UNIVERSITY OF CALIFORNIA, ACADEMIC SENATE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

UNIVERSITY COMMITTEE ON ACADEMIC COMPUTING
AND COMMUNICATIONS (UCACC)
David Kay, Chair
kay@uci.edu

ACADEMIC SENATE
University of California
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200

February 1, 2016

TO: Dan Hare, Chair
Jim Chalfant, Vice Chair
Academic Senate

FROM: David G. Kay, Chair
University Committee on Academic Computing and Communications (UCACC)

The Academic Senate's systemwide University Committee on Academic Computing and Communications (UCACC) met in Oakland on February 1. The major issue we addressed was the university's response to a cyber-attack discovered at the UCLA Health Center in June 2015. This response included the engagement of an outside firm to provide expertise and certain monitoring tools, the formation of a systemwide Cyber-Risk Governance Committee, the institution of a cybersecurity training requirement, and other actions. Many faculty have expressed concerns about the secrecy surrounding the process, the lack of consultation with faculty, and the nature and extent of the monitoring itself.

The committee met with Tom Andriola, UC's Chief Information Officer, David Rusting, UC's Chief Information Security Officer, and Roslyn Martorano, UC's Systemwide Privacy Manager. They described in some detail the UCLA incident and the actions taken in its aftermath, and they responded to the committee's questions. They have published a web site (security.ucop.edu) with cyber-security information. They have also indicated their availability to describe and demonstrate to interested faculty the security measures at issue.

As the representatives of the faculty tasked with evaluating these actions, we are satisfied with the explanations provided and we adopt the enclosed specific findings. We find no reason to distrust these UC officials or the information they supplied. Achieving a greater degree of certainty would require an independent audit, which we are not prepared to undertake and which would still be subject to question. We believe that the most productive course of action at this juncture is twofold: (1) to acknowledge that the manner in which UC officials responded to the UCLA attack, and the degree to which these actions were kept secret, constituted a serious failure of shared governance and (2) to work with the UC Information Technology officers to institute appropriate consultation protocols to be applied going forward.

UCACC Statement on UCOP Response to June 2015 Cyber-attack at UCLA
February 1, 2016

Openness and transparency of process are hallmarks of shared governance and should be the default practice in adopting any new security measures. We find that the observance of due process in the adoption of security measures is critical.

The faculty should have been informed and consulted at the earliest stages of the process and should be involved in future decision making. Going forward we strongly encourage greater engagement with the faculty via the Academic Senate.

We endorse the UC Privacy and Information Security Initiative (ucop.edu/privacy-initiative) and encourage the adoption of all of its recommendations as a means to achieve the necessary shared governance on privacy and information security matters.

Given the information we have as of this date:

- The committee recognizes that the immediate response to the UCLA cyber attack was proportional and appropriate.
- We recognize that the essential openness of the University represents a cybersecurity challenge.
- We recognize that coordinated monitoring of traffic patterns across UC campus networks can reveal multi-campus security attacks.
- We understand why an outside firm with the needed expertise was engaged to deal with the urgent UCLA threat and its aftermath in a coordinated manner across the system.
- We have been informed that the monitoring of communications looked only for “malware signatures” and Internet traffic patterns. As neither message content nor browsing activity were monitored, we believe this level of monitoring can be appropriate.
- We have been informed that monitoring of transmissions occurs only at campus edge, and does not capture internal campus traffic. Monitoring of traffic patterns for a pre-defined purpose can be appropriate given that results are maintained for a limited time and limited use.