically provide sufficient evidence that controls pertaining to such risks are effective; and**
- c. include in future IT contracts, involving cloud computing services with significant risks, provisions that require the vendor to address critical security and operational risks and to periodically obtain an examination of its system controls (for example by requiring the vendor to periodically obtain a SOC 2, type 2 report).**

Finding 4

The Board of Nursing did not have a complete disaster recovery plan and controls over the licensing database were not sufficient.

Analysis

The Board did not have a complete disaster recovery plan and controls over its in-house licensing database were not sufficient. Specifically, we noted the following conditions:

- The Board did not have a complete information technology disaster recovery plan (DRP) for recovering from disaster scenarios (for example, a fire). For example, the DRP did not address alternate site processing arrangements, prioritization of systems for recovery, restoration of network connectivity, and

plan testing. Without a complete DRP, a disaster could cause significant delays (for an undetermined period of time) in restoring information systems operations above and beyond the expected delays that would exist in a planned recovery scenario.

- Auditing capabilities were not enabled for the licensing database. Accordingly, critical security data were not collected and analyzed. Examples of database activities which should be logged and analyzed include direct changes to critical data tables and use of certain critical privileges. Therefore, unauthorized or inappropriate activities, affecting the integrity of the production database information, could occur and not be detected by management. A similar condition was commented upon in our preceding audit report.
- Database account and password controls were not in compliance with the Department of Information Technology's (DoIT) *Information Security Policy*. In particular, password aging, complexity and history, and account lockout settings were not established for certain critical database accounts.
- Procedures to store backups of this database offsite did not exist. As a result of this condition, in the event of a disaster, the Board could lose a significant amount of data that it could not readily recreate.

Recommendation 4

We recommend that the Board

- a. develop a complete DRP that, at a minimum, addresses the basic elements needed for a comprehensive disaster recovery plan;**
- b. log all significant database security and audit events (repeat);**
- c. verify that database password and account controls are in compliance with the requirements of the DoIT *Information Security Policy*; and**
- d. ensure that the licensing database backups are stored at a secure off-site location.**

Audit Scope, Objectives, and Methodology

We have audited the Regulatory Services Unit of the Department of Health and Mental Hygiene (DHMH) for the period beginning February 1, 2008 and ending August 2, 2010. The Unit consists of the Health Professionals Boards and Commission (comprised of 16 separate boards and one commission), the Board of Nursing, the Board of Physicians, and the Office of Health Care Quality (OHCQ). The Unit was created as a result of certain organizational changes made within DHMH. 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 the Unit's financial transactions, records and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations. We also determined the status of the findings included in our preceding audit reports.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of materiality and risk. The areas addressed by the audit included health professionals licensing, cash receipts, and information systems. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of the Unit's operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

Our audit did not include certain support services provided to the Unit by DHMH – Office of the Secretary. These support services (such as payroll, purchasing, maintenance of accounting records, and related fiscal functions) are included within the scope of our audit of DHMH's Office of the Secretary and Other Units.

The Unit'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 that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect the Unit's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to the Unit that did not warrant inclusion in this report.

DHMH's response, on behalf of the Unit, 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.

APPENDIX



STATE OF MARYLAND

DHMH

Maryland Department of Health and Mental Hygiene
201 W. Preston Street • Baltimore, Maryland 21201

Martin O'Malley, Governor – Anthony G. Brown, Lt. Governor – Joshua M. Sharfstein, M.D., Secretary

November 4, 2011

Mr. Bruce Myers, CPA
Legislative Auditor
Office of Legislative Audits
301 West Preston Street
Baltimore, MD 21201

Dear Mr. Myers:

Thank you for your letter regarding the draft audit report of the Department of Health and Mental Hygiene - Regulatory Services for the period beginning February 1, 2008 and ending August 2, 2010. Enclosed you will find the Department's response and plan of correction that addresses each audit recommendation.

I wanted to take this opportunity to address one finding of particular concern to me, and the steps taken in response. Finding 1, as to the Board of Nursing, addresses allegations from 2009 that an employee fraudulently sold and issued Certified Nursing Assistant certificates. This was discovered on May 6, 2009. Since that time, the Board of Nursing and the Department have taken a number of actions to protect the public and to assure that this should never recur. These responses, discussed in detail in the audit responses, include:

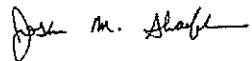
- Prompt referral of potential criminal activity to the Department's Office of the Inspector General and the Office of the Attorney General;
- Termination of the employee;
- Review by the Board of Nursing of all certificates which could be linked to the employee;
- Letters notifying 157 individuals that their certificates were null and void;
- Listing all such individuals on the Board's website;
- Notifying trade associations and other industry representatives who employ certified nursing assistants;
- Review of State employment records of all individuals issued null and void certificates and individualized written notification to any employer of such an individual; and
- Systems changes in the process of issuing certificates, so this should not recur.

In order to assure that the Board had done all that it could, on April 19, 2011 I asked the Department's Inspector General to conduct an independent follow up review. The Inspector General had conducted an investigation in 2009 and made a number of recommendations. In this follow up review, the Inspector General's Chief Compliance Officer confirmed that the Board has taken significant steps to prevent a reoccurrence of the alleged issuance of fraudulent certification.

With these concerns and with all others, I will continue to work with the appropriate Administrators, Executive Directors, and the Assistant Secretary to promptly address all 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 of my staff at 410-767-5862.

Sincerely,

A handwritten signature in black ink, appearing to read "Josh M. Sharfstein".

Joshua M. Sharfstein, M.D.
Secretary

Enclosure

cc: Patricia A. Noble, R.N., Executive Director, Maryland Board of Nursing, DHMH
C. Irving Pinder, Jr., Executive Director, Maryland Board of Physicians, DHMH
LaVerne G. Naesea, Executive Director, Maryland Board of Pharmacy, DHMH
Nancy Grimm, Director, Office of Health Care Quality, DHMH
Paula C. Hollinger, Associate Director, Health Workforce, DHMH
Thomas V. Russell, Inspector General, DHMH
Ellwood L. Hall, Jr., Assistant Inspector General, DHMH
Patrick Dooley, Chief of Staff, Office of the Secretary, DHMH

Findings and Recommendations

Finding 1

Certain boards had not established sufficient controls over the accounting for professional licenses and related collections.

Recommendation 1

We recommend that the applicable Boards

- a. establish procedures to ensure that an employee independent of the collections verifies that all amounts received are deposited and recorded in the State's accounting records (repeat);**
- b. verify that all licenses issued were paid for and were proper (repeat); and**
- c. periodically account for all licenses as being issued, voided and/or on-hand (repeat).**

Board of Pharmacy Response:

- a. This recommendation does not apply to the Board of Pharmacy.
- b. The Board concurs and has reinstated procedures for verifying that all licenses are paid for and are proper. The Board had followed a process to verify payment for all licenses issued, in response to a previous audit report. However, most of the involved tasks were to be performed by the Licensing Manager. The Licensing Unit Manager position had been vacant for a significant period of time before and during the audit period (recently filled March 2011). The below summarized procedures are now reinstituted:

To reconcile the licenses for any one month, the "Printed Licenses Report" is printed out the first of every month. This reports allows the Licensing Manager to verify: Control Number, Account Name (License type) ,Check Amount, Comments (usually Confirmation numbers issued for Online payment), Check Received Date, Name of applicant, Check or Credit Card Transaction Number, License Number, Date Printed, Verified By (Name of staff person who verified license). The Licensing Manager reviews the complete reports to ensure that no licenses were issued that did not have a related payment, signs and dates the report. She also reviews with staff why any applicant who paid within any 30 day period has not receive a license, as necessary.

- c. The Board concurs and updated its process for periodically accounting for all licenses as being issued, voided, and or on-hand following the exit conference with the auditors. The below procedures, in addition to those noted above in "b" should account for all licenses. These accounting tasks had not been performed previously or had been neglected as a consequence of the Licensing Unit Manager vacancy.

1. *Upon receipt of ordered licenses, the Executive Director stores them in a locked cabinet.*
2. *Sealed bulk licenses are subsequently provided to the Licensing Manager.*
3. *The receiving staff member must initial a log next to the date of receipt and the Executive Director's initials.*
4. *The receiving Unit Manager then distributes individual license types to various unit staff, who are required to initial a second log next to the date and initials of the person from whom they are received.*
5. *The Executive Director tracks the number of sealed packs of licenses held in the locked cabinet and the person who issues the licenses periodically checks to ensure that the licenses maintained in their locked cabinet are accounted for.*
6. *Upon ordering additional documents the Fiscal Officer ensures that the last Control number is consistent with the new set of control numbers ordered.*
7. *The Unit Supervisor (or Executive Director if a vacancy exists) must review the log book maintained in the Unit at least monthly in order to ensure an accurate count. Dates of the Supervisory review must be recorded on a third log.*
8. *To track this accounting for all pre-numbered licenses, a database will be developed no later than September 30, 2011, that accounts for all pre-numbered licenses, including: the control numbers issued for each category, the control numbers for those voided and each category, and the control numbers for those that have not been issued (as well as where they are located).*

MBON Response:

- a. The Board of Nursing concurs with this recommendation and has separated the different components among different staff so that there are checks and balances. Although all functions have been separated, there is the possibility that with an employee's prolonged absence, tasks could again overlap. Therefore, as a precaution the Board has initiated the personnel processes to secure additional positions.
- b. The MBON concurs with this recommendation. The Board now tracks the appropriate data to verify that monies are received to match each license/certificate number issued. The Office of Inspector General (OIG) has worked with the Board and the OIG agrees that the Board tracks necessary information, including license/certificate number, issue/renewal date, name, payment amount, payment date, and license type. The Board continues to work with the Inspector General to refine this tracking system. The OIG has sent your office the format used for reconciliation, and the OIG and the Board would like to review this format with your office to assure that it fully meets the concerns expressed in the audit.
- c. This does not apply to MBON.

Finding 2

The Office of Health Care Quality (OHCQ) had not conducted annual inspections of certain health care facilities as required.

Recommendation 2

We recommend that OHCQ complete inspections of the various health care facilities, as required by law (repeat).

OHCQ Response:

OHCQ concurs with the finding and recommendation.

OHCQ's capacity to complete inspections of the various health care facilities as required by law continues to be challenged by the ongoing surveyor shortage. According to OHCQ's FY 2010 Staffing Analysis, the surveyor deficit in the Assisted Living unit was seven positions; the deficit was 28 surveyor positions in the Developmental Disabilities (DD) unit. In operational terms, the deficit means that in order to complete the mandated surveys, OHCQ will need an additional 35 surveyors. The number of completed surveys is clearly influenced by the surveyor staffing deficit. It's important to point out that OHCQ the number of positions has been 194 to 183, and that the agency staffing deficit for all units is 92. These staff reductions, coupled with furloughs and administrative salary reduction days, and the lack of administrative support positions, affects the number of completed surveys.

In an effort to address the oversight concern, OHCQ implemented a number of initiatives aimed at better utilizing our limited resources; they include:

- DD unit began utilizing provider self-surveys to document mandated policy and procedure compliance and personnel training requirements, which resulted in an average savings of two days survey time per agency surveyed.
- DD unit allocated staff resources to develop a small division with the primary focus on children's issues, which includes initial and re-licensure surveys, complaint and incident investigations, and partnerships with other State and county agencies involved in supporting the needs of children. The creation of the children's unit should increase OHCQ's ability to complete mandatory annual visits to each of the 24 agencies. .
- DD unit recently began the practice of referring non-health and non-safety complaints to the four (4) DDA regional offices. Administrative investigations, rather than those performed on site, are conducted, when appropriate. Furthermore, the DD unit incorporates incident and complaint investigations into re-licensure visits whenever possible.

Finding 3

The Board of Nursing's contract with its licensing service vendor did not include provisions obligating the vendor to address certain significant information technology security and operational risks.

Recommendation 3

We recommend that the Board

- a. obtain assurances from the vendor that it has addressed critical data security and operational risks, including safeguards for sensitive data;**
- b. request that the vendor periodically provide sufficient evidence that controls pertaining to such risks are effective; and**
- c. include in future IT contracts, involving cloud computing services with significant risks, provisions that require the vendor to address critical security and operational risks and to periodically obtain an examination of its system controls (for example by requiring the vendor to periodically obtain a SOC 2, type 2 report).**

MBON Response:

The Board of Nursing concurs with this recommendation. Comments are below.

- a) In the yearly compliance audit performed by the contractor on April 11, 2011, for the MBON, the vendor was able to provide assurances that it had addressed the data security and operational risks to include safeguards for sensitive data by various system upgrades to the firewall, including spam detectors, intrusion agents and scripts.
- b) MBON concurs with this recommendation and has requested quarterly reports from the vendor providing risk management reports detailing the controls that have been put into place to ensure MBON sensitive data is protected during the short amount of time that it resides on their server. All transactions are collected daily and sent to MBON the following morning and do not reside on their servers once they are transmitted to MBON. The vendor also provides daily backups that are stored in a fire and water proof safe before being picked up and delivered to an off-site provider.
- c) The Board concurs with this recommendation and believes that we were compliant at time of signature. MBON will ensure that any further IT contracts involving Cloud Computing services with significant risk, will require the vendor to address critical security and operational risk and require a SOC2, type 2 report.

Finding 4

The Board of Nursing did not have a complete disaster recovery plan and controls over the licensing database were not sufficient.

Recommendation 4

We recommend that the Board

- a. develop a complete DRP that, at a minimum, addresses the basic elements needed for a comprehensive disaster recovery plan;**
- b. log all significant database security and audit events (repeat);**
- c. verify that database password and account controls are in compliance with the requirements of the DoIT *Information Security Policy*; and**
- d. ensure that the licensing database backups are stored at a secure off-site location.**

MBON Response:

The Board of Nursing is in agreement with this recommendation. Comments are below.

- a) The Board is currently working to acquire an independent company to assist with completion of our DRP and plan to have them participate in scheduling all testing. It is anticipated that this will be resolved by January 1, 2012.
- b. In response to a previous audit, the Board has enabled the necessary database security and audit events. It was through this second audit that the Board found out there was actually a second parameter that needed to be enabled. The Board believes this has been enabled.
- c. The Board is currently working with our database vendor to ensure that all database passwords and account controls are in compliance with DoIT Information Security Policy. We are also working with them to change any accounts that access between and among component subsystems in order to meet DoIT Information Security Policy. It is anticipated that this will be resolved by January 1, 2012.
- d. The Board is continuing to find off-site storage for our backups. We are hopeful that the company assisting in our DRP will help with this. It is anticipated that this will be resolved by January 1, 2012.

AUDIT TEAM

Peter J. Klemans, CPA
Audit Manager

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

W. Thomas Sides
Senior Auditor

A'knea K. Smith
Jennifer L. Thompson
Staff Auditors

Michael K. Bliss
Information Systems Senior Auditor