April 3, 2009

MEMORANDUM

TO: The Audit and Compliance Committee:

Austin Ligon, Chair
Helen E. Dragas
Robert D. Hardie
Vincent J. Mastracco, Jr.
Don R. Pippin
Warren M. Thompson
W. Heywood Fralin, Ex Officio

and

The Remaining Members of the Board:

Daniel R. Abramson  Glynn D. Key
A. Macdonald Caputo  Lewis F. Payne
Alan A. Diamonstein  E. Darracott Vaughan, Jr., M.D.
Susan Y. Dorsey  John O. Wynne
Thomas F. Farrell, II  Adom Getachew

FROM: Alexander G. Gilliam, Jr.

SUBJECT: Minutes of the Meeting of the Audit and Compliance Committee on April 3, 2009

The Audit and Compliance Committee of the Board of Visitors of the University of Virginia met, in Open Session, at 8:35 a.m., on Friday, April 3, 2009, in the Board Room at the Rotunda; Austin Ligon, Chair, presided.

Present were Ms. Helen E. Dragas, Robert D. Hardie, Vincent J. Mastracco, Jr., Don R. Pippin, Warren M. Thompson, and W. Heywood Fralin, Rector.

Also present were John O. Wynne, A. Macdonald Caputo, The Hon. Alan A. Diamonstein, Thomas F. Farrell, II, Ms. Glynn D. Key, and The Hon. Lewis F. Payne.

Rahul Gorawara, the Student Member-elect, was present.

Ms. Helen Vanderland, from the Office of the Auditor of Public Accounts of the Commonwealth, was present.

The Chair asked Ms. Deily, Chief Audit Executive, to present the Agenda.

Approval of the Program to Prevent, Detect, and Mitigate Identity Theft.

Ms. Deily introduced Mr. Stephen Kimata, University Comptroller, who gave a presentation on the University’s program to prevent, detect, and mitigate identity theft. The program must be approved by May 1st and will apply to the University and to the Medical Center, as well as to the College at Wise.

By law, the program must be in compliance with what is commonly referred to as the “Red Flags Rule,” issued by the Federal Trade Commission and several federal banking agencies in late 2007.

The Committee adopted the following resolution and recommended it to the full Board of Visitors for approval:

APPROVAL OF THE PROGRAM TO PREVENT, DETECT, AND MITIGATE IDENTITY THEFT

WHEREAS, Federal regulations require the University to approve a program to prevent, detect, and mitigate identity theft; and

WHEREAS, the University of Virginia Program to Prevent, Detect, and Mitigate Identity Theft, a copy of which is appended to this resolution, has been devised;

RESOLVED, the Board of Visitors approves the University of Virginia Program to Prevent, Detect, and Mitigate Identity Theft and assigns the Executive Vice President and Chief Operating Officer as the oversight executive for the Program; he shall be authorized to make appropriate revisions to the Program, and may delegate its administration to appropriate senior University officials.
The University of Virginia Program to Prevent, Detect, and Mitigate Identity Theft

The University of Virginia Program to Prevent, Detect, and Mitigate Identity Theft is composed of existing University policies and procedures, related to identity theft and incident reporting, along with a plan for the development of new policies and procedures in specific areas.

The institution already has in place several core existing policies and procedures which address various aspects of identity theft. These policies and procedures include, but are not limited to:

- Protection and Use of Social Security Numbers
- Electronic Storage of Highly Sensitive Data
- Rights of Students at the University of Virginia Pursuant to the Family Educational Rights and Privacy Act (FERPA)
- Issuance and Use of University Identification Cards
- University Payroll Employee Responsibilities
- Release of Information from Faculty Personnel Records
- Confidentiality of Patient Information
- Patient Identification
- Verification for Release of Patient Information
- Information Technology Security Risk Management Program
- Electronic Data Removal Policy
- University Information Technology Security Incident Reporting Policy
- Reporting Fraudulent Transactions

These policies and procedures will continue to be in effect to reduce the risk of identity theft at the University of Virginia.

There are also new and proposed policies and procedures to further enhance the institution’s compliance with the requirements of the Red Flags Rule. These new and proposed policies and procedures include, but are not limited to:

- Medical Center Policy: Prevention, Detection, and Mitigation of the Theft of Patients’ Identities (NEW)
- Academic Division Policy: Prevention, Detection, and Mitigation of Identity Theft (PROPOSED)
These policies will require relevant University departments to create procedures to:

1. Identify indicators of identity theft ("red flags") that are relevant to the University’s operations;
2. Detect identified red flags and respond appropriately to detected red flags in order to prevent and mitigate identity theft;
3. Educate employees regarding their responsibilities under the Identity Theft Prevention Program;
4. Require vendors that perform activities involving accounts covered by the Red Flags Rule to have equivalent policies and procedures, and to report observed red flags to the University;

Responsible University Official

The Executive Vice President and Chief Operating Officer shall be the oversight executive for the Program and may delegate administration of the Program to appropriate senior University officials. The oversight executive or his designees shall exercise appropriate and effective management of the Program, and shall update it periodically to respond to evolving risks of identity theft.

The 2009-10 Entrance Conference of the Auditor of Public Accounts of the Commonwealth

Ms. Deily introduced Ms. Helen Vanderland, of the Office of the Auditor of Public Accounts of the Commonwealth. Ms. Vanderland conducted the 2009-10 Entrance Conference, which is a prelude to the Auditor’s annual audit of the University.

Mr. Wynne asked Ms. Vanderland to send to the Committee a copy of the Auditor’s guidelines for the audit.

Executive Session

The Committee adopted the following motion and went into Executive Session at 8:45 a.m.: 
That the Audit and Compliance Committee of the Board of Visitors convene in Closed Session to discuss the audit of University operations as it concerns the performance of specific University managers and personnel, the adequacy of patient tracking and security procedures and controls at the medical center and enhancing security controls and training in our information technology facilities and wireless networks, as permitted by Section 2.2-3711 (A) (1),(8),(19) and (22) of the Code of Virginia.

The Committee resumed its meeting in Open Session at 9:00 a.m., and adopted the following resolution certifying that its discussions in Executive Session had been held in accordance with the exemptions permitted by the Virginia Freedom of Information Act:

That we vote on and record our certification that, to the best of each Board member’s knowledge, only public business matters lawfully exempted from open meeting requirements and which were identified in the motion(s) authorizing the closed session, were heard, discussed or considered in closed session.

Approval of the Summary of Audit Findings

On motion, the Committee adopted the following resolution approving the Summary of Audit Findings, and recommended it to the full Board for approval:

APPROVAL OF THE SUMMARY OF AUDIT FINDINGS

RESOLVED, the Summary of Audit Findings for the period January 1, 2009, through February 28, 2009, as presented by the Chief Audit Executive, is approved as recommended by the Audit and Compliance Committee.

On further motion, the Committee adjourned.

These minutes have been posted to the University of Virginia’s Board of Visitors website.
http://www.virginia.edu/bov/auditminutes.html