UNIVERSITY OF CALIFORNIA **ACADEMIC SENATE**

UNIVERSITY COMMITTEE ON ACADEMIC COMPUTING AND COMMUNICATIONS

Thursday, December 12, 2019

Meeting Minutes

I. Chair's Announcements, Agenda Review

Chair Anthony Joseph began the meeting with updates on items relevant to the agenda:

- The implementation of the new IS-3 policy is shifting some IT responsibility from IT administrators to faculty or "Unit Heads" and may be starting to cause concern. Unit Heads are determined at the campus or school level, and could be a high-level administrator or a PI, depending on the situation. In terms of security, some of the controls are already in place at UC's medical center locations. The call for tracking and inventorying will be new to other locations. Campus IT administrators should be communicating about this widely.
- UCACC will be asked to review the revised IS-12 policy requirements in January.
- Cybersecurity audit personnel are visiting all campuses and trying to include faculty in each briefing. UCSB faculty had had concerns based on the information provided earlier in the year, but the audit scope letter and visit has allayed most fears. The audit is primarily looking at configuration and whether the system is functioning as intended.

Action: The October 22, 2019, meeting minutes were approved.

II. UC IT Services Updates

Mark Cianca, Interim Chief Information Officer
David Rusting, Chief Information Security Officer
Robert Smith, Systemwide IT Policy Director (via Zoom)

Systemwide Electronic Information Security Policy (IS-3) update on rollout progress

In response to a request from UCLA to revise one of the nine approved standards, an "Event Logging Standard" workgroup will convene in January. A UCACC member is invited to join the group.

IS-12 update

IS-12 will be a Presidential policy on "IT Disaster Recovery and Service Continuity" going forward (summarized as "IT Recovery"). Based on the Gartner model, the locations will decide which business functions and units fall within the scope of the policy. It will use a risk-based approach with tiered recovery levels (1=low, 5=high). The location's designated Cyber-risk Responsible Executive (CRE) will be the senior person responsible for key elements and exceptions. CREs were first established by Presidential directive when the Cyber-Risk Governance Committee was established, and are now enshrined in IS-3. The policy will continue using Units & Unit Heads as key points of accountability. The Unit Head would almost never be an individual faculty member, except in the case of a PI for a big research project.

The policy requirements will be ready for review in February, with a larger "management" review of the draft policy in the spring. The comprehensive systemwide review will take place in fall, 2020, for an anticipated effective date of July 1, 2021.

UCACC members asked about education and outreach. There is always a need for better communication, but this is generally left to the locations to determine. Faculty would appreciate workshops or training to inform faculty about any new responsibilities. One UCACC member mentioned mandatory online training, like UC requires in other areas, but others felt there would be opposition to more training.

Members also asked whether some of the responsibility could be outsourced, such as in the instance of a department head with no technological knowledge. There will be FAQs for faculty that could be drafted at the systemwide level and then customized at the campuses. It was suggested that personas or use cases be used to develop education and outreach materials. CISOs, Export Control Officers, Information Technology Leadership Council, and other groups that meet regularly can share best practices. Contracts & Grants Offices and related websites would be good places to share important data with faculty about, for example, data management plan resources (e.g., https://dmptool.org/).

CCPA – California Consumer Privacy Act

The California Consumer Privacy Act is a consumer-rights bill that was signed into law on June 28, 2018, and goes into effect in January 2020. The law applies to businesses, and gives the public the right to know what personal information is collected and the right to control how personal information is used. It includes requirements for de-identification, security, and administrator controls. The biggest impact for UC will be in public-private partnerships and at the health centers. The UC Office of General Council and Research Offices are working on developing guidance, but UC employees should be aware of contractual agreements that include a provision for CCPA compliance.

CRGC update

Each Cyber-Risk Governance Committee meeting includes a general update about cybersecurity at the university and in general. CRGC learned that a large company that provides services to academic community had a data breach over a year ago and recently found that student information was being sold and used. There are 80,000 potentially compromised accounts. Information on this and other breaches is regularly provided to CREs and CISOs.

UCACC members discussed the need for responsible password management and how to convey that to students (and others in UC community). Password management apps are the safest method and widely available, but risks need to be taken seriously. Multi-factor authentication is part of the administration's efforts to ensure greater protection. UCACC members wanted to know if it was possible for UC to obtain a site license for a password management app, or at least to recommend software.

III. UCOP Office of Ethics, Compliance and Audit Service (ECAS)

Alexander Bustamante, Senior Vice President and Chief Compliance Officer
Shanda Hunt, Research Compliance Manager
Greg Loge, Systemwide Cybersecurity Audit Director (via Zoom)

Update on cybersecurity audits

The threat detection and identification (TDI) audit is looking at implementation of FireEye across the system. Cybersecurity Audit Director Greg Loge reminded the committee that UC began its TDI implementation after the UCLA breach in 2016 as an incident response and protection, to manage risk. The audit attempts to review how well the implementation has worked, and whether there are practices to be shared. The review will also look at total cost and return on investment. Loge is visiting each campus and meeting with CIOs and CISOs, and he reports that the in-person contact has been positive. Part of the work at the locations is scoping for “Phase 2” of the FireEye implementation which will be determined by end of January. Deloitte is providing additional personnel and expertise to UC for the evaluation. The volume and nature of threats apprehended are included in the data points be used to evaluate the systems. The audit will also look at additional local systems in place, and assess the value of having a systemwide approach. FireEye is very expensive, and some stakeholders are interested in whether open source software could be less costly.

UCACC members suggested that messages to the broader UC community about the audit should state that the audit is part of the oversight and review process, and might also assure faculty that FireEye data has never been used in disciplinary actions and is not intended to be used in that way. Other concerns from the faculty include whether the costs will eventually be shifted to campuses, and the appropriate allocation of resources between FireEye and other security and IT needs.

Machine learning and artificial intelligence

SVP Bustamante returned to UCACC to update the committee and get additional input regarding machine learning and artificial intelligence from a compliance and ethics perspective. Since the last meeting, Bustamante has met with professors at UCB and researchers at CITRIS to learn about concerns. Interested stakeholders include data scientists, legal scholars, ethicists, and others. Once again, Bustamante would appreciate referrals to knowledgeable people in the UC community.

The purpose for the information-gathering is initially just to have discussions and identify important areas, with a potential plan for the issuance of guidance and/or a planning process from the university at the systemwide level. There are compliance officers on the campuses, who will also work on the issues, but possibly from a more regulatory perspective.

UCACC members and Bustamante discussed the scope of the inquiry, and what is different now from 20-30 years ago. Data sets are larger (in many areas), more inference is available, and legislators are paying attention. UC would like to get out in front of any wave of legislation or imposition of laws and to lead the way. It was noted that the underlying issues are not necessarily specific to AI, but AI is bringing them to the forefront. There was a suggestion to provide examples or case studies for potential situations. UCACC members mentioned the related topic of research information management systems (RIMS) and the newly-formed UC RIMS Working Group that will investigate how data is being used.

IV. Member/campus issues

UC Davis: Privacy of faculty communication (email) has been a concern at UC Davis since before the FireEye implementation was announced. Lately, the committee participated in the review of the revised copyright ownership policy, and discussed questions around privacy and FireEye data. The local committee drafted principles that the CIO and CISO reviewed and will be voted on for endorsement at the Executive Council. Due to publicity about the breach of student information (mentioned by the ITS guests earlier in the meeting), the use of Duo and multifactor authentication has become more accepted. While UC Davis is having email compatibility problems with Duo, other campuses have integrated it successfully. It was suggested that the campus CISOs share information. Another issue was that the local committee felt that employees should not have to pay for the tokens (that may be used in place of a cell phone app). In practice, other campuses have found that the tokens were inexpensive to purchase in bulk, and they ended up needing fewer than anticipated.

UCSD: UCSD's local committee has discussed Research Information Management Systems and the formation of the new RIMS Working Group, which is co-chaired by UCSC Professor Maryann Martone. Adobe licenses are a big concern, and organization of instructional computing resources. The local committee wanted know if there was a system-level solution to help bring costs down. The "Blink" central campus system is supposed to be an organized resource for information, but it contains contradictory and outdated information and can be difficult to navigate.

Berkeley: Printing has turned into a big deal at the Berkeley campus. There is interest in reorganizing the IT governance structure and looking the impact on instructors and researchers in supporting the new Data Science Division. Specific computing topics include network segmentation, and privacy issues around servers with sensitive administrative data that are now behind a firewall.

UCSF: The local committee is discussing the UC Electronic Communications Policy, which was last updated in 2005. UCACC is interested in inviting someone from the administration to a meeting to talk about the policy. At UCSF there is interest in harvesting caregiver to caregiver communications for research purposes, which raises many issues.

UCLA: Rollout of administrative programs is causing concern. One is a giant database of student and possibly faculty information. Another is campus-wide video monitoring. Issues include privacy, cost, and contracts with for-profit vendors, in addition to energy use to maintain so much data. UCACC will add this to the February agenda.

UCSC: UC Santa Cruz has had a new Chief Information Officer for about a year and is undergoing a restructuring of IT services (centralization or distributed organization). The local committee is an advisory committee only, but will provide input on the restructuring plan. The campus is almost finished with MFA rollout. The 2018 faculty IT satisfaction survey was shared with the new CIO to inform his planning efforts. UCACC would like to review the survey, and any lessons learned or outcomes that could be shared.

V. UC Health Data Update

Cora Han, Chief Health Data Officer

UC's new Chief Health Data Officer joined the meeting to talk about the Center for Data-driven Insights and Innovation (CDI2) and systemwide health data governance projects. Han started on August 1st after years of consumer protection work at the FTC.

The UC Health Data Warehouse is intended to support partnerships across the system. The goal is to harness the benefits of health care data analytics while mitigating risks. Central responsibility for security for the UCHDW is with UCOP's Cyber-risk Program Manager, Monte Raztlaff, who works with the location CISOs to develop risk mitigation strategies and ensure that cybersecurity requirements are met. The Chief Data Scientist for the University of California Health System (18 health professional schools, 6 medical centers, 10 hospitals, and over 1000 sites of care delivery) is Atul Butte from UCSF.

The UC health data center is one outcome of the President’s Ad Hoc Task Force on Health Data Governance, which completed its work in January, 2018. The report’s three foundational recommendations were for UC to:

1. Pioneer a patient-informed, justice-based model of Health Data use, and demonstrate the need for and benefits of more active data use.
2. Establish a System-level Health Data Office to identify and accelerate projects and partnerships to realize the public benefits of collaborations to analyze Health Data.
3. Develop criteria and a process for evaluating projects and transactions involving access to UC Health Data by outside parties.

UCACC members had questions about the data stored in the warehouse and who would have access. Security of the data warehouse is taken very seriously, and there has been penetration testing and an overall risk assessment by outside experts. Security assessments will be ongoing. Other questions were around data de-identification, inclusion of clinician notes (not included), validation, and encoding. Members wanted to know about documentation, whether and how the data was being made available to UC researchers, and how researchers could get more information.

A comprehensive infrastructure for researcher access is not set up. There is a small data science team led by UC Health Data Warehouse Director Lisa Dahm from UC Irvine that is focusing on partnering, training, and tracking. Once the processes are up and running access will be available more widely, potentially including researchers at locations that do not have medical centers. UCACC members offered suggestions for fostering partnerships, training, and the use of data domain experts.

VI. IT strategic sourcing

Thomas Trappler Associate Director, IT Strategic Sourcing, UC Procurement Services

Associate Director for IT Strategic Sourcing Thomas Trappler joined the meeting to talk about systemwide IT procurement. The UC IT Strategic Sourcing Center of Excellence website (https://www.ucop.edu/procurement-services/for-ucstaff/it-strategic-sourcing/) includes a link to systemwide IT agreements for goods and services. The goals for the center are reducing cost and risk and improving services. The 65 systemwide agreements include Zoom, grade scope, AWS, and more. While the systemwide IT strategic sourcing team comprises only four people, they staff partners with all of the locations via an ITLC Sourcing Subcommittee that has representatives from each location. Suggestions for purchases come in on a standardized form that includes rationale. Trappler would like to get more faculty input, possibly as part of an evaluation team that is formed to assess each proposed purchase.

UCACC members were interested in small-scale purchases/licenses, how to address the needs of individual researchers and groups, and issues around open source options. UCACC members asked about developing more creative solutions and the need for a comprehensive UC IT strategy. With only four staff people, the unit focuses on the highest priority needs. They just completed an audio/visual project, and are now turning to telecommunications.

Trappler will return to UCACC meetings for consultation and faculty input.

VII. Faculty IT Satisfaction Survey

Members discussed the possibility of a faculty survey – like the one conducted at UC Santa Cruz – to assess satisfaction with IT services. Aside from illustrating dissatisfaction, it is not clear exactly what purpose a survey would serve. Each campus could use it to find out exactly where the needs are. Four areas were mentioned: instruction, research, business applications, and clinical. Logistically, any survey would have to be conducted and assessed at the local level, but UCACC members expressed interest in using the results to determine a systemwide minimum standard for faculty IT support. Other systemwide committees, such as Faculty Welfare and Research Policy, might be interested in such a survey as well.

Action: Determine if UCFW and UCORP are interested in a faculty IT satisfaction survey.

VIII. Executive Session

No minutes were taken during executive session.

Meeting adjourned: 3:50
Meeting minute drafted by: Joanne Miller, UCACC Committee Analyst
Attest: Anthony Joseph, UCACC Chair

Meeting participants:
Members: Anthony Joseph (Chair), David Robinowitz (Vice Chair), Ethan Ligon (Berkeley), Matt Bishop (Davis, via video), Feng Liu (Irvine, via video), Susan Cochran (Los Angeles, via video), Michael Spivey (Merced, via video), Weifeng Gu (Riverside, via video), Brett Stalbaum (San Diego alternate, via video), Lisa Jevbratt (Santa Barbara, via video), Hamid Sadjadpour (Santa Cruz, via video), Dennis Ventry (UCOLASC Chair, via video),

Consultants and guests: Mark Cianca (Interim Chief Information Officer), David Rusting (Chief Information Security Officer), Robert Smith (Systemwide IT Policy Director, via Zoom), Alexander Bustamante (Chief Compliance Officer), Shanda Hunt (Research Compliance Manager), Greg Loge (Systemwide Cybersecurity Audit Director), Cora Han (Chief Health Data Officer), Thomas Trappler (Associate Director, IT Strategic Sourcing), Joanne Miller (Committee Analyst)