Recommendations for Wireless
(ECC has endorsed Phase I; Standards for extended campus implementation unresolved with CSG and OIT; returned to Campus Wireless Implementation Team)

1. Upgrade existing campus wireless pilot infrastructure and operations to production level (Phase I Implementation).
   a. Establish production level service for existing pilot areas
   b. Extend wireless coverage to open common areas recommended by the Campus Wireless Team
   c. Extend wireless service to selected conference/meeting rooms
   d. Implement an interim production VPN
   e. Conduct PDA pilot test with VPN production service

2. No usage fee for Phase I but fee assessment is possible in the future.

3. Implement Phase I with the Campus Wireless Team’s proposed Networking Standards and Policies (i.e. CTS support any ‘open common areas’ approved for data wireless production deployment and schools, departments and administrative units provision wireless access in their ‘interior’ space).

4. From the perspective of campus vision of wide mobility while supportive of local constituency needs, assess current and alternative management and policy models for:
   - extending wireless into unit spaces;
   - addressing unsecure networks established by individuals.

Recommendations for Electronic Business via Email
(Endorsed by ECC task force but not yet endorsed by ECC; reviewed by CSG with final discussion and vote planned)

Outcomes of Email Model:

1. UCLA should provide a campus email address for all students, faculty and staff through which it is expected that campus business can be conducted. BOL accounts will be provided to anyone who does not otherwise have an email account.

2. Undergraduate students must have a @ucla.edu email address.
   - the address can be selected
Summary of Proposed ITPB Endorsements

• the address is persistent for life

3. Graduate students, faculty, and staff may optionally create a @ucla.edu email address that is automatically forwarded to an ‘actual email account’. Either a @department.ucla.edu or @ucla.edu email account may be used as the ‘actual email account’ in accordance with departmental policy.

4. If an email account is provided by a department, the department must update the ‘actual email account’ field in the central directory database.

5. Faculty and staff should be required to publish their email addresses unless there are safety or privacy concerns. A way to accomplish this is to publish an internal (visible only to UCLA) directory and an external directory. Publishing in the internal directory would be the default and mandatory. The external directory could have an opt-out feature.

Assumptions of BruinPost:
No fee for these services

6. Official Notifications are sent to fixed lists of recipients who satisfy the selection criteria (e.g. all staff, all students, Academic Senate Members, etc.) that is built into the system and does not change between messages. Individuals who satisfy the selection criteria are automatically included in the list and they do not have the ability to remove themselves from the list.

• Plain or formatted text
• No attachments, use web links
• Scheduled distribution – within 2 business days

7. Weekly Digest is used for non- ‘official’ emails. Recipients can opt-out.

8. Sender is responsible for message content and quality. MDDS is gatekeeper for faculty and staff; Registrar’s Office is gatekeeper for students.

Recommendations for Increased IT Security
(Preliminary assessment with CSG)

Campus-Wide Security Recommendation

1. Set the expectation that all campus units will have in place an IT security approach and process that minimizes threats not only to each local system but also to other systems and networks in the unit, across the campus or on the Internet, consistent with institutional values and institutional risks.
Summary of Proposed ITPB Endorsements

2. Define campus requirements, appropriate enforcement mechanisms and protocols and procedures for communications about security events.

Specific Recommendations

Incident Response

3. Update campus network procedures to clearly define the isolation process, including communications and delegation of authority, for errant systems or networks.

4. Explore requirements to establish an emergency response team (CERT/FIRST).

Campus Investment in Desktop Antivirus Software

5. Move to require antivirus software on campus equipment (noting that there will always be exceptions), including definition of appropriate enforcement mechanisms.

6. Consider the Sophos funding model for other security products as appropriate.

Scanning

7. Set the expectation that the regular scanning and intrusion detection of the entire UCLA network is necessary (will require cooperation between central and distributed units).

8. Set clear responsibilities for remediation of errant systems.

Patch Management

9. Set the expectation that all campus units will have in place a patch management approach (whether through use of a patch management tool or otherwise) that ensures all systems are patched in a timely manner, including definition of appropriate enforcement mechanisms.

10. Explore funding and other requirements for ubiquitous adoption of patch management tools by all campus units, similar to antivirus software.

Campus Mail Gateway

11. Deployment of SpamAssassin on the campus mail gateway for spam identification.
12. Deployment of Sophos AntiVirus Interface (SAVI) software on the campus mail gateway for virus detection. Infected messages will be available for viewing on one of the quarantined mail servers for up to seven days under normal conditions.

*BOL*

13. Deployment of SAVI on BOL.

**Recommendations for Project Assessment Process**  
(Assessment by CSG)

1. Continue to apply the process to all high impact, campus-wide projects.

2. Continue to refine the process from three perspectives:

   a. Communication – Ensure vetting, endorsement and closure at the appropriate stakeholder and governance levels (CSG, ECC, ITPB) and communication flow between all groups.

   b. Review - Ensure 1) reviews are timely; 2) makeup of review panels are appropriate; 3) questions asked will reveal project motivations, value and risks; surface technical architecture considerations; and uncover inter-project dependencies; 4) outcomes of review are documented and published.

   c. Operationalization - Promote better understanding and acceptance of the process by working with project managers to clarify process assessment components and best practices; promote and enable sharing of experiences among project managers to gain synergies.