UNIVERSITY OF CALIFORNIA, ACADEMIC SENATE

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

J. Daniel Hare
Telephone: (510) 987-9303
Fax: (510) 763-0309
Email: *dan.hare@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 2, 2016

TOM ANDRIOLA
VICE PRESIDENT AND CHIEF INFORMATION OFFICER
UNIVERSITY OF CALIFORNIA

Re: Senate Representation on Cyber-Risk Governance Committee and Advisory Board

Dear Tom:

At its May 25, 2016 meeting, the Academic Council approved a plan from the University Committee on Academic Computing and Communications (UCACC) for the addition of Senate faculty representatives to the Cyber-Risk Governance Committee (CRGC) and its technical Advisory Board.

As noted in the attached letter from UCACC Chair David Kay, the three representatives to the CRGC will be the UCACC chair and vice chair, and a representative from either UCAF or UCFW selected by UCOC. UCOC will also be working with the Senate divisions to select three faculty with appropriate technical expertise to represent the Senate on the Advisory Board.

I want to thank you again for agreeing to add additional faculty membership to the CRGC, for your commitment to shared governance, and willingness to work closely with the systemwide Senate and campus Senates on cybersecurity issues and concerns.

Sincerely,

J. Daniel Hare

J. Daniel Hare, Chair
Academic Council

Cc: UCACC Chair Kay
UCOC Chair Kaufman
Academic Council
Senate Director Baxter
Senate Executive Directors

UNIVERSITY OF CALIFORNIA, ACADEMIC SENATE

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

UNIVERSITY COMMITTEE ON ACADEMIC COMPUTING
AND COMMUNICATIONS (UCACC)
David G. Kay, Chair
kay@uci.edu

ACADEMIC SENATE
University of California
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200

May 10, 2016

DAN HARE, CHAIR
ACADEMIC COUNCIL

Dear Dan,

The University Committee on Academic Computing and Communications (UCACC) asks that the Academic Council approve the plan described in this letter for the addition of Senate faculty to both the Cyber-Risk Governance Committee (CRGC) and its technical Advisory Board. (For completeness, background details on these groups appear below.) I have consulted the University Committee on Committees (UCOC) and they join UCACC in this recommendation.

1. We suggest that the three representatives to CRGC be the chair and vice chair of UCACC (or their designees) and a representative from UCAF or UCFW. UCOC would make these appointments in consultation with the chairs of the committees.

2. We suggest that UCOC select the three representatives to the Cyber-Risk Advisory Board by soliciting nominations from divisional COCs, selecting faculty members with broad technical expertise in cyber-risk and computer security issues such as encryption, threat detection and monitoring, malware, privacy, and deployment of enterprise-scale security measures.

Regards,

David G. Kay, Chair
UCACC

Cc: Hilary Baxter, Academic Senate Executive Director
UCACC Members
Tom Andriola, Vice President and Chief Information Officer

Appendix

The **Cyber-Risk Governance Committee (CRGC)** is a systemwide body comprising CREs[*] from all locations along with up to three (3) faculty representatives and subject matter experts from the Office of the President responsible for monitoring UC's risk profile, overseeing cyber-risk strategies, and coordinating cybersecurity efforts across the system. Other responsibilities include developing policy recommendations, establishing rules for information sharing, and ensuring vertical and horizontal communication in a crisis response situation. The Committee currently meets four times per year.

The **Cyber-Risk Advisory Board** is an advisory body to CRGC comprising cybersecurity subject matter experts from inside the UC system and externally who will meet with the CRGC twice per year to provide information and advice about industry trends and best practices. The Advisory Board will be made up of six members: 3 faculty members appointed by the Academic Senate and 3 external members selected by UCOP.

The full charters of both groups are attached.

[*] Cyber-Risk Responsible Executive (CRE): Senior official appointed by the Chancellor who coordinates and is responsible for efforts to strengthen cybersecurity at their respective location. This person shall be a direct report of the Chancellor for this purpose.

CYBER-RISK GOVERNANCE COMMITTEE PROJECT CHARTER

Version 2.0, April 15, 2016

Executive Sponsor:	**Janet Napolitano, President**
Project Lead:	**Tom Andriola, Vice President and Chief Information Officer**
Project Manager:	**David Rusting, Chief Information Security Officer**

Committee Purpose and Charter: The Cyber-Risk Governance Committee (CRGC) is responsible for monitoring the University's risk profile, overseeing investment strategies, and coordinating cybersecurity efforts across the system. Additionally, the CRGC ensures that UC's work is informed by the latest research, subject matter expertise and best practices in the cybersecurity context.

The CRGC's work is a component of a broader UC strategy put forth by President Napolitano to enhance UC's cyber security efforts through the implementation of the following five pillars of cyber related activity:

- Enhanced governance structure including the creation of the Cyber-Risk Governance Committee and connections to existing administrative, joint and Academic Senate committees;
- Enhanced risk management by implementing consistent detection, notification and remediation protocols for cybersecurity incidents;
- Adoption of modern technology including execution of a plan at each location to upgrade technology and share best practices. This will not only create consistency in our cyber defense approaches but also leverage the investments that are being made across the UC system;
- Hardened security environment through the sharing information across the system, with an emphasis on best practices and security protocols; and
- Systemwide culture change including educating our faculty, staff, and students and the creation and execution of clear protocols of escalation.

In addition to the five pillars of cyber related activity, CRGC members - each location's responsible executive and members of the faculty - are accountable for leading cybersecurity related efforts which include the following activities:

- Participate in Systemwide Initiatives. Participate in systemwide discussions and planning efforts to facilitate and promote cyber-risk reduction, including prevention and early and effective detection of and response to cyberattacks;
- Develop Routine and Incident-Driven Cybersecurity Risk Reporting Processes. Arrange for regular (at least quarterly) executive-level discussion of cyber-risk management across the campus, including independently managed campus components and controlled affiliates, with regularly scheduled meetings with the Chancellor, Lab Director, or other chief executive of the location; and assure local development, implementation, training on, and regular review of incident response plans consistent with systemwide standards; and
- Develop a Cybersecurity Resource Plan and Implementation Timeline. Confirm the campus's and each component unit's and controlled affiliate's commitment to adequate staffing and budget to support cybersecurity enhancement initiatives, driven by consistent, risk-based analysis.

Project Governance and Roles Summary:

President of the University: Serves as the executive sponsor for the cybersecurity effort and liaise with the Board of Regents to provide updates on progress and issues.

Chancellors, the Director of the Lawrence Berkeley National Laboratory, and Vice President of the Division of Agriculture and Natural Resources: Accountable to the President for ensuring that cybersecurity related activities are achieved and that ongoing monitoring and mitigation are occurring.

Cyber-Risk Responsible Executive (CRE): Senior official appointed by the Chancellor who coordinates and is responsible for efforts to strengthen cybersecurity at their respective location. This person shall be a direct report of the Chancellor for this purpose.

Project Lead: Overall responsibility for the achieving the goals and meeting the project's objectives, negotiates viable solutions for areas of conflict, oversees team organization and performance and provides quality assurance.

Cyber-Risk Governance Committee: System-wide body comprised of CRE's from all locations along with up to three (3) faculty representation and subject matter experts from the Office of the President responsible for monitoring UC's risk profile, overseeing investment strategies, and coordinating cybersecurity efforts across the system. Other responsibilities include developing policy recommendations, establishing rules for information sharing, and ensuring vertical & horizontal communication in a crisis response situation. If the CRE is unable to participate in a committee meeting they can send a delegate on their behalf.

Cyber-Risk Advisory Board: Advisory body comprised of cybersecurity subject matter experts from inside the UC system and externally who will meet with the Governance Committee twice per year to provide information and advice about industry trends and best practices. The Advisory Board will be made up of six members – 3 faculty members appointed by the Academic Senate Leadership and 3 external members selected by the Project Sponsor and Project Lead.

The University Committee on Academic Computing and Communications (UCACC): Faculty Senate committee representing all matters involving the uses and impact of computing and communications technology. The committee also advises the President concerning the acquisition and usage, and support of computing and communications technology and related policy issues at the University. The UCACC will be the formal mechanism for faculty issues and concerns around cyber-risk and cyber-security to be raised to the CRGC.

Cyber-Risk Coordination Center: The Coordination Center is a program office located at the Office of the President that supports the governance processes and acts as a single point of contact and expertise within the University for cyber-security topics, systemwide cyber communication, and best practices for cybersecurity information and templates.

Project Milestones:

- ☐ Milestones are set in the CRGC meeting

Cyber-Risk Governance Committee Appointees:

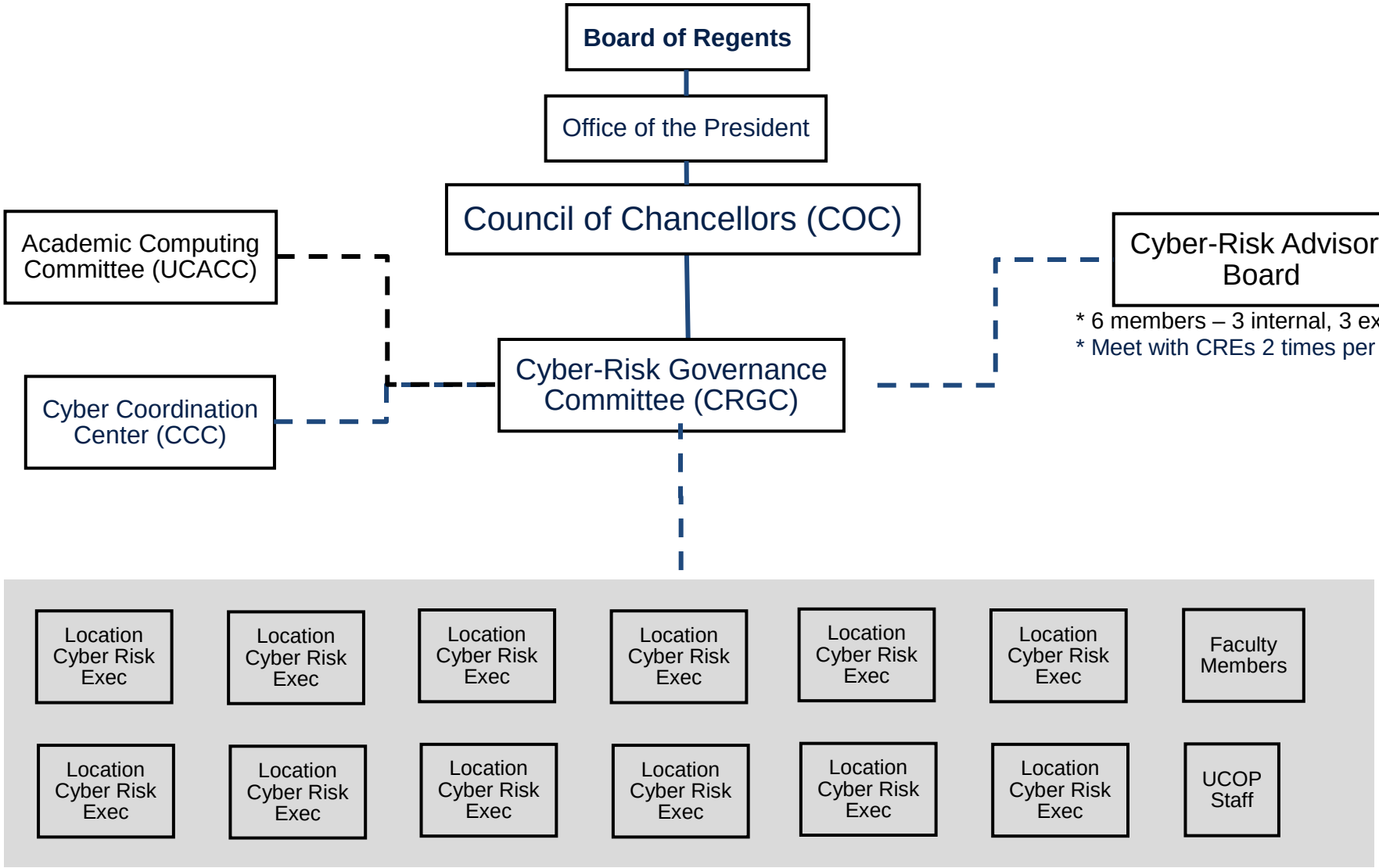
Name	Title	Location
Rosio Alvarez	Chief Information Officer	LBNL
Joe Bengfort	Senior Vice President and Chief Information Officer	UCSF
Christine Borgman	Vice Chair, Academic Senate's Committee on Academic Computing and Distinguished Professor & Presidential Chair in Information Studies	UCLA (Faculty)
Ron Coley	Vice Chancellor for Business and Administrative Services	UCR
Mary Doyle	Vice Chancellor Information Technology	UCSC

Anthony Joseph	Chancellor's Professor	UCB
Ralph Hexter	Provost and Executive Vice Chancellor	UCD
David Kay	Chair, Academic Senate's Committee on Academic Computing and Senior Lecturer SOE, School of Information and Computer Sciences	UCI (Faculty)
Enrique Lavernia	Provost and Executive Vice Chancellor	UCI
Pierre Ouillet	Vice Chancellor and Chief Financial Officer	UCSD
Luanna Putney	Associate Chancellor and Senior Advisor to the Chancellor	UCM
Matt Hall	Chief Information Officer	UCSB
Barrie Strickland	Chief Financial Officer	UC Health
Gabriel Youtsey	Chief Information Officer	ANR
Scott Waugh	Provost and Executive Vice Chancellor	UCLA
Tom Andriola	Vice President and Chief Information Officer	UCOP
Kim Budil	Vice President, National Laboratories	Labs
Cheryl Lloyd	Chief Risk Officer	UCOP
Seth Grossman	Chief of Staff to President Napolitano	UCOP
Julie Henderson	Senior Vice President, Public Affairs	UCOP
Rachael Nava	Executive Vice President and Chief Operating Officer	UCOP
Charlie Robinson	Vice President and General Counsel	UCOP
David Rusting	Chief Information Security Officer	UCOP
Sheryl Vacca	Senior Vice President and Chief Compliance and Audit Officer	UCOP

Meeting Schedule for 2016:

- Meetings in January, April, August, and November

UC Cyber-Risk Governance Structure



Cyber Risk Executives (CRE)
* 10 locations + ANR + Lab Mgmt. + OP functions
* Up to 3 Academic Senate Reps (chosen by Senate)

CRGC Meetings
* Meet as a group four times per year

CYBER-RISK ADVISORY BOARD CHARTER - DRAFT

Version 0.2; October 2, 2015

Executive Sponsor:	**Janet Napolitano, President**
Project Lead:	**Tom Andriola, Vice President and Chief Information Officer**
Project Manager:	**David Rusting, Chief Information Security Officer**

Advisory Board Purpose and Charter:

The Cyber-Risk Advisory Board is comprised of cybersecurity subject matter experts from across the University and external to the University who will meet with the Cyber Risk Governance Committee (CRGC) to provide information and advice about industry trends and best practices in the area of cyber risk and cyber security.

Advisory Board Responsibilities:

- Meet with the CRGC twice per year, in conjunction with the CRGC meeting calendar
- Review with CRGC significant policies, procedures, processes and systems, as requested by the Committee, to evaluate effectiveness and impact for the identification, management and planning for cyber risks
- Identify and articulate the issues, topics and challenges related to cyber risk and cybersecurity in the context of today's environment, including "best in class" developments within the appropriate context
- Identify other subject-matter experts and knowledge leaders who can support the University in ways that help assist in the identification and management of cyber risk
- Provides strategic input and insight as to the focus of the CRGC in terms of the role, perspective and priority of cyber risk topics
- May be requested by the CRGC or the Executive Sponsor for specific advice or presentation

Potential Advisory Board Members

- Leverage subject matter experts already in the UC
    - Amit Sahai, Professor of Computer Science at UCLA and Director of the Center for Encrypted Functionalities
    - Shankar Sastry, Dean of the College of Engineering at the University of California at Berkeley
    - Rosio Alvarez, Lawrence Berkeley National laboratory, Division Director for the Information Technology Division and Chief Information Officer

- External Advisors
    - Catherine Bessant, Bank of America, Chief Operations and Technology Officer
    - Paul Proctor, Gartner Research, VP, Distinguished Analyst, and Chief of Research for Security and Risk Management
    - Rand Beers, former Deputy Assistant to the President and Deputy Homeland Security (DHS) Advisor and former Under Secretary for the National Protection and Programs Directorate at DHS