



Robert C. May
Telephone: (510) 987-0711
Email: robert.may@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

May 3, 2019

**JANET NAPOLITANO, PRESIDENT
UNIVERSITY OF CALIFORNIA**

Re: Response to Reports from two Tiger Teams on International Research and Students

Dear Janet:

The Academic Council has endorsed the attached statement in response to your letters of February 7 2019, which conveyed recommendations from two systemwide tiger teams for protecting UC from potential risks from foreign entities, and February 13, which provided additional guidance for UC engagements with specific Chinese network equipment companies.

We understand that the two tiger team reports on *Vulnerabilities Associated with International Students*, and *Sensitive Information and Materials Related to International Agreements*, offer recommendations for protecting UC systems and intellectual property in ways that attempt to balance national security concerns with the University's commitment to an open and collaborative research environment.

The Academic Council found the combined recommendations helpful to the extent that they raise awareness about real, organized efforts to remove intellectual property and sensitive information from the University and express general principles related to foreign visitors, faculty, and students. However, the Council also identified several issues that we believe did not receive adequate attention in the reports, related to 1) the broad nature of potential risks; 2) the role of faculty in balancing academic freedom with University and national security concerns; and 3) the implicit—and at times explicit—racialization of the issues. The statement elaborates on these points.

Please do not hesitate to contact me if you have additional questions.

Sincerely,



Robert C. May, Chair
Academic Council

cc: Provost Brown
Senior Vice President Bustamante
Vice President Ellis
Academic Council
Senate Directors

Academic Council Statement on International Risk Tiger Teams Reports

We write in response to President Napolitano's letters of February 7 and 13, 2019, and accompanying appendices. We would like to add our voice of concern with regard to the potential theft of intellectual property and unauthorized access to protected information, but we also want to call attention to the fact that these concerns are presented specifically as arising from University collaborations and agreements with transnational corporations and international research institutions. The issue is similarly described in these documents as tied to the University's relationships with international visitors and students. While we understand the particular political circumstances that motivated writing these letters as well as the work of the Task Forces summarized in the accompanying appendices, as University of California faculty we want to underscore that there is a collective institutional need to identify and share best practices to protect all intellectual property and sensitive data *in general*, thus shifting the emphasis from *international* or *foreign* threats to *all* threats to our research and other forms of confidential data.

As faculty at the University of California, our primary obligations involve the generation and dissemination of scholarly knowledge. Within that framework, we produce valuable intellectual property (IP) that we recognize must be properly safeguarded. We take our role as stewards of this IP very seriously. Moreover, because our access to protected information extends beyond technology and trade secrets to information about ourselves, our students, our staff, and (in the case of our medical centers) our patients, we understand that legal, ethical, and professional responsibilities require us to minimize the risk of exposing data that is at once confidential and/or privileged in nature. That is to say, as faculty we understand the vulnerabilities and real threats to the University, in particular, and to the country in general. Such threats can be posed by carelessness and/or misinformed and/or nefarious actions and access to highly sensitive, at times confidential, data. As such, we are committed to operating with best practices that mitigate potential threats.

This being said, we would like to highlight three issues that we believe to be of critical importance and that did not receive adequate attention in President Napolitano's letters and appendices: (1) the broad nature of potential risks; (2) the role of faculty in balancing academic freedom with University and national security concerns; and (3) the implicit—and at times explicit—racialization of the issues.

1. Potential Risks: *The potential risks to IP and sensitive data emerge not only from the malevolent actions of a few bad actors, but also from the faculty's lack of familiarity with the best practices required to protect our intellectual property.*

The exposure of sensitive data may arise from the unintended consequences of appropriate but poorly constructed collaborations with industry partners and researchers from other institutions, regardless of national origin, or from our day-to-day activities as we create and access protected information within the University. The liability of data exposure is hardly new, and UC faculty have been dealing with intellectual property protections, knowledge transfer, and research collaborations and relationships for many decades. On the whole, faculty have acted in good faith and have been good stewards during this time. More recently, however, our research collaborations and relationships

have expanded rapidly and have correspondingly grown in complexity; our data banks are much larger than ever before. While this development has allowed for a dramatic increase in the acquisition, sharing, and production of knowledge, it has also increased the risk of exposure; our mechanisms for controlling access—as well as our understanding of the attendant risks—have not kept up with these flourishing and complex research efforts. We must, therefore, concentrate on strengthening and implementing best practices to ensure that we remain well-informed and proactive stewards of our intellectual property and sensitive data. In this regard, we find good guidance in the UCSF Data Sharing and Security Task Force report of October 2018, which has both defined the risks and suggested recommendations for minimizing them. We also note the creation of mechanisms to protect the open access digital data.

2. Academic Freedom and National Security: *We believe it is critical that faculty remain empowered to balance academic freedom with the need to protect the University and the country from any risks to national security, whether domestic or international.*

While we recognize and appreciate the fact that there may be serious national security concerns related to intellectual property and our access to sensitive, often confidential, data, we want to underscore the point that faculty are not the agents of national security. As such, any efforts to mitigate risks to national security must be set against the need to protect the University's core principles of academic freedom, which enable our faculty, staff, and students of all nationalities to discuss ideas openly, to publish research results, and to determine research teams without regard to citizenship restrictions. The University of California's teaching and research excellence has established us as a global leader in the creation and dissemination of new knowledge, which ensures that we are the destination of choice for many of the world's best scholars and students. We deeply value the significant contributions that members of the international scholarly community have made to the University's research and teaching missions, to California's and the nation's prosperity, and to the global production of knowledge and scholarly excellence.

3. Racialization of Risk: *We are particularly concerned about the ways in which these University discourses of risk are implicitly—and, in some cases, explicitly—racialized.*

We find that an emphasis on “high-risk” countries to be highly problematic and inappropriate given our belief that the unintentional actions that put the University at risk will outpace the threats from domestic and international malevolent actions. Specifically, the recent focus on Huawei and ZTE in the February 13 letter—together with the widespread dissemination of similar correspondence on some campuses without Senate consultation—is very disconcerting, especially given the anticipatory and conditional language of President Napolitano's letter. Although the February 13 letter makes clear that “there is currently no legal prohibition against the University directly entering into telecommunications contracts with Huawei and ZTE or from receiving grant funds or gifts from such entities” (p. 2) and “neither Huawei nor ZTE is currently listed on any government restricted parties list” (p. 3), it goes on to describe possible actions that the White House and the NDAA *could* take. That these *potential* outcomes are driving University discourse, and even actions at some campuses, is extremely disturbing for two

reasons: first, such actions reproduce long legacies of racial profiling, exclusion, discrimination, and oppression that severely undermine UC's core values; and, second, both the University administration and Academic Senate have a strong tradition of resisting U.S. presidential decrees and actions that go against our core values. We are thus dismayed and concerned to see the University echo the racialized language of a perceived foreign threat.

To be clear, we are not suggesting that there are no real threats to University IP and to national security. We also recognize that these threats can derive from foreign governments working through international researchers and students. That being said, we advocate for a broader articulation of the nature of these threats to IP and a better understanding of the need to protect sensitive and confidential University data as well as national security. Such broader understanding must avoid perpetuating those racialized discourses and legacies that distort our understanding of the high risks at stake.