Audit Report

Baltimore City Community College

December 2014

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

Thomas J. Barnickel III, CPA
Legislative Auditor

December 9, 2014

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

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Baltimore City Community College (BCCC) for the period beginning November 17, 2010 and ending October 23, 2013. BCCC is an urban two-year institution that primarily offers associate of arts degrees and certificate programs in the business and health services fields, as well as general studies for the purpose of continuing education at a four-year institution.

Our audit disclosed that adequate security measures were not in place to protect BCCC's computer network and related administrative systems from security risks. For example, certain of BCCC's firewalls allowed numerous unnecessary connections to portions of its network, and account controls, password controls, and administrative access were not sufficient to properly protect its network. Sensitive personally identifiable information, such as student records, was also not encrypted within database tables.

Our audit also disclosed that BCCC did not comply with State procurement regulations when purchasing certain services. For example, during fiscal years 2012 and 2013, BCCC made repeated purchases for maintenance services from three vendors totaling $293,000 without obtaining competitive sealed bids. Additionally, BCCC did not comply with certain requirements of the Comptroller of Maryland's *Corporate Purchasing Card Program Policy and Procedures Manual*. Finally, our audit disclosed internal control weaknesses related to payroll.

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

BCCC'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 BCCC.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

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

Background Information

Agency Responsibilities

The Baltimore City Community College (BCCC) is an urban two-year institution and operates under the jurisdiction of BCCC's Board of Trustees. BCCC primarily offers associate of arts degrees and certificate programs in the business and health services fields, as well as general studies for students to continue their education at a four-year institution. BCCC has one main campus, five satellite locations, and more than 80 off-campus sites throughout Baltimore. BCCC's reported full-time equivalent enrollment for credit courses in the Fall 2013 semester totaled 1,588. According to the State's accounting records, BCCC's fiscal year 2013 revenues totaled approximately $81 million, which included a State General Fund appropriation of approximately $40 million.

Financial Statement Audits

BCCC engaged an independent accounting firm to perform audits of its financial statements for the fiscal years ended June 30, 2012 and 2013. In the related audit reports, the firm stated that BCCC's financial statements presented fairly, in all material respects, the financial position of BCCC and the changes in its financial position and cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Accreditation

On June 26, 2014, the Middle States Commission on Higher Education (MSCHE) warned BCCC that its accreditation may be in jeopardy because of insufficient evidence regarding compliance with its standards, including those related to resource allocation, integrity, and institutional effectiveness. BCCC is required to submit a report documenting its progress in meeting the standards by March 2015. Based on the results of this report and an on-site visit, MSCHE will make a determination, such as to reaffirm the accreditation or request BCCC to "show cause" for retaining its accreditation.

In our preceding audit report, we commented that MSCHE had placed BCCC on probation because of insufficient evidence that it complied with certain standards. Upon completion of a monitoring report and an MSCHE review, the probation was removed and its accreditation was reaffirmed in June 2012. During 2013 and 2014, BCCC performed a self-study which, in part, was used by MSCHE in evaluating BCCC's accreditation status.

Accreditation is critical to BCCC, because according to federal regulations, non-accredited colleges are not eligible for federal funding (such as Pell grants). In fiscal year 2013, BCCC received federally funded student financial aid totaling approximately $13 million.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the seven findings contained in our preceding audit report dated April 18, 2012. We determined that BCCC satisfactorily addressed six of these findings. The remaining finding is repeated in this report.

Findings and Recommendations

Information Systems Security and Control

Background

The Baltimore City Community College's (BCCC) Information Technology Services Division manages the development, maintenance, and support of BCCC's information technology infrastructure, including all related networking, telecommunications, and business information systems. The Division maintains an integrated administrative and academic computer network which includes separate email and file servers, Internet connectivity, and multiple firewalls. The Division also maintains critical enterprise applications supporting student, human resource, and financial information systems. Furthermore, the Division operates web-enabled applications used by students to make payments to BCCC and by faculty to record student grades.

Finding 1
BCCC's computer network was not properly secured.

Analysis

Proper security measures had not been established to protect BCCC's critical network devices and administrative systems from external and internal threats.

- Firewall rules on two firewalls allowed numerous unnecessary connections to portions of the BCCC network, thereby placing various network devices at risk. For example, third party vendors had unnecessary network level access to two internal critical devices. A similar condition was commented upon in our two preceding audit reports.

- The device used to collect and analyze firewall logs was not configured to receive any logs from a critical firewall. Accordingly, significant events affecting this firewall's operations were not subject to review for incident response purposes. In addition, BCCC did not review the logs for all of its other firewalls. Similar conditions were commented upon in our preceding audit report.

- The configurations for all four operational BCCC firewalls were not regularly backed up. We determined that as of May 7, 2014, firewall configurations had not been backed up for almost seven months. Since BCCC's network and necessary access to/from network devices are constantly changing, firewall configuration backups that are seven months old do not accurately reflect the current state of conditions.

The Department of Information Technology (DoIT) *Information Security Policy* requires that agency systems be configured to monitor and control communications at external boundaries and that comprehensive audit logs be maintained and regularly reviewed.

Recommendation 1
We recommend that BCCC

a. configure its firewalls to achieve a "least privilege" security strategy giving individuals and devices only those privileges needed to perform assigned tasks (repeat);
b. configure the device used to collect and retain firewall logs to receive and retain the logs from all BCCC operational firewalls and regularly review these logs, investigate unusual or suspicious items, and retain documentation of these reviews and investigations (repeat); and
c. generate a copy of the configuration file for each of its firewalls at least once every three months and whenever significant changes are made to a configuration, and store these backup copies at a secure offsite location.

Finding 2
Account and password controls and administrative access to the BCCC network, workstations, and servers were not adequate.

Analysis
Account and password controls and administrative access to the BCCC network, workstations, and servers were not adequate.

- Domain account and password settings were not sufficient to properly protect the BCCC network. For example, we noted 133 accounts with passwords set to never expire, 275 accounts that were unused for at least one year, and the minimum password length set to six characters.

- Account and password controls for the student and faculty web portals, which are used to post and view student grades, were not adequate. Specifically, password length, password complexity, and account lockout requirements were not in compliance with the requirements of the DoIT *Information Security Policy*.

- All eight workstations tested included a locally defined administrator group which included all BCCC domain users. As a result of this condition, all BCCC users logged into the domain, upon establishing a remote connection to these workstations, would have local administrative privileges and could improperly access and read and modify any files on these workstations.

- Seven accounts were improperly placed in domain groups which have powerful system capabilities and privileges. For example, four of these accounts were improperly placed in the domain administrator group. As a result of this condition, these accounts had excessive administrative control over domain resources and could access and make unauthorized modifications to critical data and objects without detection by management.

- Two accounts were improperly placed in the local administrator group on a critical application server. As a result of this condition, these accounts had full control over all data files and programs residing on this server.

The DoIT *Information Security Policy* requires that passwords have an eight-character minimum length, that they meet certain complexity requirements, and that they be changed at regular intervals. This *Policy* further requires that accounts be disabled or locked after 60 days of inactivity and that accounts be locked out after no more than four invalid attempts, while allowing a minimum of a ten (10) minute automatic reset of the account. Finally, this *Policy* requires that agencies establish an authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of "least possible privileges" and "need-to-know."

Recommendation 2
We recommend that BCCC

a. establish account and password settings in accordance with the aforementioned DoIT *Information Security Policy*;
b. restrict membership in domain groups with powerful capabilities and privileges to only those accounts requiring membership in these groups; and
c. limit membership in the local administrator group, on all of its workstations and servers, to only those accounts requiring such privileges.

Finding 3
Malware protection on workstations and servers needs improvement.

Analysis
Malware protection on workstations and servers needs improvement.

- All eight workstations tested were improperly configured with users having administrator rights. Administrator rights are the highest permission level that can be granted to users and it allows users to install software and change configuration settings. As a result, if these workstations were infected with

malware, the malware would run with administrator rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights. In addition, as a result of the administrator privileges assigned, these eight users had the ability to disable the malware protection software on their workstations.

- Workstations and servers tested had not been updated with the latest releases for software products that are known to have significant security-related vulnerabilities. Although the vendors for these software products frequently provide software patches to address these vulnerabilities, BCCC had not updated its workstations and servers for these patches. For example, our test of eight workstations for one of these software products disclosed that all eight workstations were running older versions of this software that had not been updated for periods ranging from 8 to 21 months.

- The malware protection software used to protect BCCC workstations was not properly configured to limit users' capabilities. Specifically, users of all eight workstations tested could disable malware protection software features that would render the software unable to protect against malware threats.

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 and protect against malicious code by implementing protections that, to the extent possible, include a capability for automatic updates.

Recommendation 3
We recommend that BCCC

a. ensure that administrator privileges on workstations are restricted to network administrators,
b. promptly install all critical security-related software updates, and
c. configure its malware protection software so that users cannot disable the settings which allow users to override and modify default security controls established by management.

Finding 4
BCCC stored sensitive personally identifiable information (PII) within database tables in clear text.

Analysis
BCCC stored sensitive PII within database tables in clear text. Specifically, we determined that BCCC stored PII, including full names, social security numbers,

and dates of birth in clear text in 58 database tables located in 5 databases. Furthermore, the sensitive PII fields (such as social security number) were not masked or truncated to prevent online application users from viewing complete information.

BCCC personnel identified approximately 312,000 unique student records, in one of the aforementioned 58 tables which contained the aforementioned PII, which were not encrypted. This sensitive PII, which is commonly sought by criminals for use in identity theft, should be protected by appropriate information system security controls. The DoIT *Information Security Policy* requires each agency to protect confidential data using encryption technologies and/or other substantial mitigating controls.

Recommendation 4
We recommend that BCCC

a. encrypt all database tables containing PII, and
b. mask or truncate social security numbers from online application users that do not need to see these full social security numbers.

Procurement

Finding 5
BCCC did not comply with State procurement regulations when purchasing certain maintenance and audit services.

Analysis
BCCC did not comply with State procurement regulations regarding the use of competitive procurements when purchasing certain maintenance and audit services. Consequently, there is no assurance that BCCC obtained these services at the lowest cost.

- Based on our review of corporate purchasing card and disbursement transactions, BCCC made repeated purchases from three vendors without a formal procurement process (such as competitive sealed bidding) and did not enter into contracts. Purchases from these three vendors during fiscal years 2012 and 2013 for maintenance services (such as electrical and air conditioning repairs) totaled $293,000. While BCCC was able to provide us with some bidding documentation for $61,000 of these purchases, no bidding documentation was available for the remaining purchases. State procurement regulations generally specify that contracts in excess of $25,000 shall be awarded by competitive sealed bidding, and that procurements exceeding $5,000 must also have written contracts.

- In April 2013, BCCC contracted with an audit services firm on an emergency basis and entered into two contracts with this firm, totaling $68,100, for the period from April 2013 to October 2013, but did not comply with the applicable State emergency procurement regulations. Specifically, one of the two contract awards was not submitted to the Board of Public Works (BPW) for approval nor was the notice of the award for either contract published in *eMaryland Marketplace* as required. In addition, BCCC did not have an executed copy of either contract on hand. Finally, procurement regulations require that competitive bids be obtained for emergency procurements to the extent possible and practical; however, there was a lack of documentation to substantiate that BCCC sufficiently justified why it was unable to solicit bids from other firms. We were advised by BCCC that this firm was selected based upon a recommendation from one BCCC employee who had prior knowledge of this firm. In our opinion, BCCC should have considered obtaining other competitive bids from the 19 available audit firms under the Statewide audit services master contract.

Recommendation 5
We recommend that BCCC

a. comply with State procurement regulations by using a formal written procurement process for purchases that are reasonably expected to exceed $25,000 and ensuring that procurements exceeding $5,000 have written contracts;
b. comply with State procurement regulations for emergency purchases by soliciting competitive bids when possible and practical, publishing the notice of awards in *eMaryland Marketplace*, and submitting contract awards to the BPW for approval; and
c. ensure that formal written contracts are executed with vendors.

Payroll

Finding 6
BCCC did not ensure the propriety of payments made to full-time instructors for teaching courses beyond their required course loads.

Analysis
BCCC did not ensure that only proper payments were made to full-time instructors for courses taught beyond their required course loads. Instructors were paid based on payroll authorization forms provided to the payroll department by the respective BCCC education department. According to BCCC's policy, prior to submitting each payroll authorization form, the applicable education department, such as the School of Allied Health and Nursing was required to

document that the course exceeded the instructor's required workload (typically 15 credit hours) by completing a Teaching Assignment Unit (TAU) form. However, our test of payments to instructors for these additional courses disclosed that such documentation was not always on file.

We tested 10 full-time instructors who were paid approximately $95,000 in fiscal years 2012 and 2013 for teaching courses beyond their required course loads. For 3 instructors, who were paid approximately $28,000, approved TAU forms were not on file. We were advised by BCCC that there was evidence that the courses were taught by two of the instructors; however, for one of the instructors who received payments totaling $4,400, BCCC could not provide evidence (such as, class attendance or posting of grades) that the instructor taught the courses. During the period from November 2010 through October 2013, BCCC paid $2.1 million to 101 instructors for teaching beyond their required course load.

Recommendation 6
We recommend that BCCC

a. ensure that payments to instructors for courses taught beyond their required course loads are properly supported, and

b. review the aforementioned payments and take appropriate action (such as recovering improper payments).

Corporate Purchasing Cards

Finding 7
BCCC did not comply with certain corporate purchasing card requirements.

Analysis
BCCC did not comply with certain requirements of the Comptroller of Maryland's *Corporate Purchasing Card Program Policy and Procedures Manual*. According to the credit card processor's records, as of January 2014, BCCC had issued 61 corporate purchasing cards to employees, and the related expenditures totaled approximately $1.8 million during fiscal year 2013.

- Card charges for payments made to a vendor that was an online payment service were not always supported. Our test of 15 payments to this vendor totaling $19,700 disclosed that 5 payments totaling $7,900 were not properly supported. Although BCCC had receipt documentation for these payments (such as, a payment confirmation), the documentation did not provide details describing the goods and services provided. As a result, we were unable to determine the propriety of these payments. The *Manual* requires itemized

support (such as, a detailed invoice) for all purchases. BCCC made payments to this vendor totaling $145,000 from November 2010 through October 2013.

- Cards were not always promptly cancelled upon employee terminations. Our test of 12 cardholders who separated from BCCC employment during the period from December 2011 through August 2013 disclosed that 7 accounts remained active for periods between 26 and 113 days beyond their separation dates. We noted no charges were incurred on these accounts after the employees' departures. The *Manual* requires that accounts of terminated employees be closed upon their termination of employment.

Recommendation 7

We recommend that BCCC ensure that

a. proper documentation (such as itemized vendor invoices) is obtained from the aforementioned vendor to support payments, and

b. cards assigned to individuals no longer employed by BCCC are promptly cancelled.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Baltimore City Community College (BCCC) for the period beginning November 17, 2010 and ending October 23, 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 BCCC'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 purchases and disbursements, student accounts receivable, financial aid, cash receipts, payroll, and information technology systems. 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 BCCC'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 BCCC's financial system for the purpose of testing certain areas, such as student accounts receivable. 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 did not include an evaluation of internal controls for federal financial assistance programs and an assessment of BCCC'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 BCCC.

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

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

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

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect BCCC'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 BCCC that did not warrant inclusion in this report.

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

APPENDIX

BALTIMORE CITY COMMUNITY COLLEGE

OFFICE OF THE PRESIDENT

2901 Liberty Heights Ave.
Baltimore, Maryland 21215-7893

410-462-8300
www.bccc.edu

Gordon F. May, PhD
President

November 24, 2014

Mr. Thomas J. Barnickel, III, CPA
Legislative Auditor
Department of Legislative Services
Office of the Legislative Audits
301 West Preston Street, Room 1202
Baltimore, MD 21201

Dear Mr. Barnickel:

Enclosed, please find the Baltimore City Community College response to the draft audit report for the period beginning November 17, 2010 and ending October 23, 2013.

As requested, I have sent the electronic version of the response by email to response@ola.state.md.us and a paper copy to the aforementioned address.

On behalf of Baltimore City Community College, I thank you for the comprehensive review of the Colleges financial transactions, internal controls, and evaluation of our compliance with applicable State of Maryland laws. Please do not hesitate in contacting me at 410.462.8054 or by email at gfmay@bccc.edu if additional information is needed.

Sincerely,

Gordon F. May, PhD
President and CEO

c: Dr. Mary Elizabeth Owens Southall, BCCC Board of Trustees, Chair
Ms. Lyllis Green, BCCC Chief Internal Auditor
Mr. Anwer Hasan, Chair, MHEC
Ms. Catherine Schultz, Acting Secretary, MHEC

Information Systems Security and Control

Finding 1
BCCC's computer network was not properly secured.

Recommendation 1
We recommend that BCCC

a. configure its firewalls to achieve a "least privilege" security strategy giving individuals and devices only those privileges needed to perform assigned tasks (repeat);

b. configure the device used to collect and retain firewall logs to receive and retain the logs from all BCCC operational firewalls and regularly review these logs, investigate unusual or suspicious items, and retain documentation of these reviews and investigations (repeat); and

c. generate a copy of the configuration file for each of its firewalls at least once every three months and whenever significant changes are made to a configuration, and store these backup copies at a secure offsite location.

College Response: We concur. BCCC procured a firewall Event Management and Storage appliance in 2011. However, due to staffing issues, BCCC had experienced some challenges in Firewall management and consistent log review.

a) Comprehensive assessment of BCCC's network and security risks has begun with direct additional support from Maryland DoIT. This review is being staged over a three month, period, firewalls were/are upgraded and reconfigured to implement a "least privilege" security strategy and removing all rules which allow unnecessary connections to any part of BCCC's network. Meanwhile, all outdated rules and unnecessary access for third party vendors were immediately removed.

b) Log Storage – the device used to collect and analyze firewall logs has been upgraded and reconfigured to support the storage of all Firewall logs including the cited critical firewall. The Event reporting device has also been reconfigured to send immediate email alerts on critical network security events and produce daily log reports for review by the Firewall Administrators.

c) Configuration files for each firewall device was generated and sent to an offsite location in July 2014 and also in October 2014. BCCC now has a procedure in place to send a copy of the configuration files to an offsite location at least once every three months or whenever there is a major change to the network, depending on which occurs first.

Finding 2
Account and password controls and administrative access to the BCCC network, workstations, and servers were not adequate.

Recommendation 2
We recommend that BCCC

a. establish account and password settings in accordance with the aforementioned DoIT *Information Security Policy*;
b. restrict membership in domain groups with powerful capabilities and privileges to only those accounts requiring membership in these groups; and
c. limit membership in the local administrator group, on all of its workstations and servers, to only those accounts requiring such privileges.

College Response: We concur.

a) The College changed the group policies to match the current standards for password requirements in accordance with DoIT Information Security Policy. On 8/7/2014, the "Password Never Expires" option was removed from all domain user objects. On 8/15/2014, BCCC disabled all accounts that were inactive for greater than 60 days. An account review is now in place to disable expired/inactive accounts on a quarterly basis. The account and password controls for the credit faculty portal are in compliance with the requirements of the DoIT Information Security Policy. The faculty portal uses LDAP authentication and password controls. The non-credit faculty portal will transition to LDAP authentication in January 2015.

b) Domain group accounts with administrative level privileges are reviewed through a review and restriction policy of the groups on a monthly basis. The improper domain groups and Admin accounts were removed from access. Specific ITS personnel have been assigned the recurring task to ensure timely delivery and security assessments.
This is performed by manually verifying the group membership contains only authorized user objects.

c) IT Services removed all non-essential accounts from Local Administrator privileges on endpoints with the exception of specific ITS administrative personnel and critical application-related concerns tied to college productivity. This was accomplished through distributed group policies and by cleaning up the initial imaging and deployment process through defining tighter restrictions on local account policies.

Finding 3
Malware protection on workstations and servers needs improvement.

Recommendation 3
We recommend that BCCC

a. ensure that administrator privileges on workstations are restricted to network administrators,
b. promptly install all critical security-related software updates, and
c. configure its malware protection software so that users cannot disable the settings which allow users to override and modify default security controls established by management.

College Response: We concur.

a) BCCC removed employees from the Local Administrator privileges on Operating System images and endpoints with the exception of specific IT Services **administrators** and related functions.

b) To address common software vulnerabilities, ITS purchased an administrative tool and implemented it on August 5th, 2014. This administrative tool is utilized to install the latest versions of application products on endpoint workstations/systems. Critical updates are applied globally on a weekly basis after passing daily testing and approval on select endpoints that mimic the overall environment.

c) Policies were changed to prevent the disabling of active protection on the endpoint clients. Domain Admins currently retain the privilege to disable the endpoint client for troubleshooting purposes. In addition, a new anti-virus/malware prevention product has been purchased for enterprise endpoints providing greater security and access controls.

Finding 4
BCCC stored sensitive personally identifiable information (PII) within database tables in clear text.

Recommendation 4
We recommend that BCCC

a. encrypt all database tables containing PII, and
b. mask or truncate social security numbers from online application users that do not need to see these full social security numbers.

College Response: We concur.
The security vulnerabilities that were noted in the database tables will be mitigated as soon as possible. In an effort to mitigate the identified vulnerabilities, BCCC has received approval to pull ahead on a short-term solution of implementing an identity management system to resolve current known security vulnerabilities and the long-term solution of implementing a new ERP system that meets all required security standards. However, in the interim, the following precautions are in place to safeguard tables containing PII:

a) Our database tables have a 'privileged mode' file security level; they can **only** be opened with programs using the system's proprietary interface and intrinsic functions. These programs are restricted to authorized staff only.

b) Only authorized FT staff that have a direct business need can see the student information via online applications. An institutionalized annual process is performed across the entire college to review and update (review of user account logon audit/validation process) the online applications and who has access to the sensitive student related screens. The Records and Registration group also performs internal monthly reviews of who has access to these online screens.

The college is in the process of procuring a modern ERP system with assistance from DoIT/Procurement. The new modern ERP system will inherently support encryption and be able to mask all personally identifiable information (PII) by using a system generated Student ID as the primary key. Completion of a project to review and mask printed reports was completed in mid-2012 to only show partial social security numbers.

A security matrix (industry best practice) will be developed that will stipulate who has access by functional role and which screens those functional roles have access to, as soon as the new ERP system is selected and implemented.

Procurement

Finding 5
BCCC did not comply with State procurement regulations when purchasing certain maintenance and audit services.

Recommendation 5
We recommend that BCCC

a. comply with State procurement regulations by using a formal written procurement process for purchases that are reasonably expected to exceed $25,000 and ensuring that procurements exceeding $5,000 have written contracts;

b. comply with State procurement regulations for emergency purchases by soliciting competitive bids when possible and practical, publishing the notice of awards in *eMaryland Marketplace*, and submitting contract awards to the BPW for approval; and

c. ensure that formal written contracts are executed with vendors.

College Response: We concur.
The College's current processes coupled with recent personnel changes will ensure future compliance.

Payroll

Finding 6
BCCC did not ensure the propriety of payments made to full-time instructors for teaching courses beyond their required course loads.

Recommendation 6
We recommend that BCCC

a. ensure that payments to instructors for courses taught beyond their required course loads are properly supported, and
b. review the aforementioned payments and take appropriate action (such as recovering improper payments).

College Response: We concur.
BCCC has re-evaluated the TAU process and enhanced its internal procedures. All payments for overloads will be properly supported. The aforementioned payments noted in the finding have been researched. Only one instructor was found to have been paid for courses not taught. The instructor was invoiced for these payments on 10/17/14.

Corporate Purchasing Cards

Finding 7
BCCC did not comply with certain corporate purchasing card requirements.

Recommendation 7
We recommend that BCCC ensure that

a. **proper documentation (such as itemized vendor invoices) is obtained from the aforementioned vendor to support payments, and**
b. **cards assigned to individuals no longer employed by BCCC are promptly cancelled.**

College Response: We concur.
The administration of the CPC card program was transferred to another individual who resides in the General Accounting department as of April 2014. This individual has implemented a re-training program to all cardholders to ensure that all online payment services transactions are properly documented. In addition, all cards assigned to individuals no longer employed by BCCC are promptly "cut up" and accounts officially closed by the CPC administrator upon notification of separation of employment from the HR department.

AUDIT TEAM

Joshua S. Adler, CPA, CFE
Audit Manager

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

Menachem Katz, CPA
Senior Auditor

Christopher D. Jackson
Edwin L. Paul, CPA, CISA
Information Systems Senior Auditors

Lisa M. DeCarlo
Jessica A. Foux
Ryan A. Myles
Staff Auditors

Matthew D. Walbert
Information Systems Staff Auditor