UNIVERSITY OF CALIFORNIA, ACADEMIC SENATE

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

James Steintrager
Telephone:(510) 987-9983
Email: james.steintrager@ucop.edu

Chair of the Assembly of the Academic Senate
Faculty Representative to the Regents
University of California
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200

June 6, 2024

MICHAEL V. DRAKE, PRESIDENT
UNIVERSITY OF CALIFORNIA

Re: Information Security Investment Plans

Dear President Drake,

At its May 22, 2024 meeting, the Academic Council endorsed the attached letter from the University Committee on Academic Computing and Communications (UCACC). The letter responds to your February 26, 2024 communication to campus chancellors requesting an updated information security investment plan. Council joins UCACC in acknowledging the importance of robust cybersecurity policies that balance security measures with research and educational activities. We also would like to highlight several concerns about the plan:

- UCACC notes the lack of faculty input into the standards, timelines, and non-compliance consequences outlined in the letter, and stresses the importance of faculty consultation in cybersecurity measures.
- The plan proposes a corporate-style cybersecurity model that appears unsuitable for UC due to logistical issues and cost. UCACC emphasizes the challenges of implementing these requirements in a distributed environment where the majority of faculty own their own devices.
- New email restrictions proposed by campuses in response to the letter will disrupt workflows and productivity for some faculty. Additionally, new mandates for Endpoint Detection and Response (EDR) and tracking software could affect academic freedom, personal privacy, and computer performance. Clear definitions of devices subject to EDR are needed. UCACC also questions the effectiveness of EDR, multifactor authentication, and cybersecurity training in preventing cyberattacks, given the prevalence of social engineering and vendor software vulnerabilities.
- The letter treats university networks monolithically. UCACC recommends distinguishing between public and trusted networks, with different cybersecurity measures respectively.
- Many faculty rely on legacy systems that may not be able to come into compliance with the new standards. UCACC calls for exceptions for these systems.
- The proposed consequence of withholding merit increases for leaders of non-compliant units – which includes faculty – could discourage faculty from seeking extramural funding or from serving as department chairs.

- The implications for high-performance computing systems and research-information technology (IT) infrastructure are unclear. Research-IT and other IT professionals on the campuses should be included in any implementation plans.
- Plan implementation will increase IT workloads and require additional funding. UCACC is concerned about the lack of clear funding sources and about budget impacts on local priorities.

The Academic Council requests the following:

- Meaningful consultation with faculty and research-IT personnel on all significant cybersecurity measures and policy discussions, particularly when they involve restrictions affecting faculty.
- Clear definitions and guidelines for devices subject to any required cybersecurity measures.
- Consideration of the implications of new restrictions on email and other digital communication tools.
- An effort to address funding and workload issues related to implementation of cybersecurity measures.

We look forward to working with you to increase shared governance in this area. Please do not hesitate to contact me if you have additional questions.

Sincerely,

James Steintrager, Chair
Academic Council

Cc: Academic Council
Executive Vice President & Chief Operating Officer Nava
Vice President & Chief Information Officer Williams
Vice President and Chief of Staff Kao
Chief Risk Officer Confetti
Interim Chief Information Security Officer Ratzlaff
Chief Policy Advisor McAuliffe
Senate Division Executive Directors
Senate Executive Director Lin

UNIVERSITY COMMITTEE ON ACADEMIC COMPUTING
AND COMMUNICATIONS (UCACC)
Kyaw Tha Paw U, Chair
Email: ktpawu@ucdavis.edu

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

May 15, 2024

JAMES STEINTRAGER, CHAIR
ACADEMIC COUNCIL

Re: February 26, 2024, Letter from President Drake Regarding Information Security Investment Plans

Dear Chair Steintrager,

The University Committee on Academic Computing and Communications (UCACC) discussed the letter from President Drake to campus chancellors, dated February 26th, 2024, at its April 26th, 2024, meeting. The letter requests an updated information security investment plan "To strengthen our cybersecurity posture and mitigate potential risks." Our committee supports the concept of robust and timely cybersecurity policies and practices and is well aware of potential cybersecurity risks. The committee also understands that in an R1 University, with a significant portion of the budget garnered from extramural sources by academics, along with its educational responsibilities, it is critical to balance faculty and student research and educational opportunities with constraints related to cybersecurity measures. In the spirit of shared governance and constructive engagement, UCACC offers the following discussion points, comments, and concerns:

1. The University of California is dedicated to the principle of shared governance. UCACC members believe unequivocally that no substantive action should be taken without faculty consultation, recommendation, and ultimately endorsement by the Academic Senate. Such consultation can produce effective, constructive, and timely results from the close partnership of faculty and the administration. The faculty were not consulted about standards and controls described in the letter, nor the scope, timelines, and non-compliance consequences. Indeed, UCACC was made aware of the letter only weeks after it had been sent to the Chancellors, through rumors from IT staff that eventually made their way to individual committee members. Given the far-reaching nature of the letter, UCACC is deeply disappointed at the lack of consultation and believes timely consultation on each of the most significant items in the letter could have considerably improved the letter contents. Shared governance was not respected in this case.

2. The letter is guided by corporate cybersecurity models, but these models are not well-suited to the research universities. Corporations often provide free laptops, workstations, and devices such as mobile phones to all employees with corporate network access and can thus claim ownership. UC cannot easily follow this model as it would require a massive initial investment in hardware and prohibitively expensive ongoing maintenance/replacement costs. This is partially the reason for thousands of BYOD (bring your own device) units across UC. Hundreds of thousands of UC students

also connect personal devices to the UC network. The President's letter fails to address this crucial issue and the complications it imposes on the campuses as they attempt to respond.

3. Mandates for Endpoint Detection and Response (EDR) and tracking software could have both academic freedom and personal privacy implications. Further, many faculty have encountered issues with computer performance after having the software installed. Trellix, the EDR system used at UC, can in certain situations track endpoint website browsing, delete files and folders, and remotely shutdown devices without saving work in progress; this implies use of Trellix can potentially invade private personal data or cause data loss. A similar concern for both university devices and BYOD is that research and teaching data could similarly be deleted or monitored. In past conversations with ITS personnel about asset inventories it was not clear that BYOD would be part of the overall asset inventory and required to covered by EDR software.

4. The letter mentions "university networks" monolithically, when discussing EDR and asset management of connected devices. The committee believes Eduroam, campus guest, and similar wifi networks should be considered in the realm of public networks, and therefore not be subject to the same cybersecurity measures (EDR and related software) as trusted (mainly "wired") campus networks. Members noted that many university community members connect their personal mobile phones to campus wifi for phone service, as mobile phone coverage is sometimes poor on portions of campuses and, in fact, over a large area of some campuses such as UCSC. There could be serious degradation of safety in such cases if non-compliant personal mobile phones were excluded from wifi access. Along the similar lines, we would like clarification of how the cybersecurity policies could adversely affect "sandboxes" used in the development of teaching and research software within trusted networks.

5. There must be an unambiguous and detailed definition of which computer devices/assets connected to university networks would be subjected to EDR and related software. If this is left to the campuses, then each campus must provide such detailed definitions in consultation with the Academic Senate. For example, there numerous internet of things/internet of everything (IOE) devices connected to university networks, including printers, other peripherals, cameras, lighting, HVAC, CO_2 and other sensors, laboratory equipment, and more. The scope of devices subject to EDR and related software controls need to be clearly documented and communicated.

6. Multiple UCACC members report that their home campuses are planning to implement significant new restrictions on email in response to the President's letter. For example, discontinuing the possibility to automatically forward University emails to another provider, disallowing the use of certain email clients, and eliminating IMAP support. It should be stressed that individual faculty incorporate email into their research/teaching/administrative workflow in very different ways, reflecting the vast range of disciplines and backgrounds represented at UC. Some faculty will face major hardships and loss of productivity if forced to adapt to new email restrictions. Additionally, robust and universal email availability, with diverse email clients to reduce the possibility of complete email blackouts, is essential for UC. Email communication restrictions, including potentially isolation of specific devices on which users rely for emails, must involve alternate non-email plans to reach community members. Individual campuses should not consider any new restrictions on faculty email without first engaging in an extensive consultation with the Academic Senate.

7. Sanctions on "unit heads" who are found to be non-compliant, such as merit increase restrictions, may violate current faculty APM policies. The vague definition of unit heads in IS-3, UC's Information Security policy, and its FAQs includes not only department chairs, but individual faculty with extramural grants in the role of PI. Not all campuses have formally defined, which roles qualify as unit heads. UCACC finds it unacceptable for faculty with extramural grants to fall in this category if subject to the consequences outlined in the president's letter and notes that the threat of withheld merit increases would have a chilling effect on faculty proposals to extramural agencies and could result in decreased UC extramural funding. Also, the designation of department chairs as "unit heads" is highly problematic in this context. In many departments, chairs lack any practical control over the faculty they ostensibly "oversee." Further, it is already difficult enough to identify candidates willing to serve as department chairs without the additional threat of sanctions related to IT-security-compliance issues.

8. The potential for quarantining LMS (Canvas, for example) users, such as students and faculty, could violate student educational access rights. Some aspects of the letter imply that these actions could take place. At the very least, we need clarity in this regard. Related to this, would all students required to use LMS by instructors then have their BYOD devices, frequently used in their own residences, subject to mandated EDR software that monitor their private website browsing histories, etc.?

9. The committee has not seen data or analysis of the effectiveness of EDR and related software, multifactor authentication, or cybersecurity training. We have also seen little showing these measures' relevance to cyberattacks on UC. Some of the most widespread and egregious successful cyberattacks on UC have been from contracted vendor software (e.g., the Accellion incident). Other more distributed incursions have been from social engineering related failures by endpoint users. A number of these incidents, perhaps even a large portion of them, would have occurred regardless of EDR and MFA protections, because personal information leading to financial damage, ransomware attacks, etc., were accidentally divulged or voluntary actions were taken by the users.

10. Implementation of many of the letter's cited activities could result in substantial increases in local IT personnels' workloads and necessitate hiring additional IT personnel. Similarly, some campuses are discussing the need to purchase entirely new networking hardware, to facilitate endpoint tracking. Where will the funding for all of this come from? UCACC notes some important local priorities may be superseded by the increased workload on IT personnel related to the letter's activities.

11. Implementation of the letter's actions have unclear implications for campus HPC and GPU (high performance computing and graphic processing units) systems and research-IT infrastructure in general. To what extent were campus research-IT personnel consulted in the drafting of this letter and to what extent are they currently being consulted at the various campuses in response to it? UCACC members report that on some campuses the research-IT staff are hardly being consulted at all; potentially impactful decisions to researchers are apparently being made solely by local ITS personnel.

12. Many faculty in the sciences and engineering rely upon legacy computer systems to drive older scientific instruments. It is not clear whether there are exceptions for systems that are unable to comply with the endpoint standards laid out in the letter. How are affected research groups expected to navigate this situation when 100% compliance is required?

13. Over the last few years, UCACC has heard many reports on cybersecurity from UC CIO Van Williams and other high-level officials within the UC ITS organization. Unfortunately, these interactions have mostly consisted of one-way reports of technical metrics and details that seemed far removed from the day-to-day life of typical faculty members. ITS never suggested to UCACC that security concerns could eventually lead to the sorts of invasive and productivity robbing "solutions" that are now being considered by individual campuses as they scramble to respond to the demands of the President's letter. The lack of meaningful consultation between ITS and the UCACC on security issues over the last several years seems to be an opportunity lost. We hope that UCOP will engage with UCACC in a more proactive way moving forward on all IT related issues.

Finally, UCACC would like to remind the administration that the UC system includes numerous faculty members with extraordinary expertise in cybersecurity solutions.[1] We urge UCOP to invite this valuable resource into the conversation from the outset, and continually during any policy development process. Thank you for your attention to these concerns.

Sincerely,

Kyaw Tha Paw U
Chair, University Committee on Academic Computing and Communications

Cc: Academic Senate Executive Director Monica Lin
UCACC members

[1] UC Berkeley, for example, is ranked #5 in the nation for cybersecurity education: https://www.usnews.com/best-colleges/rankings/computer-science/cybersecurity

UNIVERSITY OF CALIFORNIA

Michael V. Drake, MD
President

Office of the President
1111 Franklin St.
Oakland, CA 94607

universityofcalifornia.edu

February 26, 2024

CHANCELLORS

Dear Colleagues:

As you know, protecting the University's sensitive information and systems is of paramount importance. To strengthen our cybersecurity posture and mitigate potential risks, we are requesting submission of an updated information security investment plan.

Plan Expectations:

Your plan should outline your location's strategy for achieving the following key outcomes by May 28, 2025:

- Standards compliance:
  - Ensure cyber security awareness training for 100 percent of location employees.
  - Ensure timely cyber escalation of incidents in alignment with UC Incident response and cybersecurity escalation standards.

- Controls compliance:
  - Ensure identification, tracking and vulnerability management of all computing devices connected to university networks.
  - Deploy and manage UC-approved Endpoint Detection and Recovery (EDR) software on 100 percent of assets defined by UC EDR deployment standards.
  - Deploy, enable, and configure multi-factor authentication (MFA) on 100 percent of campus and health email systems in conformance with established UC MFA configuration standards.
  - Deploy and configure a robust DLP solution for all health email systems to mitigate unauthorized data exfiltration.

Scope:

The investment plan should include:

- All location units including but not limited to AMCs, schools, divisions, departments, and centers regardless of whether their IT infrastructure is managed centrally.
- All employees (inclusive of faculty).

Timeline and Reporting:

- Plan Submission: Please submit your updated comprehensive information security investment plan to interim CISO, Monte Ratzlaff (Monte.Ratzlaff@ucop.edu) by April 30, 2024.
- Plan Completion: Plan outcomes should be achieved by May 28, 2025.
- Progress Reports: Please submit written progress reports to interim CISO Monte Ratzlaff on June 30, 2024; August 30, 2024; October 30,2024; January 30, 2025; and March 28, 2025. Progress reports should be discussed as part of your location's bi-annual digital risk meetings.

Supporting Resources:

To support the execution of the investment plan, the Office of the President makes the following resources are available:

- Cyber Risk Coordination Center
- Be Smart About Cyber and Safety Programs
- ECAS Audit Advisory Services
- UC Threat Intelligence Services
- UC Threat Detection and Protection Services
- UC Security Risk Assessments
- UC Cybersecurity Consulting Services

Non-Compliance Consequences:

We understand that achieving these goals requires dedicated effort and resource allocation. However, failure to comply with these requirements will have significant consequences, including:

- Non-compliance with any outcomes stated above will result in a 15 percent increase of your location's cyber insurance premium, reflecting the elevated risk posed to your location and the system.
- Non-compliant units will be assessed all or part of the costs related to security incidents up to $500,000 that are a result of the failure to comply with these requirements.
- Merit increases for unit heads whose units are found to be non-compliant require approval from the Chancellor.

We are confident that all locations share our commitment to protecting our vital information and systems. We encourage you and your teams to utilize the resources available through UC IT and the Cyber-risk Coordination Center to develop and implement your plans effectively.

We appreciate your cooperation and look forward to receiving your information security investment plans by the deadline.

Sincerely,

Michael V. Drake, MD
President

cc: Executive Vice President and Chief Operating Officer Nava
Chief of Staff Kao
Vice President Williams
Chief Risk Officer Confetti
Interim CISO Ratzlaff
Chief Policy Advisor McAuliffe
Managing Counsel Sze