**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.

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.
Proposed ITPB Endorsements

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.