Audit Report

# University System of Maryland
# Bowie State University

May 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

May 5, 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 audited the University System of Maryland (USM) – Bowie State University (BSU) for the period beginning April 16, 2010 and ending June 30, 2013. BSU is a regional university offering a broad range of undergraduate and selected professionally oriented graduate programs.

Our audit disclosed that adequate security measures and monitoring procedures were not in place to protect BSU's computer network and related administrative systems from security risks. For example, certain of BSU's firewalls allowed numerous unnecessary connections to portions of its network and adequate backup procedures were not in place.

Our audit also disclosed that controls had not been established over BSU's High Ability Merit Scholarships. For example, there was no formal policy defining the eligibility criteria for these scholarships and award decisions were made by one individual. According to BSU records, these scholarships totaled approximately $488,000 during the 2012-2013 academic year.

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

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

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

# Table of Contents



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

# Background Information

## Agency Responsibilities

Bowie State University (BSU) is a comprehensive public institution of the University System of Maryland and operates under the jurisdiction of the System's Board of Regents. BSU is a regional university that provides a broad range of undergraduate and selected professionally oriented graduate programs, including doctoral level programs in educational leadership and computer science. BSU's undergraduate and graduate student enrollment during fiscal year 2013 totaled 4,308 full time equivalent students.

BSU's budget is funded by unrestricted revenues, such as tuition and fees and a State general fund appropriation, and restricted revenues, such as federal grants and contracts. According to the State's accounting records, BSU's revenues for fiscal year 2013 totaled approximately $102.4 million, including a State general fund appropriation of approximately $33.2 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 February 15, 2011. We determined that BSU satisfactorily addressed four of the findings. The remaining three findings are repeated in this report as two findings.

# Findings and Recommendations

## Information Systems Security and Control

### Background

Bowie State University's (BSU) Division of Information Technology provides information technology support to BSU through the operation and maintenance of campus-wide applications, such as the student administration and human resources systems and the financial system. BSU also operates an integrated administrative and academic computer network, which provides connections to multiple servers used for administrative and academic purposes. The network also includes separate email and file servers, intrusion detection systems, and firewalls. BSU also connects to the Maryland Research and Education Network to send and receive data to and from other University System of Maryland (USM) institutions and for Internet connectivity. BSU's network is also accessible to students from dormitories and computer labs.

**Finding 1**
**BSU's computer network was not properly secured or monitored.**

### Analysis

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

- Firewall rules allowed numerous unnecessary connections to portions of BSU's network, placing various network devices at risk. For example, we noted firewall rules that allowed the entire Internet unnecessary access to a number of critical network devices including critical storage devices and servers. Similar conditions have been commented upon in our three preceding audit reports.

- Key administrative systems were not properly protected from untrusted portions of the BSU network. Specifically, several computer labs located throughout BSU had unnecessary network-level access, overall protocols and ports, to critical campus administrative resources. Furthermore, traffic flowing from these computer labs to critical administrative network segments was not subject to intrusion detection prevention system coverage. Similar conditions were commented upon in our preceding audit report.

- Several critical non-public servers were improperly placed in a network segment that contained publicly accessible servers. This unnecessarily

exposed the non-public servers to security risks from the publicly accessible servers. Similar conditions have been commented upon in our three preceding audit reports.

- Monitoring of security events for critical firewalls and core routers needs improvement. We noted that logs for the critical firewalls and core routers were only reviewed on an as-needed basis, for troubleshooting purposes, and that these reviews were not documented. Similar conditions have been commented upon in our two preceding audit reports.

*USM Guidelines in Response to the State IT Security Policy*, require that firewalls should be configured to block all services not required, disable unused ports and hide and prevent direct accessing of trusted network addresses from untrusted networks. These *Guidelines* also require that entities maintain comprehensive audit trails and implement regular, documented review procedures.

**Recommendation 1**
**We recommend that BSU**

**a. configure its firewalls to adequately secure its network (repeat);**
**b. properly restrict access to key administrative systems from untrusted portions of the BSU network and ensure all traffic to the systems is subject to intrusion detection prevention system coverage (repeat);**
**c. segregate publicly accessible servers from non-public servers (repeat); and**
**d. regularly review security events for these critical devices, document the reviews of these events, and retain documentation for future reference (repeat).**

**Finding 2**
**BSU's intrusion detection prevention systems were not properly protecting the network.**

**Analysis**
BSU's intrusion detection prevention systems (IDPS) were not properly protecting the network.

- BSU did not use host-based intrusion protection systems (HIPS) on critical web servers that processed encrypted traffic. The absence of HIPS coverage for such traffic created network security risk in that BSU's network-based IDPS cannot read encrypted traffic flowing into its network whereas a HIPS

could read and analyze such traffic and protect critical web servers from any malicious traffic.

- The network-based IDPS were configured to operate as intrusion detection systems (IDS) rather than as intrusion prevention systems (IPS). As a result, all questionable network traffic identified by these systems was logged for subsequent review rather than immediately being blocked. Furthermore, logs of this questionable traffic were only reviewed on an as-needed basis, for troubleshooting purposes, and there was no documentation substantiating these reviews. Accordingly, potentially malicious traffic identified by the IDPS would reach intended network destinations without such activity being blocked or detected on a timely basis, due to the IDPS' configuration as an IDS.

Complete IDPS coverage includes use of properly configured network-based IDPS that is supplemented, where necessary, with HIPS to aid significantly in the detection/prevention of and response to potential network security breaches and attacks. Furthermore, without proper monitoring, critical network security breaches may occur that could otherwise possibly be detected and prevented.

**Recommendation 2**
**We recommend that BSU**

**a. perform a documented review and assessment of its network security risks, identify how HIPS coverage should be best applied to its network, and implement the coverage as appropriate, and**
**b. implement a network-based IDPS that is configured as an IPS which blocks all identified malicious traffic.**

**Finding 3**
**Malware protection on BSU workstations and servers needs improvement.**

**Analysis**
Malware protection on BSU workstations and servers needs improvement.

- Antivirus/antimalware software was not installed on BSU servers and workstations that used certain operating systems. We were advised by BSU network personnel that, although computers using such operating systems were in use on the network, a definitive count of the number of such computers was not available. According to BSU's records, there were at least 18 servers that were using these unprotected operating systems, but the number of workstations using such systems was not known. Without any

antivirus/antimalware software, these computers were highly susceptible to viruses and malware.

- Certain workstations were 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. Our testing of 10 workstations disclosed that 3 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 user accounts operated with only user rights.

- Workstations 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, BSU had not updated its workstations for these patches. For example, eight workstations tested for one of these software products noted that all of these workstations were running older versions of this software.

The *USM Guidelines in Response to the State IT Security Policy* state that standard virus protection programs must be installed, updated, and maintained on all microcomputers, LAN servers, and mail servers.

**Recommendation 3**
**We recommend that BSU ensure that**

**a. antivirus/antimalware software is installed on all computers,**
**b. administrative rights on workstations are restricted to only personnel that require such rights for their job duties, and**
**c. all workstations are kept up-to-date for all critical security-related updates to potentially vulnerable installed software.**

**Finding 4**
**Access and monitoring controls over critical databases and applications were not sufficient to protect critical data.**

**Analysis**
Access and monitoring controls over critical databases and applications were not sufficient to protect critical data.

- One hundred forty accounts (assigned to 131 users) were assigned unnecessary access to an application maintenance tool that could be used to modify the financial system's database security and access settings and to make unauthorized changes to the information in the related database. In addition, 8 accounts (assigned to 2 users) had unnecessary modification access to the financial system's application user profiles, roles, and permissions lists. Accordingly, unauthorized and inappropriate changes could be made to these user profiles, roles, and permissions lists which could be used to modify production data.

- Security report reviews of the human resources and student information systems' application and related database were performed by the individual responsible for making modifications to application security settings and the database. Furthermore, these reviews were not documented. Finally, the reports of additions and changes to the aforementioned application's security settings did not include all modifications to these security settings.

Best practice guidelines from the State of Maryland Department of Information Technology (DoIT) *Information Security Policy* recommend that access to information be strictly controlled, audited, and that it supports the concepts of "least possible privileges" and "need-to-know." Furthermore, the USM IT Security Council *Guide for Security Event Logging* requires each institution to maintain appropriate audit trails of events and actions related to critical applications and data, as required by State and federal laws/regulations. Further, these significant actions and events must be reviewed and documented.

**Recommendation 4**
**We recommend that BSU**

**a. limit access to the application maintenance tool to only those users requiring such access;**
**b. limit modification access to the financial system's application user profiles, roles and permission lists to only users requiring such access;**
**c. perform independent reviews of security reports for the human resources and student information systems' application and related database, document these reviews and retain the documentation for future reference; and**
**d. amend the reports of additions and changes to the human resources and student information systems' application security settings to include all changes to these security settings.**

**Finding 5**
**Backup procedures for critical servers and network devices were inadequate and a complete and comprehensive disaster recovery plan did not exist.**

**Analysis**
Backup procedures for critical servers and network devices were inadequate and a complete and comprehensive disaster recovery plan did not exist.

- Our test of 10 servers disclosed that 9 of these servers were not backed up during our one-month test period. In addition, for server backups that were performed, these backups were not taken offsite for 7 of the 8 months tested.

- Backup configuration files for numerous critical network devices, including firewalls and routers were not taken offsite but were stored in the same room as the aforementioned devices. Consequently, if a disaster occurred at that location that resulted in the destruction of both the original configurations and the related backup copies, computer operations could be disrupted for a prolonged period. A similar condition has been commented upon in our three preceding audit reports.

- BSU did not have a complete information technology disaster recovery plan (DRP) for recovering from disaster scenarios (such as, a fire). For example, the DRP did not adequately address alternate site processing arrangements and prioritization of systems for recovery. In addition, the plan had not been properly tested as restoration of critical files and programs from backup copies had not been performed. Finally, the DRP was a draft document that had not been finalized, reviewed, and approved by BSU management. 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. A similar condition has been commented upon in our three preceding audit reports.

According to the *USM Guidelines in Response to the State IT Security Policy,* backup media should be stored off-site in a secure, environmentally controlled location.

**Recommendation 5**
**We recommend that BSU**
**a. backup all critical servers on a frequent basis (daily or weekly);**
**b. store backups of critical servers and network devices configurations at an off-site, secure, environmentally controlled location (repeat); and**

**c. develop and finalize a DRP that, at a minimum, addresses the basic elements (including plan testing) needed for a comprehensive DRP (repeat).**

## Student Financial Aid

**Finding 6**
**High Ability Merit Scholarships were awarded without independent review and approval and without established eligibility criteria.**

**Analysis**
Controls had not been established over BSU's High Ability Merit Scholarships. Specifically, there were no formal guidelines defining the eligibility criteria for these scholarships. In addition, documentation supporting how the awards were determined was not maintained, and the awards were not subject to independent supervisory review and approval. We were advised by BSU management that these scholarships had been in existence for more than 15 years and were awarded to students based solely on the judgment of one management employee until the employee's retirement in July 2012. We were further advised that these scholarships were not advertised and that the students needed to contact the management employee directly to request an award. According to BSU records, during the 2012-2013 academic year (the last year that the aforementioned employee made these scholarship awards), approximately $488,000 in High Ability Merit Scholarships were awarded to approximately 175 students.

BSU awarded the High Ability Merit Scholarship without the BSU President having approved guidelines for their award or notification to USM as required. According to USM's policy, each institution is required to develop policy guidelines for the award of institutional financial aid to students. These guidelines are required to be approved by the University President and submitted to the USM Chancellor. Subsequent to our inquiries, BSU developed guidelines for this scholarship to begin with the 2013-2014 academic year. However, as of October 28, 2013, these guidelines had not been approved by the BSU President or submitted to the USM Chancellor.

**Recommendation 6**

**We recommend that BSU**

**a. ensure that the guidelines are approved by BSU's President and submitted to the USM Chancellor, as required; and**

**b. ensure that the High Ability Merit Scholarship awards are made in compliance with the established policy guidelines, are adequately supported, and are subject to independent supervisory review and approval.**

# Audit Scope, Objectives, and Methodology

We have audited the University System of Maryland (USM) – Bowie State University (BSU) for the period beginning April 16, 2010 and ending June 30, 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 BSU'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 contained in our preceding audit report.

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 purchases and disbursements, student accounts receivable, financial aid, cash receipts, payroll, and information technology systems.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of BSU'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 BSU's financial system for the purpose of testing 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 certain support services (such as bond financing) provided to BSU by the USM Office. These support services are included within the scope of our audits of the USM Office. In addition, our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of BSU'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 the components of USM.

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

The response to our findings and recommendations from the USM Office, on behalf of BSU, 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 the USM Office regarding the results of our review of its response.

# APPENDIX

OFFICE OF THE CHANCELLOR

April 28, 2014

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

Re: University System of Maryland –
Bowie State University
Period of Audit: April 16, 2010 through
June 30, 2013

Dear Mr. Barnickel:

I have enclosed the University System of Maryland's responses to your draft report covering the examination of the accounts and records of Bowie State University. Our comments refer to the individual items in the report.

Sincerely yours,

William E. Kirwan
Chancellor

Enclosures

cc:

Dr. Mickey Burnim, BSU
Mr. Karl Brockenbrough, VP for Administration and Finance, BSU
Mr. James L. Shea, Chair, Board of Regents
Mr. Anwer Hasan, Chairman, MHEC
Ms. Catherine Shultz, Acting Secretary of Higher Education, MHEC
Mr. Robert Page, Associate Vice Chancellor for Finance, USM Office
Mr. David Mosca, Director of Internal Audit, USM Office

1807 **University of Maryland, Baltimore**

1856 **University of Maryland, College Park**

1865 **Bowie State University**

1866 **Towson University**

1886 **University of Maryland Eastern Shore**

1898 **Frostburg State University**

1900 **Coppin State University**

1925 **Salisbury University**

1925 **University of Baltimore**

1925 **University of Maryland Center for Environmental Science**

1947 **University of Maryland University College**

1966 **University of Maryland, Baltimore County**

3300 Metzerott Road | Adelphi, MD 20783 | TEL: 301-445-1901 | FAX: 301-445-1931 | www.usmd.edu

# RESPONSE TO LEGISLATIVE AUDIT REPORT
# UNIVERSITY SYSTEM OF MARYLAND
# BOWIE STATE UNIVERSITY
# APRIL 16, 2010 TO JUNE 30, 2013

## Information Systems Security and Control

**Finding 1**
**BSU's computer network was not properly secured or monitored.**

**Recommendation 1**
**We recommend that BSU**

**a. configure its firewalls to adequately secure its network (repeat);**
**b. properly restrict access to key administrative systems from untrusted portions of the BSU network and ensure all traffic to the systems is subject to intrusion detection prevention system coverage (repeat);**
**c. segregate publicly accessible servers from non-public servers (repeat); and**
**d. regularly review security events for these critical devices, document the reviews of these events, and retain documentation for future reference (repeat).**

**University response**
BSU agrees with the recommendations.

a. BSU has installed updated firewall equipment. Initial configuration of the firewall was completed during April 2014. The firewall rule sets are now being tested and fine-tuned.

b. BSU is working to restrict access. The majority of the untrusted portion of the network has been segregated from key administrative systems. We are working to ensure all traffic from untrusted to trusted segments is covered by the intrusion detection prevention system.

c. BSU will continue to segregate publicly accessible servers from non-public servers with the new server architecture implementation.

d. BSU will begin regular reviews of security events for critical devices, will document the review of these events, and will retain the documentation for further reference.

# RESPONSE TO LEGISLATIVE AUDIT REPORT
# UNIVERSITY SYSTEM OF MARYLAND
# BOWIE STATE UNIVERSITY
# APRIL 16, 2010 TO JUNE 30, 2013

**Finding 2**
**BSU's intrusion detection prevention systems were not properly protecting the network.**

**Recommendation 2**
**We recommend that BSU**

**a. perform a documented review and assessment of its network security risks, identify how HIPS coverage should be best applied to its network, and implement the coverage as appropriate, and**
**b. implement a network-based IDPS that is configured as an IPS which blocks all identified malicious traffic.**

**University response**
BSU agrees with the recommendations.

a. The University purchased a HIPS application for servers based on an initial network assessment. The HIPS application will be applied and implemented to best protect the network.

b. The University purchased a new IPS device to provide additional coverage to block all identified malicious traffic and has implemented the recommendations for IDPS coverage for portions of BSU network which were deemed critical by DIT. BSU will complete the implementation of the network-based IDPS, configured as an IPS to block malicious traffic.

**Finding 3**
**Malware protection on BSU workstations and servers need improvement.**

**Recommendation 3**
**We recommend that BSU ensure that**

**a. antivirus/antimalware software is installed on all computers,**
**b. administrative rights on workstations are restricted to only personnel that require such rights for their job duties, and**
**c. all workstations are kept up-to-date for all critical security-related updates to potentially vulnerable installed software.**

# RESPONSE TO LEGISLATIVE AUDIT REPORT
# UNIVERSITY SYSTEM OF MARYLAND
# BOWIE STATE UNIVERSITY
# APRIL 16, 2010 TO JUNE 30, 2013

**University response**
BSU agrees with the recommendations.

a. We will ensure that antivirus/anti-malware software is installed on all machines not previously covered.

b. BSU is working to implement a process to assist personnel requiring additional workstation rights without implementing administrative rights. We are also developing specific policies to ensure that administrative rights on BSU owned workstations is restricted to personnel that require such rights to perform job duties.

c. The University has developed and implemented procedures to ensure security related updates are kept current for all BSU owned workstations to protect against potentially vulnerable installed software.

**Finding 4**
**Access and monitoring controls over critical databases and applications were not sufficient to protect critical data.**

**Recommendation 4**
**We recommend that BSU**
**a. limit access to the application maintenance tool to only those users requiring such access;**
**b. limit modification access to the financial system's application user profiles, roles and permission lists to only users requiring such access;**
**c. perform independent reviews of security reports for the human resources and student information systems' application and related database, document these reviews and retain the documentation for future reference; and**
**d. amend the reports of additions and changes to the human resources and student information systems' application security settings to include all changes to these security settings.**

**University response**
BSU agrees with the recommendations.

a. In June 2013 we restricted access that was inadvertently set during the financial system's application upgrade/conversion phase.

b. BSU has limited the modification access to application user profiles, roles, and permission lists to users requiring such access.

c. BSU will perform independent review of security reports for the BSU human resources and student information systems' application and related databases. The reviews will be documented and retained for future reference.

d. BSU will amend the reports to reflect all additions and changes to the human resources and student information systems' application security settings, including changes to the security settings.

**Finding 5**
**Backup procedures for critical servers and network devices were inadequate and a complete and comprehensive disaster recovery plan did not exist.**

**Recommendation 5**
**We recommend that BSU**

**a. backup all critical servers on a frequent basis (daily or weekly);**
**b. store backups of critical servers and network devices configurations at an off-site, secure, environmentally controlled location (repeat); and**
**c. develop and finalize a DRP that, at a minimum, addresses the basic elements (including plan testing) needed for a comprehensive DRP (repeat).**

**University response**
BSU agrees with the recommendations.

a. As of July 2013, we have completed implementation of an updated backup structure for all critical servers on a daily basis.

b. As of February 2014 we are storing backups of critical servers and network device configurations at an off-site, secure, and environmentally controlled property.

c. BSU has received funding and has started work to facilitate and finalize a DRP that addresses the basic elements (including plan testing) needed for a comprehensive DRP.

**Finding 6**
**High Ability Merit Scholarships were awarded without dependent review and approval and without established eligibility criteria.**

**Recommendation 6**
**We recommend that BSU**

**a. ensure that the guidelines are approved by BSU's President and submitted to the USM Chancellor, as required; and**

**b. ensure that the High Ability Merit Scholarship awards are made in compliance with the established policy guidelines, are adequately supported, and are subject to independent supervisory review and approval.**

**University response**

BSU agrees with the recommendations.

a. Effective October 2013 the University has revised its procedures for awarding High Ability Merit Scholarships. A draft policy outlining the process will be reviewed by the University's shared governance groups, approved by the President and submitted to the USM Chancellor for approval.

b. In the 2013-2014 academic year the University recognized that it was not in compliance with USM requirements for awarding the High Ability Merit Scholarships and established new procedures for awarding the scholarships. To ensure that students meet the award criteria and to prevent over-awarding, the responsibility for awarding students was transferred from the Assistant Vice President for Enrollment Management to the Scholarship Coordinator in the Office of Financial Aid. The awards are reviewed and approved by the Director of Financial Aid, Assistant Director of Financial Aid or Program Management Specialist.

## AUDIT TEAM

**Bekana Edossa, CPA, CFE**
Audit Manager

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

**J. Alexander Twigg**
**Edward J. Welsh, CFE**
Senior Auditors

**Omar A. Gonzalez, CPA**
**Christopher D. Jackson**
Information Systems Senior Auditors

**Marissa L. Eby**
**Isatta B. Mead**
**Brittany M. Solomon**
Staff Auditors

**Matthew D. Walbert**
Information Systems Staff Auditor

**Michell Min**
Staff Audit Intern