COMMITTEE ON ACADEMIC FREEDOM
Annual Report, 2016 – 17

To: Academic Senate, Santa Cruz Division

The Committee on Academic Freedom (CAF) met quarterly, as issues arose for discussion and review. This year the committee reviewed policy changes locally and systemwide as well as following up on the implementation of a threat detection software system, FireEye. A summary of committee business follows.

Committee Issues

One topic of discussion at the University Committee on Academic Freedom (UCAF) meetings concerned the Anti-Semitism Awareness Act, which was approved by the U.S. Senate in December 2016, but has not yet been approved by the House. This Act directs the Department of Education to use the U.S. State Department definition of "Anti-Semitism" in the *Special Envoy to Monitor and Combat Anti-Semitism of the Department of State*[1] when investigating and responding to alleged violations of Title VI of the Civil Rights Act of 1964 at educational institutions that receive federal funding. UCAF, working with UC campus representatives drafted a statement on the Act to be endorsed by the Academic Council at their June 2017 meeting. The draft was discussed by the UCSC CAF with comments being provided to UCAF.

CAF received a faculty request to endorse a statement of principles based on a document created by Middlebury University faculty following an incident with disruption of a controversial speaker and some minor violence after the event. CAF did not proceed with this, as the topic is wrapped up with the difficult situation at UCB and UCD concerning advance cancellation of controversial speaker events in the wake of violent protests that appear to have included non-UC personnel. Public safety issues are in tension with the desire to protect freedom of speech and to ensure broad intellectual discourse on the campus, and UC does need to find a better way of handling this complex issue. That may be an agenda item for next year's CAF (UCAF similarly opted not to endorse the specific Middlebury faculty statement, but provided input to the UC President, reviewed and commented on by UCSC CAF) outlining guiding principles.

An inquiry was made to CAF regarding the degree to which academic freedom protections in the Academic Personnel Manual (APM) apply to academic titles held by campus librarians. The union contract with the librarians does not specify specific portions of the APM concerning academic freedom the way they are called out in the union contract for lecturers, so it is not evident that the academic title for librarians provides general APM academic freedom protections. No action was taken on this topic, as it appears to be an issue of the contract with the union for the librarians and there is not a self-evident intrinsic linkage to the faculty academic freedom protections.

FireEye Implementation Progress at UCSC

The Office of the President rapidly, and with little/no Senate consultation, initiated a contract with Fidelis for monitoring cyberattacks on UC Campus network systems two years ago, following a breach of patient information at the UCLA Medical School. This was in response

[1] The *Special Envoy to Monitor and Combat Anti-Semitism of the Department of State* can be found here - https://www.state.gov/s/rga/resources/267538.htm

to a Federal mandate to protect confidential patient information in the UC Medical schools. UC has now developed a new contract with FireEye, a more capable, and potentially more intrusive threat detection system with a wide range of implementation levels. CAF consulted during the year with Janine Roeth, Information Technology Services (ITS) Director Client Service and Security, ITS infrastructure technician Bryon Walker who oversees the FireEye "black box" (which monitors and temporarily holds all unencrypted web traffic data) on campus as well as with FireEye personnel. The outcome of these consultations was positive for both the committee members and ITS staff. The mandated campus implementation of FireEye is not complete, but with input from CAF and other Senate committees, the lowest level of peripheral threat detection implementation of FireEye has been selected for UCSC as the campus does not have the issue of protecting medical school patient files. The appliances (data disks with web traffic) reside here on campus; data transmitted on campus is not monitored; only unencrypted data packets entering the border of our network system are stored, and this is only for a 24 hour period. The unencrypted metadata are continuously processed by the FireEye threat detection system, with threat alerts issued if the system identifies traffic from malicious domains or malware. FireEye may then issue a request to UCSC IT to gain access to the ephemeral database of full packet information for the purpose of evaluating the scope of the attack and applying learning algorithms to improve the detection system in the face of every-varying attack strategies. ITS reviews any requests for access to the full packet information by FireEye when a threat is detected and chooses whether to provide approval for access to the stored data. There are roughly 20 to 30 malware cases a month at UCSC and the black box default storage is about 10 days worth (about 2 terabytes a day) of data, so 1 day storage is a minimal level of full packet data availability, but is deemed sufficient for threat evaluation and learning of the monitoring system. ITS staff will log FireEye requests for data access and campus approvals for reporting purposes; only ITS Staff have direct access to the UCSC servers housing the full packet information. These data reports will provide some level of transparency and future Senate oversight. CAF and the Committee on Information Technology (CIT) plan to send out a memo during Fall quarter 2017 to inform faculty of the FireEye implementation and to recommend following best practices outlined on the ITS Security page.[2]

Policy Issues Under Review

Learning Data Principles

Senate committees were requested to review the draft principles and practices created by the Ed Tech Leadership Committee (ETLC) surrounding data privacy for students and faculty with regard to data analytics generated by service providers such as Canvas, Sakai, and Piazza for the UC system. Members reviewed this policy and were supportive of establishing principles around privacy and transparency but were concerned that the principle of freedom of expression not be compromised by metadata collection efforts. In light of this concern – and of the principle stated in the draft "Learning Data Privacy Principles and Recommended Practices" that UC faculty and students retain "ownership" of the data, and "ultimate authority of control" the Committee recommended creating a policy of a) documentation of any and all circumstances under which UC learning data could be accessed by or transferred to some other entity, without the express approval of UC faculty and students, and b) an indication of what the university's response will be to attempts at or requests for such access or transfer. Members found the failure of an acceptable agreement between UC and Piazza troubling with regard to the use and protection of data in its system. The Committee agreed that University policy on

[2] The ITS Security page may be viewed at https://its.ucsc.edu/security/stay-secure.html

learning data should consider specifically prohibiting faculty from requiring students in a given course to use learning applications that involve the transfer of learning data to outside vendors or other entities, unless students are given the option to "opt in" or "opt out" of any arrangement that would allow the data to be transferred to and/or used by that outside vendor or entity. Faculty and students should be informed of potential data mining of personal information when signing up to access these websites.

Systemwide Review Draft Presidential Unmanned Aircraft System Policy
CAF commented on a new proposed policy for Unmanned Aircraft Systems (UAS). The policy is to establish minimum standards for the safe use and operation of UAS and Small Unmanned Aircraft Systems (SUAS), including drones and model aircraft, on any University location or at any "Authorized University Activity". This policy requires that all UAS operations are performed in a manner that mitigates risks to safety, security, and privacy, and ensures compliance with the Federal Aviation Administration (FAA) Modernization and Reform Act of 2012 (Public Law 112-95) and all applicable laws.

The Committee had no argument with ensuring compliance with State and Federal laws for safe UAS operation and for reducing risk to liability. However, we share the concern raised by the Committees on Information Technology (CIT) and Research (COR) that the campus authorization process may become excessively burdensome on faculty and researchers, inhibiting their utilization of UAS technologies in research and instruction. The committee recommended clarifying and simplifying the authorization process required of researchers to deal with the practical issues of multiple flights, adjusted flight paths, and other realities of UAS deployments for research applications.

Systemwide Review of Draft Electronic Information Security Policy
The Committee reviewed the Office of the President's draft Electronic Information Security Policy Manual and found the policy to be difficult to evaluate with regard to what is new and what changes were made to earlier IT security guidelines. This draft policy appears to be a combination of past policies, it would have been helpful for review if a red-line version had been provided noting all changes and additions. Members found it difficult to detect specific situations in which the security policies may impact academic freedom issues, so the overall policy manual was not troubling to CAF members.

Systemwide Review of Proposed Revised Academic Personnel Manual (APM) - 285, 210-3, 133, and 740
The Academic Affairs/Academic Personnel Vice Provost Lecturers with Security of Employment (LSOE) Subcommittee identified major areas requiring policy revision for the current LSOE faculty title series clarifying their roles for teaching, scholarly activity and service. CAF reviewed proposed revisions to Academic Personnel Manual (APM) - 285, 210-3, 133, and 740, and found the overall change of the Lecturer with Security of Employment series to the Teaching Professor series largely unproblematic, although vagueness remains with respect to the proportion of "Professional and Scholarly achievement and activity" expected for appointment and promotion in the Teaching Professor Series. While the description of Professional and Scholarly Achievement and Activity is significantly elaborated, there remains some concern that the vagueness of expectations offers potential for confusion. After review CAF did not see any other issues of concern for academic freedom.

CAF's recommendation for next year's committee:

- Follow up on campus final implementation of FireEye and monitoring of frequency of allocation of access to full packet information in response to threat detections.
- Monitor implementation of the UC Regents policy on intolerance and possible entry into law of the Anti-Semitism Awareness Act.
- Review academic freedom issues concerning contracted staff with academic titles.

Respectfully submitted;
COMMITTEE ON ACADEMIC FREEDOM
Gopal Balakrishnan
Eva Bertram
Darrell Long (W, S)
Tanya Merchant
Thorne Lay, Chair
Brittany Young (F), Graduate Representative

August 11, 2017