The Regents of the University of California

COMPLIANCE AND AUDIT COMMITTEE
January 24, 2018

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

Members Present: Regents Anguiano, De La Peña, Elliott, Lemus, Makarechian, Newsom, Pérez, Tauscher, Varner, and Zettel; Advisory members Anderson, Graves, and White; Chancellors Blumenthal, Gillman, and Yang; Staff Advisor Valdry

In attendance: Assistant Secretary Lyall, General Counsel Robinson, Chief Compliance and Audit Officer Bustamante, Executive Vice President and Chief Financial Officer Brostrom, Executive Vice President Stobo, and Recording Secretary Johns

The meeting convened at 10:00 a.m. with Committee Chair Zettel presiding.

1. **APPROVAL OF MINUTES OF PREVIOUS MEETING**

Upon motion duly made and seconded, the minutes of the meeting of November 15, 2017 were approved.

2. **INTERNAL AUDIT ACTIVITIES REPORT**

[Background material was provided to Regents in advance of the meeting, and a copy is on file in the Office of the Secretary and Chief of Staff.]

Systemwide Cybersecurity Audit Director Greg Loge recalled that the Cybersecurity Audit Team had been fully staffed for just over a year. The members of the Team, based at the Office of the President, were individuals with cybersecurity expertise as well as experience in the higher education and healthcare arenas. Most UC internal audit entities are based on the campuses, but in order to leverage expertise broadly and invest effectively in an area that is difficult to staff, the Team had been established as a systemwide resource. The Team's work is focused in three primary areas: to support local audit offices with cybersecurity subject matter expertise; to support systemwide cyber initiatives in an advisory role; and to provide independent audit and validation assurance functions for systemwide cyber risks. In its first year, the Team had focused on supporting campus internal audit offices and systemwide cyber initiatives. As an example, Mr. Loge highlighted systemwide vulnerability assessment and penetration test work, which served as an opportunity to identify high-risk vulnerabilities such as missing security patches and configuration errors that could result in system compromise. The work involved scanning systems for vulnerabilities, using technical software, as well as manual attempts to break into systems. When issues of concern were identified, the Team worked with management

to address the vulnerabilities identified and to identify their root causes in order to reduce the likelihood of future problems.

A number of notable themes emerged. The vulnerability management programs at many locations were of an ad hoc nature. Security teams at many campuses did not have a complete overview of all the networks at their locations. There was sometimes ambiguity regarding responsibilities, so that it took time for management to identify who was responsible for fixing a problem. There was a general lack of performance reporting for vulnerability management programs; reports should include information on the number of vulnerabilities that have persisted in an environment over time, the timeliness of patching activity, and other performance measures. Finally, the Team found that there was a lack of engagement by the cyber risk responsible executives at the locations in overall vulnerability management. Mr. Loge recalled that the cyber risk responsible executive role had been created about two years earlier for each location. He then drew attention to several improvements made by management as a result of this review. Vulnerability management programs had been expanded, and reporting of statistics for these programs had improved. The Team had worked with management to improve overall risk acceptance and relevant management processes, ensuring that the right level of executive leadership was engaged.

Mr. Loge then outlined two main activities in the current fiscal year. One was a continuation of the vulnerability assessment and penetration audit just described, but focusing this year on the health sciences locations. The second activity was an advisory services project reviewing the instant response process across all UC locations. As cyber threats become more pervasive and the sophistication of cyber attacks increases, the ability to respond quickly and effectively to incidents is critical to minimizing their impact. This project's objectives were to obtain and analyze instant response plans from each location, whose key elements should align with best practices and national standards; to determine the degree of awareness of the instant response process and ensure that the right people are engaged in the process at each location; and to determine the effectiveness of the cybersecurity incident prioritization process, the triage process for incidents.

Committee Chair Zettel asked if the University's challenge in updating its information technology systems and protecting data was primarily financial. Mr. Loge responded that the focus of this audit had not been on overall resources and staffing. Ensuring that there are sufficient staff in this area was an ongoing challenge for the UC system, as it was for other institutions and industries. Committee Chair Zettel emphasized the importance of this work in protecting UC data.

Regent-designate Anderson asked about the number of cyber-related incidents of attempted financial fraud and data breaches at UC, recalling that millions of customers' financial profiles had been accessed in a cyber attack on the Target Corporation in recent years. Mr. Loge responded that he could not provide a specific number of incidents. The University faces the same types of threats as other large organizations and like them, has an extensive and complex infrastructure. The University engages in financial transactions, processes credit cards, and faces challenges by those attempting to defraud UC, compromise its accounts, and gain access to its funds.

Mr. Anderson asked if Mr. Loge was aware of any incidents of the University wiring funds to individuals who posed as vendors and shadowed UC accounts. He stressed the need for appropriate training for employees to protect against this kind of incident. Mr. Loge responded that this was a concern for the UC system. There has been mandatory cyber awareness training for UC faculty and staff for a number of years to prevent this kind of attack and reduce this risk. Systemwide Deputy Audit Officer Matthew Hicks added that if the University becomes aware of an attack on its financial functions at a location, it notifies all the campuses, providing information on the nature of the attack and how it was perpetrated, to ensure that effective controls are in place.

The meeting adjourned at 10:15 a.m.

Attest:

Secretary and Chief of Staff