A3

Office of the President

TO MEMBERS OF THE COMMITTEE ON COM PLIANCE AND AUDIT:

DISCUSSION ITEM

For Meeting of July 17, 2013

PRESIDENT'S PRIVACY AND INFORMATION SECURITY INITIATIVE

Senior Vice President – Chief Compliance and Audit Officer Vacca and Director of Strategic Information Technology Policy and Chief Privacy Officer Kent Wada from University of California, Los Angeles will provide an overview of the *Privacy and Information Security Initiative Steering Committee Report to the President* which describes the importance of Privacy and Information Security at the University of California. Listed below are the Report's revised recommendations to the President:

1. The report speaks to the University's adoption of Statement of Privacy Values, Privacy Principles, and Privacy Balancing Test. These are the most basic conceptual building blocks underlying the University's ability to fluently manage privacy issues. It is requested that the President initiate the action needed to have these items adopted by the University (similar to the Statement of Ethical Values and Standards of Ethical Conduct).

2. The report speaks to a requirement for each campus to designate a privacy official – an operational point person to make privacy "visible," to begin incorporating the Privacy Statement, Principles, and Balancing Test into the fabric of campus life; and to coordinate with peers systemwide. This designation does not require the creation of a new position, though the simple act of highlighting privacy likely will quickly reveal an unmet need. It is requested that the President initiate the action needed to have each Chancellor designate a privacy official for his or her campus.

3. The report describes a model for governance through campus privacy and information security boards. However, allowing the University to gain experience with the implementation of the recommendations above will inform campus planning for achieving the goals articulated in the Steering Committee's report – campuses will need flexibility, appropriately leveraging what they already have in place. It is requested that this overarching need be identified in communicating to the Chancellors as a longer-term goal.

The presenters will discuss the President's endorsement of the recommendations and the plan for moving the specific recommendations forward.

(Attachment below)

President's Privacy and Information Security Initiative

July, 2013

Privacy …

- Is fundamental to the University, long part of the UC culture
- Underpins academic and intellectual freedoms key to the mission
- Provides a basis for an ethical and respectful workplace
- Together with information security, is critical to the University's ability to be a good steward of information entrusted to it by students, faculty, staff, and community

What's Changed? Why Now?

- ↑ Technology (e.g., smartphones, expectations in the Facebook era)
- ↑ Consequences of failure (e.g., breaches)
- ↑ Proliferating obligations (e.g., law, regulation, etc.)
- ↑ Proliferating partnerships with external vendors (e.g., Google, Microsoft)
- ↑ Tensions between privacy and information security
- ↑ And much more …

- No vehicle to adjudicate circumstances which cross policy jurisdictions or to consider balance with other University values and obligations (challenging)

The Charge from the President

- Take a step back and consider what is appropriate for UC in today's world, and recommend:
  - An overarching privacy framework
  - Governance, implementation and accountability structures
  - Formal ongoing process to address technical and societal changes impacting privacy and information security
  - Specific actions to implement the framework

The Committees

- Working Group
  - 16 members: faculty and staff representing key areas
  - Developed concepts and recommendations
- Steering Committee
  - 28 members: faculty, students, and administrators representing campuses and UCOP
  - Reviewed recommendations of Working Group and gave direction for next steps

Key Deliverables

- *Definitions*
- *Three recommendations* that together provide an overarching framework to guide decision-making and policy development at UC when privacy is involved:
  - A set of privacy values and principles, and a balancing test to adjudicate between multiple competing factors
  - A governance structure integrating privacy and information security
  - An operational point for privacy matters on each campus
- *Implementation schedule*

Definitions

Autonomy Privacy
ability of individuals to conduct activities without observation

Individuals
(e.g., web sites visited, research being conducted and related data)

Information Privacy
protects information about individuals

Information about individuals
(e.g., student or patient records; or SSNs)

Confidential information
(e.g., intellectual property, security info)

Information

Information Security
protects all information and infrastructure

Infrastructure
(e.g., computers and networks)

Recommendation 1

- University shall adopt:
  - UC Statement of Privacy Values
  - Privacy Principles
    - for Autonomy Privacy
    - for Information Privacy
  - Balancing Process

R2: Campus Privacy and Information Security Boards

- Each Chancellor assign to an existing body or form a Board: advisory
- leverage what they already have in place
- Joint Academic Senate – Administration
- Set strategic direction, not operational
- Champion privacy values, principles and balancing process
- Monitor compliance and assess risk

R3: Campus Privacy Official

- Each Chancellor designates a Privacy Official to be operational/management point on privacy matters
  - Responsible for collaborative development, implementation and administration of unified campus privacy program
  - Work's closely with campus Board
  - Responsible for infusing understanding and use of privacy values and principles across the campus
  - Does not need to be a new position, but at least a new responsibility for someone

Systemwide Board for Privacy and Information Security

- Should await campus experience
- In the interim Office of Ethics and Compliance will serve as the unit collecting case studies and best practices systemwide

Implementation Schedule

- 2013-14
  - Adopt committee recommendations
  - Board formations
  - Privacy Officials designated
  - System work group – policies and communication
  - Training and education
- 2014-15
  - Training and education
  - Build out campus privacy programs
  - Collect metrics and evaluate overall approach
- 2015 and beyond
  - Revise approach according to feedback received
  - Establish privacy reviews
  - Review and share balancing cases

Key Outcomes

- Identifying and distinguishing *autonomy privacy* from *information privacy*, and relating them to *information security*
- Integrating autonomy privacy and information privacy into a holistic framework led by the University's mission and values
- Allowing for institutional deliberation across values, obligations, policies, and jurisdictions through the Boards
- Increased awareness and communication

The Report's Intent

- "The report's recommendations, if adopted, put into place a unified privacy model, led by the University's mission and values, against which existing guidance for decision-making, policy, and practice in the area of privacy and information at the University of California can and should be aligned over time."