Audit Report

University System of Maryland
University of Maryland, College Park
Office of Information Technology

October 2009

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

Bruce A. Myers, CPA
Legislative Auditor

October 6, 2009

Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Senator Verna L. Jones, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the University System of Maryland – University of Maryland, College Park (UMCP), Office of Information Technology (OIT). OIT provides computing and network resources and operates as a computer service bureau for UMCP. Our audit included an internal control review of the UMCP data center and the network administered by OIT.

Our audit disclosed that proper internal control had not been established over several significant areas. For example, the UMCP internal network was not properly protected from external exposures. Furthermore, controls over modifications made to critical data center system files were not adequate. Systems that operate on the UMCP computing platforms include student information, student accounts receivable, and financial aid.

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

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

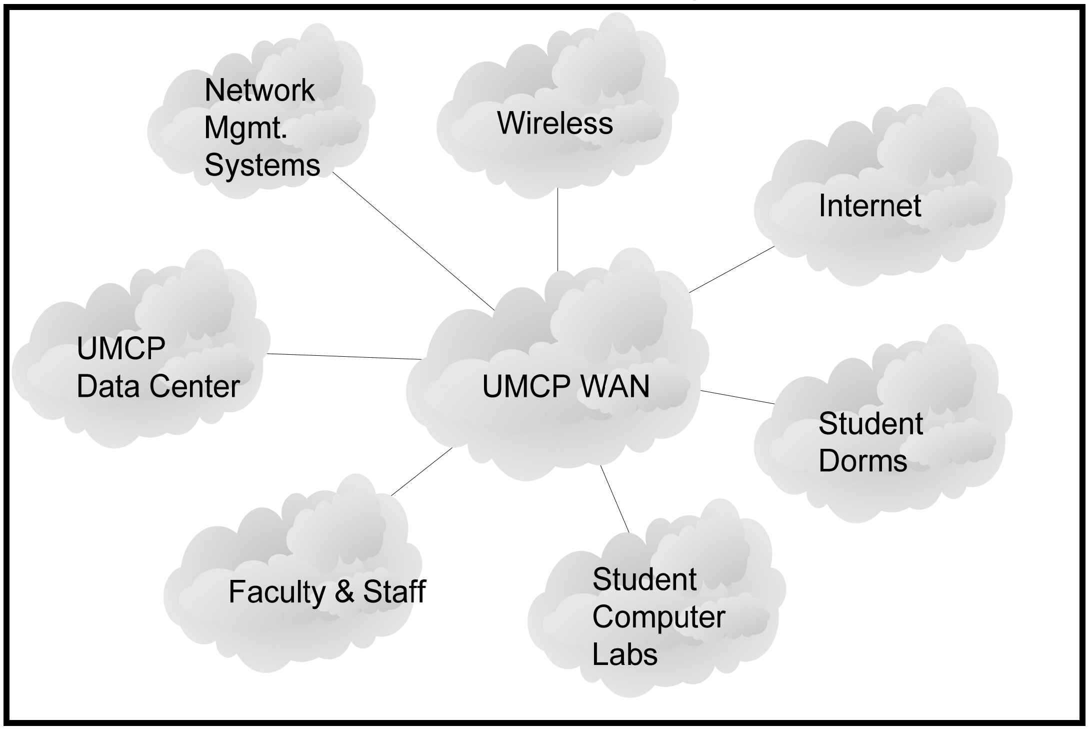
* **Denotes item repeated in full or part from preceding audit report**

Background Information

Office of Information Technology Responsibilities

The Office of Information Technology (OIT) is responsible for providing computer and communications resources and services to faculty, staff, and students at the University of Maryland, College Park (UMCP). Its staff develops and supports applications (for example, payroll, student accounts receivable, student grade files) on a variety of computers and operates an extensive computer network. OIT uses a mainframe and numerous servers for UMCP's primary applications. The network is managed by OIT's Network Telecommunications Services Division and provides Internet access, wireless network access, email, and file sharing to approximately 37,000 students and 9,500 full-time equivalent faculty and staff in more than 200 buildings on the UMCP campus. According to UMCP records, OIT has a budget of approximately $39 million, and has 354 permanent and contractual positions for fiscal year 2009. See below for a graphic depiction of the UMCP's network and its components.

Overview of the UMCP's Networking Environment



OIT operates a network for UMCP that includes numerous servers, a mainframe computer, numerous firewalls, critical routers, and connectivity to the Internet.

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 January 19, 2006. We determined that OIT satisfactorily addressed five of these seven findings. The remaining two findings are repeated in this report.

Findings and Recommendations

Network Security and Control

Background

The Office of Information Technology (OIT) is responsible for managing UMCP's wide area network (WAN) and for providing external connectivity to UMCP's computing systems. The UMCP WAN comprises more than 1,500 network devices. The core portion of the WAN includes a number of switches/routers and firewalls which are used to protect critical network segments including the data center (which houses the mainframe and critical production servers) and the network management systems (which contain critical servers used to maintain the UMCP network). The WAN also includes several virtual private network devices used by staff and faculty. The UMCP network is connected to the Internet through three Internet service providers and to the network.MD Statewide Government Intranet network (SwGI). In addition, the UMCP WAN has a wireless component that covers the UMCP Campus for use by faculty, staff, students, and visitors.

Finding 1
The internal computer network was not adequately protected.

Analysis

The internal network was not adequately protected. Specifically, we noted the following conditions:

- The data center and the network management systems were not adequately secured from certain traffic from several untrusted third parties, including the Internet, students, computer labs, and the wireless network. For example, students and the public, through the Internet, could access internal servers used for the student admissions process and for viewing and posting student grades. Access rules for critical network devices should use a "least privilege" security strategy that gives users only the access needed to perform assigned tasks.

- Account controls over administrative access to core network devices were inadequate. For example, 23 employees (including 3 terminated employees) had unnecessary administrative read access to core network devices responsible for protecting the internal network. Unnecessary read access could allow an individual to gather information with the intent of attacking these network devices.

- Numerous outdated access rules resided on several firewalls/routers tested. As a result, access to network devices that was not warranted may have been allowed.

Recommendation 1
We recommend that adequate controls be established to protect the internal network. We made detailed recommendations to OIT which, if implemented, should provide for adequate security in this area.

Finding 2
Monitoring of critical network devices was not adequate.

Analysis
Monitoring of critical network devices, including routers and the mainframe firewall, was not adequate as follows:

- The firewall protecting the mainframe computer was not configured to log all key user and system activity and to alert administrators to critical firewall operating conditions. Furthermore, we were advised that the firewall event log was not routinely reviewed; in addition, the reviews performed were not documented.

- We were advised that the security and event logs for all core routers and critical management and authentication servers were not regularly reviewed. Furthermore, the reviews performed were not documented.

Recommendation 2
We recommend that OIT

a. ensure that all key security events recorded by critical network devices are logged, and that administrator alerts are enabled; and

b. regularly review security and event logs for critical network devices, follow up on questionable items, and document these reviews and investigations.

Finding 3
Wireless network access to critical applications was not adequately secured through encryption.

Analysis
Wireless network access to critical applications was not adequately secured through encryption. Individuals could choose to establish a wireless connection either in a secured (encrypted) mode or in an unencrypted mode. Wireless connections made involving an unencrypted session exposed the wireless transmissions to improper disclosure. Software is readily available on the Internet that can intercept and scan unencrypted wireless network traffic to obtain confidential information. A similar condition was commented upon in our preceding audit report.

The University System of Maryland's (USM) *Guidelines in Response to the State's IT Security Policy*, dated March 2008, require that institutions use encryption for any transmission of, or access to, sensitive information.

Recommendation 3
We again recommend that UMCP require that all wireless connections to critical UMCP applications use secure (encrypted) methods.

Data Center Information System Security and Control

Finding 4
Logging and reporting over certain critical system and production data file modifications were not adequate to ensure the propriety of the modifications.

Analysis
Logging and reporting over certain critical system and production data file modifications were not adequate to ensure the propriety of the modifications. Specifically, we noted the following conditions:

- Modifications to numerous critical system files were not logged by the security software. A similar condition was commented upon in our preceding two audit reports.

- Direct modifications to production data files used by the student information, student accounts receivable, and financial aid systems were not logged by the security software. A similar condition was commented upon in our preceding audit report.

- The computer program that generated the report of logged changes to critical system files did not include numerous system files in its search parameters. In addition, the report generated by this program did not identify the specific files that were changed; rather it only identified the libraries containing the changed files. Accordingly, this report was of limited use in monitoring changes to system files.

As a result of these conditions, there was a lack of assurance as to the propriety of changes made to numerous system and production data files.

Recommendation 4
We recommend

a. that modifications to critical system files be logged by the security software (repeat);

b. that direct modifications to production data files used by the student information, student accounts receivable, and financial aid systems be logged by the security software (repeat); and

c. that the report of logged changes to critical system files be amended to include changes to all critical system files and to specifically identify the files that were changed.

Audit Scope, Objectives, and Methodology

We have audited the University System of Maryland – University of Maryland College Park (UMCP), Office of Information Technology (OIT). Fieldwork associated with our audit of OIT was conducted during the period from May 2008 to March 2009. Additionally, fieldwork associated with our audit of the network was conducted during the period from December 2008 to June 2009. 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 OIT's internal control over the UMCP data center and network, and to evaluate its compliance with applicable State laws, rules, and regulations for the computer systems that support UMCP. Our audit also included an assessment of the security controls for critical routers, firewalls, switches, and virtual private network appliances, as well as an assessment of security controls related to UMCP's wireless connectivity and the use of software vulnerability assessments for critical network servers. OIT's fiscal operations are audited separately as part of our audit of UMCP; the latest report that covered OIT's fiscal operations was issued on March 25, 2009. We also determined the status of the findings included in our preceding audit report on OIT, dated January 19, 2006.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of materiality and risk. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of OIT'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.

OIT'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 OIT'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 OIT that did not warrant inclusion in this report.

The University System of Maryland Office's response, on behalf of OIT, 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 the Office regarding the results of our review of its response.

APPENDIX

UNIVERSITY SYSTEM OF MARYLAND

OFFICE OF THE CHANCELLOR

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

1985
University of Maryland Biotechnology Institute

October 5, 2009

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, MD 21201

Re: Audit of University System of Maryland –
University of Maryland, College Park, Office of
Information Technology
Report Date: September 2009

Dear Mr. Myers:

I have enclosed the University System of Maryland's response to your draft report covering the examination of the accounts and records of the University System of Maryland, University of Maryland, College Park – Office of Information Technology. Our comments refer to the individual items contained in the report.

Sincerely,

W E Kirwan

William E. Kirwan
Chancellor

Enclosure
WEK:mpk

cc: Dr. C.D. Mote, Jr., President, UMCP
Mr. Clifford M. Kendall, Chair, Board of Regents, USM
Dr. Jeffrey C. Huskamp, Chief Information Officer, UMCP – OIT
Mr. Robert L. Page, Comptroller, USM
Mr. Kevin M. O'Keefe, Chair, MHEC
Dr. James E. Lyons, Sr., Secretary of Higher Education, MHEC
Mr. David Mosca, Director of Internal Audit, USM
Dr. Anne G. Wylie, Vice President for Administrative Affairs, UMCP
Ms. Julie K. Phelps, Asst VP for Administrative Affairs, UMCP

University of Maryland, College Park
Response to OLA Audit Dated September 2009
September 25, 2009

Recommendation 1
We recommend that adequate controls be established to protect the internal network. We made detailed recommendations to OIT which, if implemented, should provide for adequate security in this area.

Response 1

The University concurs. OIT agrees to implement additional corrective actions to further protect the internal network.

Due Date: 1/31/2010

Recommendation 2
We recommend that OIT

a. ensure that all key security events recorded by critical network devices are logged, and that administrator alerts are enabled; and
b. regularly review security and event logs for critical network devices, follow up on questionable items, and document these reviews and investigations.

Response 2

The University concurs.

a. OIT will take the necessary corrective actions to ensure that all key security events recorded by critical network devices are logged, and that administrator alerts are enabled; and
b. OIT will implement processes to regularly review security and event logs for critical network devices, follow up on questionable items, and document these reviews.

Due Date: 6/30/2010, contingent upon budget and resource availability.

University of Maryland, College Park
Response to OLA Audit Dated September 2009
September 25, 2009

Recommendation 3
We again recommend that UMCP require that all wireless connections to critical UMCP applications use secure (encrypted) methods.

Response 3

The University concurs.

Since the previous audit, OIT has made substantial infrastructure improvements to implement OLA's recommendations with regard to this control weakness. All critical applications commonly accessed from the wireless network have been encrypted for the past two years. Efforts reflected in the response to finding #1 will close any remaining gaps.

Due Date: 1/31/2010

Recommendation 4
We recommend

a. **that modifications to critical system files be logged by the security software (repeat);**
b. **that direct modifications to production data files used by the student information, student accounts receivable, and financial aid systems be logged by the security software (repeat); and**
c. **that the report of logged changes to critical system files be amended to include changes to all critical system files and to specifically identify the files that were changed.**

Response 4

The University concurs with one exception.

a. OIT will log modifications to critical system files with the security software. However, we strongly disagree that this is a repeat finding. The specific file cited had not previously been identified as "critical".
b. OIT will implement corrective actions to log modification access to all administrative systems.
c. OIT will amend the modifications report to include all critical system files and specifically identify the files that were modified.

Due Date: 6/30/2010, contingent upon budget and resource availability.

AUDIT TEAM

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

R. Brendan Coffey, CPA
Omar A. Gonzalez, CPA
Information Systems Senior Auditors

Michael K. Bliss
Amanda L. Roller
Information Systems Staff Auditors