The Regents of the University of California

COMMITTEE ON AUDIT

January 17, 2007

The Committee on Audit met on the above date at UCSF–Mission Bay Community Center, San Francisco.

Members present: Regents Coombs, Lozano, Parsky, Ruiz, Schilling, and Varner; Advisory member Oakley; Expert Financial Advisor Vining

In attendance: Regents De La Peña, Dynes, Hopkinson, Johnson, Ledesma, Preuss, and Schreiner, Regent-designate Brewer, Acting Secretary Shaw, General Counsel Robinson, Chief Investment Officer Berggren, Provost Hume, Vice Presidents Broome and Sakaki, Chancellors Fox and Vanderhoef, Acting Chancellor Blumenthal, University Auditor Reed, and Recording Secretary Bryan

The meeting convened at 3:10 p.m. with Committee Chair Ruiz presiding.

1. APPROVAL OF THE MINUTES OF THE PREVIOUS MEETING

Upon motion duly made and seconded, the minutes of the meeting of November 16, 2006 were approved.

2. APPROVAL OF REGENTS' POLICY ON AUDIT COMMITTEE CHARTER

Committee Chair Ruiz recommended that the attached Charter be adopted as a Regents' Policy.

University Counsel Thomas informed the Committee that development of a charter designed to provide a detailed description of an audit committee's responsibilities under corporate bylaws is recommended as a best practice in both the for-profit and nonprofit sectors. The Regents' Committee on Audit discussed a draft charter at its November 2006 meeting. The attached version has been modified to reflect that discussion. This charter would confirm the Committee's duties under Bylaw 12.1 for its members and for the Board of Regents as a whole, would guide the annual agenda, permit tracking of tasks, and provide part of an orientation for new members.

Following the passage of Sarbanes-Oxley in 2002, board audit committees have taken on expanded responsibilities. In 2003, The Regents amended Bylaw 12.1 to reflect best practices regarding the scope of duties for the Committee on Audit. Since 2003, it has become a best practice for audit committees to develop detailed charters implementing the scope of duties that are described generally in the bylaw. The proposed charter would function as confirmation of the Committee's duties under Bylaw 12.1 for its members and for the Board of Regents as a whole, would guide the annual agenda, permit tracking of tasks, and provide part of the orientation for new Committee members. It is recommended that the charter issue as a Regents Policy in order to facilitate periodic review and change as needed.

Upon motion duly made and seconded, the Committee approved the recommendation and voted to present it to the Board.

3. **INFORMATION SECURITY**

Acting Chancellor Abrams recalled that there had been a security breach at UCLA in which a database was broken into. The campus communicated with the 800,003 individuals whose names were in the database that was penetrated and took steps to ensure that all systems are secure and that only necessary information is retained in the database. Given the number of people whose information was subject to being stolen, their potential exposure to the risk of identify theft, and their feelings of being victimized, it was important to respond immediately and comprehensively. While databases are continually under attack and there is always the possibility of a break in, the campus has worked to keep the risk as low as possible. When the security break was detected, the campus focused immediately on its response to those who might be affected. As a result of a continuing investigation, it is known that only 3.5 percent of the total of 800,003 names and Social Security numbers were retrieved. Those individuals received a second communication to put them on still higher alert. Meanwhile, security reviews of other campus systems and ongoing programs have been accelerated to further eliminate the use of Social Security numbers. The other campuses have been informed, so that they can be on the alert for similar attacks.

Administrative Vice Chancellor Morabito provided further information about the circumstances surrounding the illegal access of a UCLA restricted campus database containing personal information. He reported that the database contained data on UCLA's current and some former students, faculty, and staff, some student applicants, and some parents of students or applicants who applied for financial aid. The database also included information about current and some former Office of the President and UC Merced employees for which UCLA does administrative processing. In total, information for 800,003 persons was stored in this database which contained Social Security numbers but did not contain driver's license numbers, credit card, or banking information. UCLA administrators discovered the breach on November 21, 2006 when they noticed an unusually high volume of activity on a campus data server. Further investigation indicated that an attack was in progress, and security staff took steps to take the compromised system off the network and begin a forensics investigation. UCLA's Incident Response Plan was invoked, including notifying UCOP and contacting the FBI, which began an investigation that continues. System log analysis indicated sophisticated and malicious attacks exploiting a previously undetected flaw in one of UCLA's applications. These attacks were specifically targeting the retrieval of Social Security numbers. The attack was undetected by UCLA staff until November because the hacker effectively concealed his or her activity or made it blend in with legitimate activity.

Further computer log analysis, in close cooperation with the FBI, indicated that the attacks were organized, sophisticated, and launched from network addresses external to UCLA.

A key step in the campus' response was the expeditious notification of potentially affected individuals to assist them by providing important information on fraud protection. The notification was made in accordance with the requirements of University policy and California Civil Code. While strict interpretation of the law would have required informing only a much smaller population, after considering the indications of criminal intent seen and the potential for broader access, the campus decided to notify everyone in the database who could have been affected. Notification was made as soon as possible after determining the scope of the incident and setting up arrangements to communicate to 800,003 people and handle the huge volume of anticipated telephone inquiries and e-mails in response. Notification was made through e-mail, U.S. Mail, and the UCLA gateway page, starting on December 12, 2006. A press release was issued simultaneously, and news stories were published nationally and internationally. To provide information and respond to queries, a special website was established and a toll-free information hotline was put in place. Up to 26 call centers throughout the United States and Canada with 1,600 operators were responding to as many as 1,000 calls per hour in the first days following the campus' announcement. To date, more than 35,000 calls have been received, representing just over 4 percent of the affected population, and UCLA personnel have responded to all of the over 400 calls requiring a direct contact.

Based on the continuing investigation, there is evidence that of the group of 800,003, about 28,600 Social Security numbers in combination with names were retrieved over a period of several months starting in October 2005. While the 28,600 are the only records the campus can confirm were retrieved by a hacker, given the sophistication and multiple methods used in the attack and the hacker's successful efforts to cover his or her identity, it is not certain whether other records in the database were retrieved. A second notification was made to those in this subset population of 28,600 on January 10, as soon as a notification database could be constructed from analysis of the computer logs. UCLA took several precautionary measures in the immediate aftermath of the attack. All access to Social Security numbers in the affected database has been blocked while new options for data storage are being evaluated. A security consulting firm was engaged to assist campus computer staff with forensics and in securing the systems. The database that was attacked has been completely rebuilt to afford greater security.

Over the past several years and prior to this incident, UCLA had implemented many protective policies and procedures to strengthen the security of sensitive information. These have included surveying and identifying all repositories of sensitive information on campus, removing Social Security Numbers (SSNs) from most computer screens and printed reports, prohibiting the storage of SSNs on portable devices, encrypting data flows containing sensitive information, limiting access to SSNs only to those with a compelling business need, restricting most campuswide applications to access from UC networks, and implementing firewalls and intrusion detection systems to help heighten vigilance in identifying threats. An applied security task force was formed to identify and promulgate security best practices across the campus and has instituted new policy that sets minimum standards for devices connecting to the campus network. A campus data counsel was also established to review the type of data stored. All credit card processing is in a central application that has been subjected to strict payment card industry security audit standards. As part of the systematic effort further to secure centrally managed applications, older applications that might contain undetected security weaknesses are being analyzed and rewritten as necessary.

Moving forward, UCLA launched a comprehensive review of all computer security measures on campus to accelerate its existing systematic review. It is planned to conduct regular third-party security audits of all technical environments in which sensitive data are stored, updated, or accessed. This will include periodic vulnerability testing as well as a review of security best practices. Encryption of sensitive data will be evaluated. Despite these measures, it will never be possible to guarantee absolute security. UCLA is under constant attack, with thousands of unsuccessful attempts being made daily to penetrate its security. It is imperative that IT security measures be undertaken in concert with preparations for managing a coordinated response to incidents, education of the campus community on strong security practices, and minimizing or eliminating the use of protected data.

UCLA uses its own unique identification number other than Social Security number to identify all UCLA students and employees. The campus must collect Social Security numbers as part of verifying identity and must use SSNs to coordinate with organizations outside UCLA where no other identification schema are available. For example, the federal government requires SSNs for all students applying for financial aid. They are needed to comply with the Federal Tax Relief Act, which provides tax credit for tuition payments, and SSNs are used for reporting outside UCLA such as to UCOP to compile systemwide student data and to the National Student Clearing House for verifying attendance and degrees. They are required also for reporting earnings to the California Employment Development Department and the Internal Revenue Service. Also, UCLA and UCOP collect and retain SSNs for all current and former students and staff for identity matching when assigning new University identifiers or when reactivating an identifier for a returning student or employee and to keep the employee database synchronized with the student database. Earlier in the month, UCLA convened its campus data council, which includes representatives from all areas of the campus and is charged with reviewing current practices with regard to the use of personally identifiable information. The council will make recommendations for reducing access further, improving security, and where possible eliminating all use of sensitive data and relying on the unique identifier.

Associate Vice President Hafner commented that she was working with the campuses, medical centers, and national laboratories to coordinate collective efforts with respect to information security. She reported that in 2005, at the request of President Dynes, a systemwide task force and information security workgroup were formed to determine where the University should focus its energies with respect to security. UCOP develops systemwide policy that assists the campuses in implementing their policies with respect to electronic information systems and the use of information technology. There are standard procedures and practices for incident handling, HIPAA issues, and personal credit card industry data security standards. There is a single UC website that has tools and guidelines and other resources for the campuses. Information about the breach activity is collected in order to provide information about the nature of the attacks. Web-based training tools are developed for use by the community.

Ms. Hafner affirmed that every UC entity receives thousands of network attacks a day. The nature of the attacks is changing, however; they are seeking specific kinds of vulnerabilities in networks. Higher education is vulnerable because it tends to have open institutions because of its research mission, and it has trusted relationships with other institutions nationwide and internationally. Within UC, most campuses, medical centers, and laboratories have experienced breaches of security involving personally identifying information. UC follows California security breach legislation. About one-third of the breaches have involved stolen laptops from offices, cars, and homes. About one-fifth involved hacked servers and desk tops. Some breaches come from software problems, which was the case at UCLA. There are four other UC institutions that are working with the FBI looking at attacks that appear to have patterns similar to the UCLA attack. None has uncovered any evidence that personal information was accessed. In about half of the cases where breaches occurred, the University notified individuals.

Regent Coombs asked whether any reports of identity theft resulting from the breach had been made. Mr. Morabito responded that the campus has been notified of no identity theft to date.

Faculty Representative Oakley pointed out that in dealing with sensitive data, there are best practices available from institutions that maintain a greater level of security than the University. He believed that, despite the chance of successful attacks, the University should take every available precaution to protect itself. He noted that the University has experts in cyber security in many of its departments and at the laboratories who are in a position to assist the Office of the President and the campuses.

Regent-designate Brewer asked whether mechanisms are in place to trawl systems looking for inappropriate activity. She was informed that vulnerability scanning, penetration testing, audits, and other measures have been in place and are ongoing. Despite that the records kept in the database are purged periodically, their high volume is the result of the fact that the campus receives 95,000 applications a year.

4. STATEMENT ON AUDITING STANDARDS (SAS) NO. 112 – COMMUNICATING INTERNAL CONTROLS-RELATED MATTERS IDENTIFIED IN AN AUDIT

The Committee was informed that a new audit standard issued by the American Institute of Certified Public Accountants will require The Regents' auditors to comply with new criteria when reviewing financial reporting controls surrounding the preparation of the University's 2006-07 financial statements.

Vice President Broome discussed the University's plan to prepare for implementation of this new standard. The new standard gives guidance to the auditors as to what they must report when they come across a deficiency when conducting a financial statement audit. Similar to Sarbanes-Oxley legislation, the new standard defines the three categories of control issues – "control deficiency," "significant deficiency," and "material weakness," – provides guidance on quantifying the potential financial effect of such control issues, and requires auditors to report, in writing, identified control issues to The Regents. A general control deficiency is where either the design or the operation of a control probably would not alert management to the detection of an error. A significant deficiency is a combination of one or more control deficiencies which could present more than a remote likelihood that a financial misstatement could occur. Materiality is defined as 0.2 percent but less than 1.0 percent of total expenses. A material weakness is where a significant deficiency or a combination of significant deficiencies could present more than a remote likelihood that a financial misstatement could occur. Although on a combined basis 1.0 percent of total expenses for the University would be $195 million, each location will be evaluated individually, and if there are control points they will be made by campus.

The University held a meeting of all controllers systemwide to discuss the types of deficiencies and what they would mean for the University. An action plan was developed whereby each location would meet with its PricewaterhouseCoopers team to review what they considered to be the significant control areas in their conducting of the audit. They also reviewed prior years.

After Sarbanes-Oxley took effect, approximately 15 percent of all public companies had material weaknesses that became reportable. Recently, over 60 percent of the companies were found to have significant deficiencies because of the change in the reporting standard. The standard allows for considerable judgment. In general, the bar for evaluating control deficiencies has been lowered significantly. The University will probably have some control deficiencies noted in the management letter. This will not mean that the controls of the University have deteriorated, only that there are more items reportable.

Expert Financial Advisor Vining emphasized that, although the new standard has resulted in better control measures and better documentation of them, there will still be an increased number of deficiencies reported.

5. REVIEW OF INTERNAL AUDIT PLAN FOR EXECUTIVE COMPENSATION

It was recalled that the approved 2006-07 Audit Plan included an unspecified commitment to perform audit work to be determined at a later date in the area of executive compensation. University Auditor Reed presented the plan to use the committed resources to perform followup on and validation of the University's various compensation reforms as reported to The Regents.

Mr. Reed reported that throughout the year, the Committee on Compensation had taken formal action to accept and approve the action plan for the recommendations for the Task Force on UC Accountability, Transparency, and Governance, the PricewaterhouseCoopers report, and the internal audit reports on compensation and travel expenses. He had recommended that the University's internal auditors spend the next few months validating the implementation of various reforms to give the University, the public, and the Legislature further confidence that the reforms reported are in place, functioning as designed, and effective. A report on their findings will be presented at the May meeting.

6. COMPLIANCE TOPIC: HEALTH SCIENCES COMPLIANCE PROGRAM ANNUAL REPORT

University Auditor Reed recalled that historically the health sciences report has been presented to this Committee.

Mr. Rory Jaffe, Executive Director–Medical Services and Systemwide Compliance Officer, presented the consolidated annual report of the Health Sciences Compliance Program. He reported that the healthcare compliance programs are fairly mature, having been in effect for eight years. There are seven basic requirements for a compliance program: standards of conduct and appropriate policies; a chief compliance officer and oversight committees; training programs; a complaint process such as a hotline; a system to respond to allegations of improper activities along with enforcement and discipline; auditing and monitoring to identify potential problems; and investigation and remediation of systemic issues. Each health system is organized somewhat differently, partly because their business models are different. There is central establishment of minimum standards for the activities of each institution, however, and activities are compared frequently.

Mr. Jaffe reported that he oversees the compliance activities at each campus and is the Health Insurance Portability and Accountability Act privacy and security official for the University along with his job as the medical director. All campuses with medical schools have instituted the code of conduct and are reviewing policies. There are compliance and oversight committees at each institution. The compliance officer meets regularly with the CEO of the hospital and dean of the medical school. There are extensive training programs at each institution that reach all affected employees. There is an active complaint process with respect to compliance issues. Enforcement actions include 102 instances of verbal or written warning, one demotion, four suspensions, and 2 terminations. There were another 148 corrective actions taken that did not include a personnel action. Auditing and monitoring detected and refunded billing errors totaling about $4 million last year, which represents about 0.9 percent of the net revenue of the health systems. The University is revising its monitoring standards to match advancements in the field. There have been audits and investigations on 1,300 providers in the past year and 111 hospital reviews. The vast majority were routine, done for surveillance purposes. The goal is to have every provider reviewed regularly to check billing practices.

In summary, Mr. Jaffe stated that the healthcare compliance programs are relatively mature and are doing a good job and that the University is taking steps to make them even better.

The meeting adjourned at 4:10 p.m.

Attest:

Acting Secretary