Audit Report

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

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

December 4, 2014

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

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 – University of Maryland, College Park (UMCP), Division of Information Technology (DIT). DIT maintains UMCP's data center which provides computing and network resources and operates as a computer service bureau for UMCP. Our audit included an internal control review of the data center and the network administered by DIT.

Our audit disclosed that firewalls were not used to secure all UMCP network segments from the Internet and untrusted portions of its internal network. In addition, certain firewalls allowed insecure and unnecessary connections to critical data center computer resources, and the intrusion prevention system was not configured to monitor traffic from several untrusted sources. We also noted that DIT did not ensure that anti-malware software was installed, up-to-date, and operating properly on most DIT-managed computers.

In addition, during the course of our audit, a data breach occurred at UMCP which resulted in the unauthorized disclosure of personally identifiable information in the custody of UMCP. The breach involved 287,580 records from an identity card database for faculty, staff, students, and affiliated personnel. The compromised records included each individual's name, social security number, date of birth, and UMCP identification number. This report contains a description of the events related to this data breach and UMCP's response.

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

Respectfully submitted,

Thomas J. BarnickelIII, 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

Background Information 4

Division of Information Technology Responsibilities 4
University of Maryland, College Park (UMCP) Data Breach 4
Status of Findings From Preceding Audit Report 7

Findings and Recommendations 8

Information System Security and Control
Finding 1 – UMCP Did Not Ensure that Firewalls Were Used to Properly Secure All Campus Network Segments 8
* Finding 2 – Firewalls and Intrusion Prevention Systems Were Not Configured to Ensure the Network Was Properly Secured 9
Finding 3 – Malware Protection for UMCP Computers Needs Improvement 10

Statewide Maryland Automated Record Tracking (SMART)
Finding 4 – UMCP Lacked Assurance that the SMART System and Its Sensitive Data Were Properly Secured 12

Audit Scope, Objectives, and Methodology 14

Agency Response Appendix

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

Background Information

Division of Information Technology Responsibilities

The Division of Information Technology (DIT) 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. DIT uses a mainframe and numerous servers for UMCP's primary applications.

Within DIT, the Networks and Communication Technologies (NCT) unit maintains a wide area network (WAN) and local area networks in all campus buildings. NCT is responsible for managing the network devices, resolving network problems, and providing external connectivity to UMCP's network users and systems. The UMCP WAN comprises over 1,500 network devices including firewalls, routers, and switches. The UMCP network is connected to the Internet through two separate providers and is also connected to the Network MD Statewide Government Intranet and the Maryland Research Educational Network. In addition, the UMCP WAN has a wireless network that covers the UMCP campus for use by faculty, staff, and students. According to UMCP records, the DIT had a budget of approximately $50 million, and had 419 permanent and contractual positions for fiscal year 2014.

UMCP Data Breach

On February 18, 2014, a data breach occurred at UMCP which resulted in the unauthorized disclosure of personally identifiable information (PII) in the custody of UMCP. The breach involved 287,580 records from an identity card database for faculty, staff, students, and affiliated personnel. The compromised records included each individual's name, social security number, date of birth, and UMCP identification number.

Data Breach Timing and Method

DIT personnel advised us that the attacker responsible for the breach performed a series of steps that provided increasing levels of improper access into UMCP's systems and network, which culminated with unauthorized access to the identity card database. Collectively, the attack involved compromising multiple computer resources hosted or maintained by DIT while taking advantage of certain security weaknesses. UMCP databases, systems, applications, and websites attacked and utilized in this compromise included: 1) a vulnerable publicly accessible web server and web application, 2) a back-end file system web administrative user

group with excessive group membership, 3) a management utility's source code, 4) an authentication server and the its associated back-end directory, 5) the system hosting DIT employee login credentials, 6) critical application source code associated with the identity card database, and finally, 7) the identity card database userid and password, and the identity card database itself.

UMCP Response

DIT immediately notified the University of Maryland Police Department of the data breach. Within 24 hours of discovering the breach UMCP officials notified the public by establishing a data breach website which presented a letter on the matter from the UMCP President. Shortly after the breach, UMCP took the following measures:

- **Notification -** UMCP attempted to notify individuals whose sensitive PII data were stolen using various methods to contact these individuals including: mailings, emails, phone calls, a website, media stories, and social media channels.

- **Credit Monitoring -** UMCP offered a free five-year, opt-in credit monitoring service to all affected individuals who applied for the service by May 31, 2014.

- **Task Force -** UMCP created a Task Force on Cybersecurity to identify policies and procedures for ensuring the future security of UMCP confidential data. The Task Force was also charged with accounting for all other confidential data on the UMCP network and for planning and performing a penetration test over UMCP systems.

- **Remediation -** UMCP corrected known system vulnerabilities that allowed the breach to occur.

Related Costs

We were advised by UMCP's Comptroller's Office that, of the population affected by the data breach, 35.1 percent (100,803 individuals) applied for the free credit monitoring service. Per UMCP's records, as of June 2, 2014, the cost of the credit monitoring service for fiscal year 2014 was approximately $818,000 and the estimated cost for fiscal year 2015 was approximately $1.6 million. Additional costs of $350,000 were incurred during fiscal year 2014 for providing a call center and for notification mailing services. We were advised by UMCP personnel that electronic data loss or data breach insurance was not maintained.

Task Force on Cybersecurity

UMCP's Task Force on Cybersecurity released its findings on June 12, 2014 and presented a report containing 18 recommendations which were described as being "necessary to bring the University of Maryland's IT environment to an acceptable level of security and to be in compliance with the University System of Maryland Security Standards." The recommendations encompassed policies, procedures, technology, and resources as they relate to the security of confidential data. The report and the detailed documentation included the following noteworthy issues:

1. **Existence of Confidential Information on UMCP systems -** The Task Force surveyed UMCP departments concerning the collection and storage of confidential information. The survey revealed that there were over 1,500 databases, systems, applications, and websites managed at the unit level that contain some amount of confidential data. Our review of the survey results revealed that 399 of these 1,500 objects collected and/or stored higher risk personal data such as social security numbers, bank account information, credit card numbers, or grades.

   Several Task Force report recommendations were related to confidential data as follows:

   - Data retention policies need to be implemented by the Data Policy Advisory Committee and data stewards.
   - UMCP must minimize the number of systems that contain confidential data and ensure that all confidential data are known and securely managed at approved locations.
   - UMCP should ensure the isolation of confidential data, limit access to it, and log access to it.
   - UMCP should implement a plan for the future discovery of confidential data and eliminate unnecessary locations with such data.
   - UMCP should use stronger authentication and authorization controls for accessing confidential data, as appropriate to the risk.

2. **Penetration Testing -** The Task Force recommended periodic penetration testing of central systems that use or access sensitive data. Consequently, an outside vendor was hired to perform penetration testing on UMCP systems. Separately, the penetration testing vendor's report cited six risks rated either high or medium including departmental segmentation/filtering and a lack of Internet border filtering of traffic using network management protocols.

3. **Balance between DIT and department operated IT systems -** The Task Force reviewed the balance between DIT and UMCP department operated IT systems and considered existing policies and recommended changes or additions as necessary. The Task Force recommended the creation of an IT

security advisory committee to facilitate collaboration between DIT and UMCP departments operating their own IT systems. Such collaboration should include developing and implementing IT security policy and processes, and developing a mechanism for periodic review and reporting on the security of UMCP departments which store or provide access to confidential data.

The actions taken by UMCP and its Cybersecurity Task Force, to assess security risks associated with retention and transmission of confidential data and to mitigate those risks now and in the future, appear to be appropriate. However, due to the focus of the Task Force being primarily the security over confidential data, those actions may not fully address the findings in our report.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the four findings contained in our preceding audit report dated October 6, 2009. We have determined that UMCP had satisfactorily addressed two of these four findings. The remaining two findings are repeated as one finding in this report.

Findings and Recommendations

Information Systems Security and Control

Background

The University of Maryland, College Park (UMCP) wide area network (WAN) is connected to various third-party networks including the Internet. Within the WAN, connections existed to UMCP departments, student computer labs, and student dormitories. According to the UMCP website there are over 500 separate departments that use the UMCP WAN. The Division of Information Technology (DIT) maintained network firewalls at the locations where certain critical UMCP network segments connected to the UMCP WAN.

Finding 1
UMCP did not ensure that firewalls were used to properly secure all campus network segments.

Analysis

UMCP did not ensure that firewalls were used to secure all campus network segments from the Internet and untrusted portions of its internal network.

- Firewalls were not in use at the points where the UMCP WAN connected to third-party networks including the Internet. Additionally, our review determined that only limited network traffic filtering was performed at these connections to protect the WAN from third-party networks.

- UMCP did not have a campus-wide policy mandating the use of firewalls to secure departmental local area networks from untrusted parties. Additionally, we were advised that DIT did not determine if all UMCP departments were maintaining firewalls. As such, there was no assurance that all UMCP departmental networks were secured against unauthorized traffic from untrusted parties including the Internet, student computer labs, and student dormitories. Furthermore, while DIT did provide an optional (opt-in) firewall service to all other UMCP departments that would filter traffic at the department's network interface with the UMCP WAN, DIT maintained firewalls for only 15 of the over 500 campus departments as of February 26, 2014, according to UMCP records.

  We tested eight departments (separate from DIT) which had not used the DIT provided opt-in firewall service, and determined that for all eight departments tested, firewall coverage did not exist to filter network-level traffic to departmental workstations, including traffic that could originate from untrusted parties. As a result, the Internet, student computer labs, and

dormitories had unnecessary, unfiltered network-level access to the faculty and staff workstations in these tested departments which included the President's Office, the Comptroller's Office, and the Bursar's Office. We were advised that there were approximately 500 workstations in these eight departments.

Firewalls should be used to help implement a least privilege security strategy, giving individuals, including those accessing the network via the Internet, only those privileges needed to perform assigned tasks. In this regard, the University System of Maryland (USM) *IT Security Standards* dated July 2014 state that institutional networks must be protected by firewalls at identified points of interface as determined by system sensitivity and data classification.

Recommendation 1
We recommend that UMCP implement a campus-wide policy which ensures that the UMCP WAN and all departmental networks are secured against unauthorized traffic from untrusted parties including the Internet, student computer labs, and student dormitories.

Finding 2
Firewalls and intrusion prevention systems were not configured to ensure the UMCP network was properly secured.

Analysis
Firewalls and the intrusion prevention systems were not configured to ensure the UMCP network was properly secured.

- Firewall rules allowed numerous unnecessary connections to portions of the UMCP network, placing various devices at risk. For example, all students, faculty, and staff had unnecessary network-level access to numerous mainframe addresses over various ports. In addition, we identified 16 firewall rules that were outdated and should be removed to better protect the network. The USM *IT Security Standards* 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. Similar conditions were commented upon in our preceding audit report.

- Security event logs for DIT maintained firewalls, routers, and switches were not properly reviewed. Although UMCP staff periodically reviewed these logs, these reviews did not specifically address security-related events (such as failed logon attempts), were not performed regularly, and were not documented. The USM *IT Security Standards* require that entities maintain comprehensive audit trails and implement regular, documented review

procedures. A similar condition was commented upon in our preceding audit report.

- Although UMCP used a network-based intrusion prevention system (IPS) to detect and prevent malicious traffic, the IPS was not configured to review traffic flowing from several untrusted network segments (campus computer labs and student dormitories) to critical administrative network segments.

- UMCP did not use host-based intrusion protection systems (HIPS) on 30 critical servers, in its data center, that processed encrypted traffic. The absence of HIPS coverage for such traffic created network security risk in that UMCP's network-based IPS cannot read encrypted traffic flowing into its network whereas HIPS can read and analyze such traffic and protect critical servers from malicious traffic. In this regard, the USM *IT Security Standards* require that institutions establish automated and manual processes for intrusion detection and/or prevention and state that host-based, network-based, or a combination of both (preferred) may be utilized.

Recommendation 2
We recommend that UMCP

a. configure its firewalls to adequately secure its network (repeat);
b. regularly review the security events on the event logs for all critical network devices, investigate any unusual or questionable items, document these reviews and investigations, and retain the documentation for future reference (repeat); and
c. perform a documented review and assessment of its network security risks and identify how IPS and HIPS coverage should be best applied to its network and, based on this review and assessment, implement such coverage as necessary.

Finding 3
Malware protection for UMCP computers needs improvement.

Analysis
Malware protection for UMCP computers needs improvement.

- Although UMCP used an enterprise-wide management tool to provide malware protection for its servers and workstations, UMCP did not use the management capabilities of this tool to verify such malware protection software was installed, up-to-date, and operating properly and that the related definitions files were kept up-to-date on DIT-managed computers (3,204 servers and workstations are managed by DIT). Accordingly, as per the

management tool's console only 131 servers were monitored by this tool although it had the capability to manage both servers and workstations. The USM *IT Security Standards* state that, where feasible, software must be installed to protect the system from malicious programs such as viruses, trojans, and worms.

- Certain workstations were configured with users having administrative rights. Administrative rights are the highest permission level that can be granted to users and allow users to install software and change configuration settings. Our test of 12 workstations disclosed that 6 employees' user accounts were inappropriately defined with administrative rights rather than with user rights. As a result, if the workstations used by these 6 accounts were infected with malware, the malware would run with administrative rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights. The USM *IT Security Standards* require that institutions use a risk-based approach and implement and document processes that minimize the provisioning of local administrative rights so that only those employees who require it are given those rights.

Recommendation 3
We recommend that UMCP

a. use the management tool to monitor all DIT-managed computers to ensure the computers have malware protection software that is operational and up-to-date, and that the related definition files are also kept up-to-date; and

b. limit local administrative rights on user workstations to only personnel that require such rights.

Statewide Maryland Automated Record Tracking

Background

UMCP's Institute for Governmental Service and Research (IGSR) is responsible for operating the Statewide Maryland Automated Record Tracking (SMART) system which contains a substantial amount of personally identifiable information (PII) and personal health information (PHI). SMART is a web-based client tracking system used by state agencies and private treatment providers to monitor and report on individuals in the Maryland drug court program.

Effective June 30, 2011, IGSR executed an agreement with a private contractor for "colocating, housing, managing, trouble shooting, and supporting the SMART production server, network infrastructure and legacy systems interface infrastructure in a shared commercial site, … in conjunction with IGSR systems

management staff." We were advised by IGSR management that the primary contractor subcontracted the colocation and hosting of SMART with a data center hosting company. We were further advised by IGSR management that the primary contractor was responsible for implementing and maintaining the general and network security controls related to the SMART system.

Within SMART, sensitive PII (name and social security number) as well as PHI (name and medical records, drug test results) exists for individuals tracked by the system. We were advised by IGSR management, that per SMART records, the system contained sensitive PII and PHI for approximately 1,250,000 individuals.

Finding 4
UMCP lacked assurance that the SMART system and its sensitive data were properly secured.

Analysis
UMCP lacked assurance that the SMART system and its sensitive data were properly secured.

- At the time of our audit work (June 2014), IGSR had not performed any security reviews of the SMART system control environment. The agreement between IGSR and the primary contractor allowed UMCP to conduct reviews of the primary contractor's operations.

- The aforementioned contract between IGSR and the primary contractor did not contain any requirements for periodic, independent reviews of the security controls of the primary contractor and any subcontractors performing material services for the SMART system.

- The network security controls pertaining to the SMART system, which were implemented and maintained by the primary contractor, were not reviewed by any independent parties.

- An independent review had recently been performed of the subcontractor used to host the SMART system. We determined that the subcontractor had Service Organization Control 1 (SOC 1) Type 2 reviews performed over its United States data center hosting services, the most recent of which covered the period of November 1, 2012 through October 31, 2013. These reviews only covered the subcontractor's general controls and, therefore, did not address other critical controls such as those over networks, applications, or databases. Furthermore, IGSR management had not obtained copies of the related reports prior to our inquiries on the subject.

As a result of these conditions, UMCP lacked assurance as to the adequacy of the general and network security controls over the SMART system and its sensitive data.

Best practices require that service providers demonstrate compliance with industry information security requirements, and that customer entities regularly obtain from service providers related reports (see SOC reports described below) that evidence such compliance.

The American Institute of Certified Public Accountants has issued guidance concerning examinations of service organizations. Based on this guidance, service organizations (like the aforementioned contractor and subcontractor) may contract for an independent review of controls and the resultant independent auditor's report is referred to as a Service Organization Controls (SOC) report. There are several types of SOC reports, with varying scope and levels of review and auditor testing. One type of report, referred to as a SOC 2 Type 2 report, includes the results of the auditor's review of controls placed in operation and tests of operating effectiveness for the period under review and could include an evaluation of system security, availability, processing integrity, confidentiality, and privacy. Due to the nature and sensitivity of the information contained in the SMART system, we believe a SOC 2 Type 2 report would be appropriate.

Recommendation 4

We recommend that UMCP

a. **either require, via contract, that the primary contractor and any subcontractors performing material services for the SMART system periodically (annually) obtain SOC 2 Type 2 reviews and reports for the provided services or, use UMCP audit resources to perform annual security and control reviews to ensure that adequate controls exist over the system;**
b. **obtain and review copies of any reports resulting from the aforementioned security and control reviews (for example SOC reports) and determine if the related independent reviews adequately address the aforementioned security concerns over the SMART system; and**
c. **ensure that all critical exceptions noted (in either these SOC reports or in the UMCP audit reports) were adequately addressed by the primary contractor and its subcontractors.**

Audit Scope, Objectives, and Methodology

We have audited the University System of Maryland – University of Maryland College Park (UMCP), Division of Information Technology (DIT). Fieldwork associated with our audit of DIT was conducted during the period from February 2013 to March 2014. Additionally, fieldwork associated with our audit of the network was conducted during the period from December 2013 to September 2014. 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 DIT's internal control over the UMCP data center and network and to evaluate its compliance with applicable State laws, rules, and regulations for computer systems that support UMCP. DIT's fiscal operations are audited separately as part of our audit of UMCP. The latest report that covered UMCP's fiscal operations was issued on July 14, 2011.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of significance and risk. The areas addressed by the audit included procedures and controls over the mainframe operating system, security software, and critical databases. 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 anti-malware software to protect UMCP computers. Additionally, we audited the controls over certain information maintained by UMCP's Institute for Governmental Service and Research. We also determined the status of the findings included in our preceding audit report on DIT.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of DIT's operations. We also tested transactions and 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.

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

The University System of Maryland Office's response, on behalf of DIT, 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

OFFICE OF THE CHANCELLOR

December 1, 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 – University of Maryland, College Park- Division of Information Technology

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 the University of Maryland, College Park, Division of Information Technology. Our comments refer to the individual items in the report.

Sincerely,

William E. Kirwan
Chancellor

WEK:mk

Enclosures

cc: Dr. Wallace D. Loh, President, UMCP
Mr. James L. Shea, Chair, Board of Regents
Mr. Eric L. Denna, Vice President and CIO, UMCP
Mr. Anwar Hasan, Chair, MHEC
Ms. Catherine Shultz, Acting Secretary of Higher Education, MHEC
Mr. Robert L. Page, Associate Vice Chancellor for Financial Affairs, 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
UNIVERSITY OF MARYLAND, COLLEGE PARK
DIVISION OF INFORMATION TECHNOLOGY

Information Systems Security and Control

Finding 1
UMCP did not ensure that firewalls were used to properly secure all campus network segments.

Recommendation 1
We recommend that UMCP implement a campus-wide policy which ensures that the UMCP WAN and all departmental networks are secured against unauthorized traffic from untrusted parties including the Internet, student computer labs, and student dormitories.

University response
We agree with this finding. Firewalls have been used extensively to defend critical networks inside the university. Using a risk based approach, we will continue to expand our firewall deployment until all departmental networks and the UMCP WAN are secured against unauthorized traffic.

Finding 2
Firewalls and intrusion prevention systems were not configured to ensure the UMCP network was properly secured.

Recommendation 2
We recommend that UMCP

a. **configure its firewalls to adequately secure its network (repeat);**
b. **regularly review the security events on the event logs for all critical network devices, investigate any unusual or questionable items, document these reviews and investigations, and retain the documentation for future reference (repeat); and**
c. **perform a documented review and assessment of its network security risks and identify how IPS and HIPS coverage should be best applied to its network and, based on this review and assessment, implement such coverage as necessary.**

University response
UMCP agrees with this finding.

a. The firewall deployments at UMCP have outgrown our ability to manage the complex configurations manually. A Firewall Management System has been

procured and is currently in testing. This system will greatly expand our ability to identify incorrect or obsolete firewall rules and alert management to unauthorized modifications to firewall rules.

b. UMCP recognizes that log review procedures need improvement. Over the past year, an investment has been made in log management technology and additional staff are now allocated to reviewing logs.

c. UMCP will conduct a network risk assessment and apply security controls based upon the results.

Finding 3
Malware protection for UMCP computers needs improvement.

Recommendation 3
We recommend that UMCP

a. use the management tool to monitor all DIT-managed computers to ensure the computers have malware protection software that is operational and up-to-date, and that the related definition files are also kept up-to-date; and

b. limit local administrative rights on user workstations to only personnel that require such rights.

University response
UMCP agrees with this finding.

a. DIT is currently extending the management tool to include desktop and laptop computers. While these systems have been protected from malware, we will now be able to monitor the status of these systems.

b. Administrative rights will be limited on user workstations to those that require such rights.

Finding 4
UMCP lacked assurance that the SMART system and its sensitive data were properly secured.

RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
UNIVERSITY OF MARYLAND, COLLEGE PARK
DIVISION OF INFORMATION TECHNOLOGY

Recommendation 4
We recommend that UMCP

a. either require, via contract, that the primary contractor and any subcontractors performing material services for the SMART system periodically (annually) obtain SOC 2 Type 2 reviews and reports for the provided services or, use UMCP audit resources to perform annual security and control reviews to ensure that adequate controls exist over the system;

b. obtain and review copies of any reports resulting from the aforementioned security and control reviews (for example SOC reports) and determine if the related independent reviews adequately address the aforementioned security concerns over the SMART system; and

c. ensure that all critical exceptions noted (in either these SOC reports or in the UMCP audit reports) were adequately addressed by the primary contractor and its subcontractors.

University response

UMCP agrees with this finding.

IGSR will work with security resources in the Division of Information Technology to ensure that contractors performing material services for the SMART system provide adequate documentation of their security controls and that critical exceptions are adequately addressed.

AUDIT TEAM

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

R. Brendan Coffey, CPA, CISA
Edwin L. Paul, CPA, CISA
Information System Senior Auditors

J. Gregory Busch
Matthew D. Walbert
Information System Staff Auditors