UC INFORMATION SECURITY WORK GROUP REPORT

I. Executive Summary

Since California's security breach notification law took effect in July, 2004, UC has followed a rigorous set of guidelines for notifying individuals whose personal information may have been acquired as a result of a computer security breach. Many UC campuses have experienced thefts of laptop computers, compromised servers or other events involving unauthorized access to personally identifying information and have notified affected individuals of the possible risks and repercussions of such breaches. Recent security breaches have captured the attention of the media and drawn the anger of many affected individuals. They have also served as catalysts for new proposed state and federal legislation focused on ensuring greater safeguards for personal data and greater accountability for organizations that are stewards of this data.

President Dynes and the Chancellors requested that a University-wide group be formed to assess the effectiveness of UC's current efforts to safeguard personal information and to recommend further initiatives to reduce the number and severity of security breaches in the future. This report summarizes the deliberations and recommendations of the work group, comprised of academic and administrative leaders throughout the University. Although it is not exhaustive of all possible preventive strategies, this report discusses a broad range of actions that the University should take in order to ensure information security and to successfully prevent breaches of restricted information in the future.

Section V summarizes these recommendations, which include:

- Leadership actions to establish roles and responsibilities for information security and to enforce standards of accountability for security breaches
- University-wide and campus-based security education and awareness activities
- Guidelines for effective handling of security incidents
- Stronger information security policies to address minimum connectivity standards and guidelines for allowable use of restricted data
- Campus security programs to ensure required risk assessments and mitigation strategies at the academic and administrative unit level
- Promotion of campus-based data encryption programs

This report will be reviewed at the September Council of Chancellors meeting.