A. Welcome, Introductions, Approval of Summaries
Dana Cuff, Chair

B. Changing Data Landscape: IDRE Updates
Bill Labate
Action: Information and Discussion

IDRE continues to see increases in its cloud storage and computational services for campus researchers. It has maxed out its current network infrastructure. IDRE recently received an NSF award of $500k to use toward a research cyberinfrastructure upgrade. The proposal has been endorsed by CITI, where an additional $900k was approved for the project. It is currently in discussion with ITPB members.

The Research Cyberinfrastructure (RCI) upgrade proposal meets the requirements and expectations for research. It will increase performance and capabilities in an efficient and scalable manner. It will also address the Medical Center’s requirements for HIPAA-compliant data computing, transfer, and storage. It will also off-load large amounts of data from the campus backbone which will alleviate traffic and make the network more efficient for the rest of campus.

The renewed systemwide University Committee on Academic Computing and Communications (UCACC) is seeing new rules emerging about keeping data for a certain amount of time without direction about the infrastructure to do so. And the NSF is envisioning how to keep data for 20 years beyond end of career. These are very relevant issues that a research cyberinfrastructure needs to address.

C. IS-3 Policy Review
Andrew Wissmiller, Mike Story
Action: Review and Comment

Overview
The last revision of the IS-3 Policy was in 2011. Though it was due for an update, recent events precipitated an accelerated process. The revision project has been led by David Rusting, Chief Information Security Officer at UCOP, and IT Policy and Security (ITPS) members.

The group has been revising the policy since summer, and the final draft is close to completion. It is expected to move to the presidential signature process shortly, where it will get 6 months for review and comments. The policy references ISO 27000, includes high-level principles, and clarifies roles and responsibilities.

Each campus must produce a plan, track progress, and share it with UCOP. This will help determine whether there is a common approach across campuses. We are moving toward more standardized processes, including inventory assessment, management, and protection of assets. We are also shifting from the old idea of data ownership to the concept of data stewardship.
IT Services will work in partnership with campus units to find common ground. Every unit will be responsible for its assessment and roll up results to IT Services. Furthermore, the policy indicates that each unit is responsible for its inventory and liable in a breach situation.

This is a risk-based approach that assesses threats and adds components of protection as necessary. Standardized audits will be scheduled regularly at the campus level. More auditing will help determine the greatest risks as well as inadvertent risks. Audits can also encourage best practices.

Once the final draft is available, it would be beneficial to get input from various groups regarding the inventory and categorization of assets, identification of gaps, etc. For example, student records for student systems – past, present and applying students – are critical across almost all we do. These data assets are important for doing business, need a good deal of protection, and need to be easily accessible to the individuals requiring use of those assets. Input will help better understand how to address the gaps and implement sustainable reviews.

**Researchers**

The controls (e.g., access controls, background checks, etc.) in the policy largely focus on an administrative context, but specifically call out duties for researchers.

In reviewing the requirements (listed on page 15 of the current draft), several members expressed concern about the requirements. The language used is unclear. If there are requirements for researchers, then the information should help and empower rather than burden the individual.

However, if researchers are using a research infrastructure such as the one available through IDRE, then researchers do not need to think about these requirements because they are built into the infrastructure.

**New Standards**

There is some urgency to update this policy due to the recent cyber attack event. Since guidance is coming from the top, our role will become very administrative and compliance-based. Clear, more prescriptive systemwide standards will be laid on top of policy.

[Mike Story provided the standards after the meeting to be included in the summary.]

1. Minimum security standard
2. Password management standard
3. Security incident response standard
4. Risk management standard
5. Encryption key and certificate management standard
6. Institutional information disclosure standard
7. Data classification standard
8. Data destruction standard
9. Software development standard
10. Secure software configuration standard
11. Test data standard
12. Environmental safeguards standard
13. Logging and event recording standard

**Privacy**

This policy reflects information privacy, and is silent on autonomy privacy. The Electronic Communications Policy (ECP) is more focused on autonomy privacy. The Board will need to decide how and through what process it will share its voice and expertise (e.g. via communication with UCACC, etc.).
Conclusion
From an administrative perspective, this is more in alignment with standard practices and can be thought of as a safety net. It is a standard framework and approach that seems to work, and there will be some latitude in the implementation process. The Board can help give input on proper, thoughtful implementation.

D. New UCLA Coordinating Committee on Information Security and Privacy
Jim Davis, Andrew Wissmiller
Action: Information and Discussion
The campuses have been tasked with putting cyber risk operational plans in place. UCLA has a robust governance structure already in place, so the campus put forth the existing structure and demonstrated how it works.

The campus and health system operate separately. The Coordinating Committee was formed to bridge gaps between the two entities, and they are working to better communicate and align where appropriate. It is an operational body, but several members also serve on the UCLA Board on Privacy and Data Protection. As appropriate, the Coordinating Committee will bring issues to the Board for review and input from faculty. The UC Office of the President also created a Cyber-Risk Committee, which include a representative from each campus (i.e., EVC Waugh represents UCLA) that meets with President Napolitano regularly.

E. New Security Training
Dana Cuff
Action: Information and Discussion
UC Office of the President recently launched mandatory systemwide online cyber security training for staff and faculty. There was a sense that the training was highly corporate and not designed for faculty. It felt compliance oriented, bland, and not particularly impactful.

At the last meeting, the Board discussed where members would like to make an impact. Is there interest in defining gaps, embedding better practices, and helping to drive culture change on these issues? Is there interest in augmenting the training to develop a better understanding of relevant topics, such as: encryption, intellectual property, or data implications when traveling abroad? There are amazing, real world examples to be learned from here at UCLA (e.g., nano data, genome data, etc.).

A couple of channels for providing input may be through the University Academic Committee on Academic Computing and Communications or the new Center of Excellence that is being developed.