UNIVERSITY COMMITTEE
ON
ACADEMIC COMPUTING AND COMMUNICATIONS

ANNUAL REPORT 2022-2023

TO THE ASSEMBLY OF THE ACADEMIC SENATE:
The University Committee on Academic Computing and Communications (UCACC) is charged in Senate Bylaw 155 to represent the Senate in all matters involving the uses and impact of computing and communications technology and advise the President concerning the acquisition, usage and support of computing and communications technology and related policy issues. UCACC met four times during the academic year. Three meetings were conducted via videoconference and one was held in-person in Oakland (with the option to join remotely). This report highlights the committee's activities in 2022-23.

This year, UCACC topics included changes made at UCOP since the Accellion data breach, the outcomes of a systemwide IT assessment, research data security, software procurement, federal government security requirement changes, and ongoing issues with the financial accounting system that was deployed at UC San Diego and UC Merced.

Cybersecurity Changes at UCOP

In December, UCACC welcomed UCOP Chief Information Officer Molly Greek and UCOP Chief Information Security Officer April Sather to discuss IT changes made at UCOP in the aftermath of the Accellion security breach that came to light in 2021. One of the first actions was the hiring of April Sather as UCOP CISO. Greek shared with UCACC a summary of the changes that were implemented and noted that UC Executive Vice President and Chief Operating Officer Rachael Nava oversees UC's Information Technology Services. COO Nava is responsible for approving all higher-level (P3 and P4) security exceptions to the IS-3 policy. The UC President gets involved when needed.

UCACC and UCOP administrators discussed the role of IT staff and the benefit of having a diverse workforce in understanding users. Approximately 40% of the UC IT staff are women. UC's Information Technology Services unit is in a pilot program with the Office of Workplace Inclusion and Belonging at UCOP.

Systemwide IT Assessment and Outcomes

Last year, UCOP engaged the consulting firm bakertilly to conduct a review of its data security program. The project included surveys and interviews, including with UCACC members. The final report from the consultants yielded four focus areas: strategy and governance, structure and roles, practices and technology, and talent and resources, along with recommendations for changes in each area. Several changes are in the process of being implemented (see below) and UCACC will continue to monitor and consult with the UC CIO as the changes progress.

Cyber-Risk Governance Committee (CRGC)

Several IT assessments conducted over the last year commented on the configuration of the Cyber-Risk Governance Committee (CRGC), which was formed under UC President Janet Napolitano, and the unusual role of the Cyber-risk Responsible Executive (CRE) from each

location, which comprise the membership. CRE is a unique designation, meant to identify a single campus person who is responsible for sharing information systemwide. The charge of the CRGC is to monitor UC's risk profile, oversee IT investments, coordinate cybersecurity efforts across the system, and facilitate information sharing about cybersecurity best practices.

In the spring, CIO Van Williams updated UCACC on the changes that were being proposed for UC's Cybersecurity Governance, including the CRGC. Based on a "RACI" matrix, which documents who is responsible, accountable, consulted, and informed, the new model recommends that CIOs and CISOs have primary *responsibility* for cybersecurity on their campuses, while chancellors are ultimately *accountable.* The roles will be formalized, with clearly defined recommendations for consultation and reporting.

Digital Risk Tolerance and UC Policy

A recent cybersecurity assessment suggested that UC create a "digital risk tolerance statement" to delineate the risks, rewards, and tradeoffs, and make it clear that UC assumes reasonable risks that are inherent in a university environment. The statement will function as an overarching document with multiple iterations and associated materials; campuses/units can create their own statements that meet the minimum requirements but are tailored to specific needs.

UC will be revising its IS-3 (Information Security policy soon, with input from UCACC. In a preliminary discussion, UCACC members questioned the combining of operational security and research security needs into a single policy and suggested that the policy should refrain from using terms like "business need" and "business unit." "Operational unit" or "academic unit" are more appropriate terms for an educational environment – possibly divided into research and teaching. The IS-3 policy is informed by UC Legal and IT experts, as well as compliance requirements from the federal government. It is meant to provide a minimum-security standard, with the understanding that risk decisions are made operationally every day.

Cybersecurity Metrics

Cybersecurity metrics were developed by the campus CISOs over the past year or so and presented to the Board of Regents at its April meeting. UC's security goal is to make sure that the most critical areas have appropriate control levels, not to protect everything against every possible threat. Examples of metrics include training, application of multi-factor authentication, end-point security implementation, and incident reporting. Considerations of cyber-insurance were among the motivating factors in developing the metrics, which will be extended and shared with the chancellors and eventually the public. CIO Van Williams pointed out that the metrics also responded to UCACC's calls over the past few years for increased information sharing and transparency around data governance at UC. Williams would like data security to be discussed regularly within local CITs and more broadly on the campuses. He noted that metrics are one way to acknowledge achievements and convey successes.

Systemwide IT procurement

IT Strategic Sourcing Associate Director Tom Trappler joined UCACC's October meeting to talk about UC IT Strategic Sourcing, which coordinates systemwide licensing of software used for administrative as well as pedagogical and research purposes. The systemwide contracts allow individual campuses, schools, departments, and smaller units to take advantage of pre-negotiated terms. An IT Sourcing Committee (ITSC) reviews new projects while the UC Strategic Sourcing

team oversees the contracts. UCSF representative Jenson Wong served as this year's UCACC liaison to the ITSC.

Regarding the Oracle financial system, Trappler said that UC Merced joined UC San Diego's contract and that decisions about those licenses were not made by the IT Strategic Sourcing team.

Research Data Backup System

In February, UCOP Strategic Advisor Anne Bessman joined UCACC to provide an update on the work of the Research Data Backup System (RDBS) Steering Committee. The committee conducted a review of the current data backup system landscape and prepared an RFP. The scope of the research data that would be included in such a UC system spans everything from data stored on individual computers to large scale server clusters, potentially necessitating two separate solutions. The Steering Committee proposed that the ongoing costs be incorporated into campus assessments due to the imperative of a systemwide solution. UCACC members noted potential challenges of user uptake and the often complicated details of data ownership at UC. The committee encouraged the RDBS Steering Committee to work closely with the California Digital Library (CDL) to coordinate research data management and stewardship efforts across the university.

Federal Government Requirements and Policy Changes

UC IT Policy Manager Robert Smith provided an overview of national cybersecurity trends and changes to policy that will be coming from the federal government. Congress and the national intelligence agencies are increasingly concerned about cybersecurity and the prevention of malicious foreign influence and security breaches. The changes will result in an increase in requirements for cybersecurity protections from federal funders, although to many faculty it will look like a directive for administrative controls on academic computing. Nevertheless, federal grant recipients will be obligated to comply with all regulations. UC receives hundreds of millions of dollars from the Department of Defense annually. Some grant recipients will have to follow the new Cybersecurity Maturity Model Certification (CMMC), which expands current controls and may require third-party certification. The framework for third party certification is underway.

ADDITIONAL BUSINESS

Campus IT Governance Structure: UCACC updated the Campus IT Governance Structures chart (shared via Google docs) that tracks faculty involvement in campus IT governance.

Financial accounting system issues: UCACC continued to hear about problems with the Oracle financial software at UC Merced and UC San Diego. The problems with the system have led to delinquent accounts, inaccurate grant fund balances, and financial losses to researchers and the university.

Inclusive Workplace Culture Megastudy: UCACC was briefed about a new study involving the collection of staff email metadata at some campuses. The purpose of the study is to learn whether specified interventions improve feelings of connection with colleagues. Although the project does not involve electronic communications of faculty, the study was brought to the attention of UCACC due to potential interest by faculty in the application of the UC Electronic Communications Policy (ECP). Campus privacy officers analyzed the protocols and determined

that it is low risk given that the content of communications will not be accessed or examined and an opt out option will be provided.

Lecture-Capture and Shifting Modes of Teaching: UCACC members spent some time throughout the year discussing issues around teaching modality and the recording of course lectures. Since the pandemic, students increasingly expect that courses will be recorded and made available. Although it is an issue of ADA accommodation for some, that is not widely the case. UCACC members talked about the various ways that campuses are coping with the demands, and whether remote class participation is in the student's best educational interest. Systemwide guidelines would be appreciated.

Systemwide and campus updates*:* UCACC devoted part of each regular meeting to discussing systemwide issues as reported by Academic Senate leadership and reports from campus representatives on individual campus activities and concerns.

SYSTEMWIDE REVIEWS AND CORRESPONDENCE

- Oracle Financial System Implementation (April 27, 2023)
- Proposed Presidential Policy on Inventions, Patents, and Innovation Transfer (April 28, 2023)

REPRESENTATION

UCACC Chair Matt Bishop, served as a faculty representative to the Information Technology Leadership Council (ITLC) and as an *ex officio* member of the University Committee on Library and Scholarly Communications (UCOLASC). Chair Bishop served as Senate representative to the Cyber-Risk Governance Committee (CRGC) and the newly constituted UC Presidential Working Group on Artificial Intelligence Standing Council.

UC Davis representative Jenson Wong served as liaison to the systemwide IT Sourcing Committee.

ACKNOWLEDGEMENTS

UCACC is grateful for the contributions made by the consultants and guests who attended meetings in 2022-23, including:

- Anne Bessman, Strategic Advisor, UCOP
- Jennifer Chatman, Co-PI of the "Inclusive Workplace Culture Megastudy" and Professor at Haas School of Business, UC Berkeley
- Molly Greek, UCOP Chief Information Officer
- Jayesh (Jay) Panchal, UC Chief Information Security Officer
- Monte Ratzlaff, Cyber-Risk Program Manager, UCOP
- April Sather, UCOP Chief Information Security Officer
- Robert Smith, IT Policy Director, UCOP
- Hoyt Sze, Managing Council, UC Legal
- Thomas Trappler Associate Director, IT Strategic Sourcing, UC Procurement Services
- Van Williams, Chief Information Officer and Vice President for Information Technology Services

RESPECTFULLY SUBMITTED,

Matthew Bishop, Chair (UC Davis)
Avi Yagil, Vice Chair (UC San Diego)
John Kubiatowicz (UC Berkeley)
Kya Thaw Paw U (UC Davis)
Kevin Thornton (UC Irvine)
Christine Borgman (UCLA)
Emily Jane McTavish (UC Merced)
Sheldon Tan (UC Riverside)
George Porter (UC San Diego)
Jenson Wong (UC San Francisco)
Frank Brown (UC Santa Barbara)
Peter Alvaro (UC Santa Cruz)
Susan Cochran, Chair, Academic Senate *(Ex Officio)*
James Steintrager, Vice Chair, Academic Senate *(Ex Officio)*
Dean Tantillo, CCGA Vice Chair *(Ex Officio)*
John Hildebrand, UCOLASC Chair *(Ex Officio)*
Joanne Miller, Committee Analyst