Draft ITPB Security Policy Resolutions

**Background:** Elements of these resolutions have been in discussion in various ITPB and CSG meetings but in a reactive and piecemeal fashion. The proposed approach is to establish campus resolutions that will structure the detailed development of UCLA security policy in the CSG.

**Proposed schedule:**

- **February 17th ITPB:** Understanding of proposed resolutions and implications; Action: General guidance for CSG work
- **February 24th CSG:** Preliminary assessment
- **March 19th ITPB:** Discussion of preliminary assessment and vote on campus resolutions
- **March 23rd and April 27th CSG:** Development and votes on individual policy recommendations
- **April 20th and May 21st ITPB:** Approval and execution of operating policy

**Draft ITPB Resolutions:**

1. **ITPB Resolution #1:** Each campus unit is responsible for its impact institutionally, on the campus backbone network and beyond.
   - **Example implication:** If a system in a department is compromised and begins generating a tremendous outbound data stream through our commodity Internet connection, any additional charge would accrue to that department. A similar system that overwhelms the campus’s connection to the world would be rate-limited, which could adversely affect that department’s connectivity in other areas.
   - **CSG work:** How should incidents be reported and how are they closed?

2. **ITPB Resolution #2:** All devices connecting to the campus network must meet minimum security standards.
• **Example implication:** If a device does meet minimum standards, it will not be allowed to connect to the network.

• **CSG work:** Define minimum standards such as antivirus software required, patch management solution required, no proxy services allowed, no unauthenticated email relays allowed, etc. (Already have a basic draft of what this should look like based on Berkeley work just released.)

3. **ITPB Resolution #3:** During a security event, CTS will first protect the campus backbone network and isolate the problem traffic, network or hosts.

• **Example implication:** This strategy prioritizes the good of the whole over the good of individuals/individual units. Thus it does not take into account whether some individuals/units/services should be more highly prioritized than others (for example: senior leadership, academic units or student administrative services).

• **CSG work:** CTS already has a blocking policy, but this needs to be reconfirmed and the details made explicit. (It's now particularly crucial to set uniform expectations with departments adopting the use of NAT, which means blocking a single IP address means blocking the entire department.)

4. **ITPB Resolution #4:** OIT, working in conjunction with CTS, will proactively work to minimize threats to the campus network.

• **Example implication 1:** The campus needs a good understanding of what its network looks like under “average” conditions to make handling of security crises more effective. To accomplish this, CTS will routinely profile the UCLA network. Campus units that have firewalls or otherwise block such scans must either allow these scans or perform these scans locally and report results to CTS.

• **Example implication 2:** CTS will routinely perform penetration testing, notifying units of vulnerable devices. (Note: This kind of activity is already happening continuously from the outside, but in a hostile manner.)

• **CSG work:** Define procedures between CTS and local units.

5. **ITPB Resolution #5:** There need to be consequences for non-compliance (beyond blocking of a device from the network) and an avenue for recourse when disputes arise.

• Proposed Policy/Campus Support Action Agenda

• ITPB Cost Reduction Response to the Chancellor
ITPB Email Namespace Resolutions

Background: The Email Model Task Force has developed a set of operating policy recommendations for email namespace and directories to position the campus for email business and communication with the individual. These recommendations have been approved by the Enterprise Computing Committee (now CITI). These recommendations are brought back to the ITPB for changes, approval and execution.

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” that can be selected, and 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 are required to publish their email addresses in an internal (visible only to UCLA) directory, but they may petition to opt-out. Publishing in an external directory is optional.

Remote Access Services

Background: The University spends significant funds to reimburse individuals for broadband home connectivity and also supports a dial-in service that is largely no cost. It is also clear that remote access services are vital to the productivity of the university. There is no apparent uniform policy or guidelines for home connectivity reimbursements and the no-cost, dial-in services philosophy has not been revisited for some time.

1. Should there be a university policy or guidelines on reimbursed home connectivity?

2. Should BOL dial-in retain its current structure of no-cost access with a liberal connectivity time?