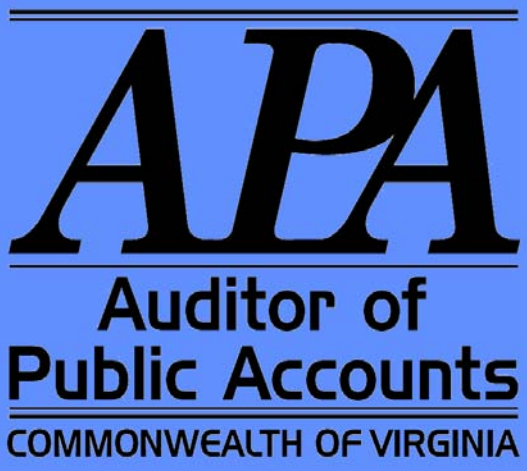
UNIVERSITY OF MARY WASHINGTON

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2008



AUDIT SUMMARY

Our audit of the University of Mary Washington for the year ended June 30, 2008, found:

- the financial statements are presented fairly, in all material respects;
- an internal control matter necessary to bring to management's attention;
- no instances of noncompliance or other matters required to be reported; and
- the University has taken adequate corrective action with respect to the audit finding reported in the prior year.

We have audited the basic financial statements of the University of Mary Washington as of June 30, 2008, and for the year then ended and issued our report thereon dated May 4, 2009. Our report, included with the University's basic financial statements, is available at the Auditor of Public Accounts' web site at www.apa.virginia.gov and at the University's web site at www.umw.edu.

–TABLE OF CONTENTS–

INTERNAL CONTROL FINDING AND RECOMMENDATION

Improve Information Systems Security Program

The University does not have practices in place to protect both the information infrastructure and data under the control of the University which would meet the basic requirements of the Commonwealth information security standard. Much of the lack of compliance with the basic requirements will become apparent by properly completing the documentation of the University's needs, training requirements, and oversight responsibility for safeguarding these resources.

While the University must improve its overall information systems security program, the following items and processes require immediate attention by management and will address some significant problems.

1. Improve the incident response plan.

2. Require vendors and their employees handling sensitive data to take data protection training and annually sign non-disclosure agreements for sensitive data in their possession. Also, amend all such contracts to have this requirement.

3. Strengthen the security of its firewalls.

An incident response plan is the actions the University would take to respond to cyber attacks and sets a process to prioritize security incidents to ensure that staff promptly identify and resolve urgent incidents. The University should supplement its current plan with Information Technology (IT) staff response procedures and preserve electronic evidence for potential investigation. Proper incident handling procedures help to minimize the loss or compromise of sensitive data and disruption of services.

The University shares sensitive data with outside entities, but does not include contract requirements that the vendor and their employees secure transmission, storage, access, system breach, and adherence to regulatory requirements. Contract provisions should include provisions for compliance with University IT policies, procedures, and requirements for information security practices.

The University does not properly install and analyze firewalls that control access to its IT infrastructure and systems that contain sensitive and mission critical data. We have communicated the details of our specific findings to the University in a separate document and since it describes security processes, this document is exempt from the Freedom of Information Act under Section 2.2-3705.2 of the Code of Virginia.

Overall, the University has not fully assessed its needs, risks and other vulnerabilities which its Information Systems Security Program should address. Without conducting the assessments and properly documenting the outcomes and processes the University will follow, the University cannot expect its information security program to protect the University from risks to its system and data.

The University's Information Security Officer (ISO) has responsibility for the development and management of the overall information security program. The ISO must also ensure that the University's security plan always meets current Commonwealth IT standards or other best practices in this area. The ISO can accomplish this by performing internal reviews to evaluate the performance of the University's information security program and making the necessary adjustments, and providing training as the IT environment changes.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

May 4, 2009

The Honorable Timothy M. Kaine
Governor of Virginia

The Honorable M. Kirkland Cox
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
University of Mary Washington

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited the financial statements of the business-type activities and discretely presented component units of the **University of Mary Washington** as of and for the year ended June 30, 2008, which collectively comprise the University's basic financial statements, and have issued our report thereon dated May 4, 2009. Our report was modified to include a reference to other auditors. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of the University of Mary Washington, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit, we considered the University's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing an opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles, such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control over financial reporting. We consider the deficiency entitled

"Improve Information Systems Security Program," described in the section of our report entitled "Internal Control Finding and Recommendation" to be a significant deficiency in internal control over financial reporting.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies and, accordingly, would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, we believe that the significant deficiency described above is not a material weakness.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

The University's response to the finding identified in our audit is included in the section titled "University Response." We did not audit the University's response and, accordingly, we express no opinion on it.

Status of Prior Findings

The University has taken adequate corrective action with respect to the audit finding reported in the prior year.

Report Distribution and Exit Conference

The "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters" is intended solely for the information and use of the Governor and General Assembly of Virginia, the Board of Visitors, and management, and is not intended to be and should not be used by anyone, other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

We discussed this report with management at an exit conference held on April 30, 2009.

AUDITOR OF PUBLIC ACCOUNTS

JHS/alh

Judy G. Hample
President

May 4, 2009

Mr. Walter J Kucharski
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218

Subject: Management Response to the Audit Recommendation for Fiscal Year Ending June 30, 2008

Dear Mr. Kucharski:

I would like to thank you and your team for their careful and methodical consideration during their IT security review. Below are our responses:

1. *Improve the incident response plan.*
   Managements' Response: IT Management will modify the existing plan to include more detailed procedures as described in VITA guidelines and emerging best practices.

2. *Require vendors and their employees handling sensitive data to take data protection training and annually sign non-disclosure agreements for sensitive data in their possession. Also, amend all such contracts to have this requirement.*
   Managements' Response: IT Management will review all existing contracts to ensure that when appropriate, agreements are in place that require vendors and their employees handling sensitive data to take data protection training and annually sign non-disclosure agreements for sensitive data in their possession. Also, IT Management will ensure that such agreements are properly documented and that such documentation is periodically reviewed for consistency with emerging policy.

3. *Strengthen the security of firewalls.*
   Managements' Response: IT Management will review and improve the management and documentation of its firewalls.

If you have any questions or need additional information, please do not hesitate to contact us.

Sincerely,

Judy G. Hample

1301 College Avenue
Fredericksburg, VA 22401-5300
Email: jhample@umw.edu
Tel: (540) 654-1301
Fax: (540) 654-1076
Cell: (540) 645-3709

UNIVERSITY OF MARY WASHINGTON

BOARD OF VISITORS
At June 30, 2008

J. William Poole, Rector

Nanalou W. Sauder, Vice Rector

Daniel K. Steen, Secretary

Randall R. Eley	Princess R. Moss
Elizabeth F. Foster	Patricia B. Revere
Benjamin W. Hernandez	Xavier R. Richardson
Martha K. Leighty	Russell H. Roberts
C. Maureen Stinger	

ADMINISTRATIVE OFFICERS

Judy G. Hample, President

Richard V. Hurley, Executive Vice President and Chief Financial Officer

Richard R. Pearce, Associate Vice President for Business and Finance

Allyson P. Moerman, Assistant Vice President for Finance and Controller